Mathematik für die Informatik I

Goethe-Universität Frankfurt am Main

Wintersemester 2017/18

Dr. Samuel Hetterich

5. Januar 2018

Inhaltsverzeichnis

Vorwort

Dieses Skript ist Grundlage der Vorlesung “Mathematik für die Informatik I” gehalten von Dr. Samuel Hetterich im Wintersemester 2017/18 an der Goethe-Universität in Frankfurt am Main.

Das Skript wird im Laufe des Semesters weiterentwickelt - die entsprechenden Abschnitte sollten aber in ihrer endgültigen Form jeweils vor den einzelnen Vorlesungen zur Verfügung stehen. Bei Anmerkungen, Kritik und Korrekturvorschlägen zögern Sie bitte nicht, sich an Herrn Dr. Samuel Hetterich (hetterich@math.uni-frankfurt.de) zu wenden.

Teile des vorliegenden Manuskripts sind aus den Skripten zu der gleichen Vorlesung vorangegangener Semester von Herrn Dr. Hartwig Bosse und Herrn Prof. Amin Coja-Oghlan übernommen.

Teil I.

Elementares

1 Grundlagen

Dieses Kapitel enthält Grundlagen aus der Vorlesung “Mathe für die Informatik I” und richtet sich an all jene, die diese Vorlesung noch nicht gehört haben.

Wir beginnen mit einigen sehr grundlegenden mathematischen Konzepten, die zum Teil schon aus der Schulmathematik bekannt sein sollten und in der Vorlesung häufig als “Handwerkszeug” in den unterschiedlichen Kontexten auftauchen werden.

1.1. Mathematische Logik: Aussagen und Logische Quantoren

Unter einer mathematischen Aussage versteht man eine mathematische Formel, oder eine formal-logische Aussage, der ein Wahrheitswert “wahr” oder “falsch” zugewiesen werden kann.

- Der Ausdruck “$x^2 - 2x + 1$” ist *keine* mathematische Aussage sondern nur ein mathematischer Term.
- Der Ausdruck “$x^2 - 2x + 1 = 0$” ist eine mathematische Aussage (die je nach Wert von x wahr oder falsch ist).
- Der Ausdruck “$1 = 0$” ist eine mathematische Aussage, die falsch ist.
- Der Ausdruck “4 ist eine Quadratzahl” ist eine mathematische Aussage, die richtig ist.
- Die Goldbach-Vermutung “Jede gerade natürliche Zahl größer als 2 kann als Summe zweier Primzahlen geschrieben werden.“ ist eine mathematische Aussage von der bisher nicht klar ist, ob sie wahr oder falsch ist.

Wie Aussagen im “normalen” Leben, muss jede mathematische Aussage ein Verb enthalten. Diese Verben stecken oft in *logischen Quantoren* oder *logischen Operatoren*, die im Grunde Abkürzungen für Textbausteine sind. In den obigen Beispielen steckt das Verb an einigen Stellen in dem Operator “=”, den man als “. . . ist gleich . . .” liest.

In den folgenden Tabelle sind die von uns verwendeten logischen Operatoren und Quantoren aufgelistet.

- **Liste der verwendeten Operatoren:**

Symbol	Name	Zugehörige Formulierung	Beispiel
$\neg$	Negation	Es gilt nicht . . .	$\neg[3 = 4]$
$\vee$	Oder	Es gilt . . . oder . . .	$[n \geq 2] \vee [n \leq 2]$
$\dot{\vee}$	Exklusives Oder	Es gilt **entweder** . . . oder . . .	$[n \geq 2] \dot{\vee} [n \leq 2]$
$\wedge$	Und	Es gilt . . . und . . .	$[n \geq 2] \wedge [n \leq 2]$

- **Liste der verwendeten Quantoren:**

Symbol	Name	Zugehörige Formulierung	Beispiel
$\forall$	All-Quantor	Für alle . . .	$\forall n \in \mathbb{N} : n \geq 0$
$\exists$	Existenz-Quantor	Es existiert (mindestens) ein . . .	$\exists n \in \mathbb{N} : n \geq 5$
$\exists!$		Es existiert **genau** ein . . .	$\exists! n \in \mathbb{N} : n^2 = 25$
$\nexists$		Es existiert **kein** . . .	$\nexists n \in \mathbb{N} : n < 0$

Es gelten in gewissem Sinne “Rechenregeln” für mathematische Aussagen. Dabei spielen die Begriffe der ***Äquivalenz*** und der ***Implikation*** eine entscheidende Rolle, welche mathematische Aussagen in Relation setzen.

Definition 1.1.1.

- Eine mathematische Aussage $\mathcal{A}$ ***impliziert*** eine weitere mathematische Aussage $\mathcal{B}$, wenn aus der Wahrheit der Aussage $\mathcal{A}$ die Wahrheit der Aussage $\mathcal{B}$ folgt. Man schreibt dann
$$\mathcal{A} \Rightarrow \mathcal{B}.$$
- Zwei mathematische Aussagen $\mathcal{A}$ und $\mathcal{B}$ sind ***äquivalent***, wenn $\mathcal{A}$ die Aussage $\mathcal{B}$ impliziert und umgekehrt auch $\mathcal{B}$ die Aussage $\mathcal{A}$ impliziert. In diesem Fall schreibt man
$$\mathcal{A} \Leftrightarrow \mathcal{B}.$$
(Die “Formel”: *. . . genau . . . dann . . . , wenn . . .* weist auf Äqivalenz in gesprochener Sprache hin.)

Beispiel 1.1.2.

- Es ist $n \geq 5 \Rightarrow n \geq 3$. Umgekehrt ist dies jedoch nicht der Fall.
- Ein Dreieck ist genau dann gleichseitig, wenn alle Seiten die gleiche Länge haben.

Bemerkung 1.1.3.

Interessanterweise sind die Implikationen $\mathcal{A} \Rightarrow \mathcal{B}$ und $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$ gleichbedeutend. Denn wenn $\mathcal{A}$ die Aussage $\mathcal{B}$ impliziert, dann kann $\mathcal{A}$ nicht wahr sein, wenn $\mathcal{B}$ nicht wahr ist. Ergo impliziert $\neg\mathcal{B}$ die Aussage $\neg\mathcal{A}$.

Bemerkung 1.1.4.

Im Fall der Äquivalenz sind die Aussagen entweder beide wahr oder beide falsch - sie sind gleichwertig. Daher erschließt sich der Name aus dem Lateinischen: *aequus* “gleich” und *valere* “wert sein”.

Eine schöne Veranschaulichung für den Unterschied zwischen Äquivalenz und Implikation ist diese Eselsbrücke: "Wenn es geregnet hat, ist die Straße nass. Aber wenn die Straße nass ist, heißt das nicht zwangsläufig, dass es geregnet hat."

$$\text{“Es hat geregnet.”} \Rightarrow \text{“Die Straße ist nass.”}$$

$$\text{“Die Straße ist nass.”} \not\Rightarrow \text{“Es hat geregnet.”}$$

Aber es ist nach Bemerkung 1.1.3

$$\neg(\text{“Die Straße ist nass.”}) \Rightarrow \neg(\text{“Es hat geregnet.”})$$

was umformuliert heißt

$$\text{“Die Straße ist nicht nass.”} \Rightarrow \text{“Es hat nicht geregnet.”}$$

Wie angekündigt nun die “Rechenregeln” für mathematische Aussagen.

Lemma 1.1.5.

Es seien $\mathcal{A}, \mathcal{B}, \mathcal{C}$ mathematische Aussagen. Dann gelten

$$\begin{aligned} \mathcal{A} \wedge \mathcal{B} &\Leftrightarrow \mathcal{B} \wedge \mathcal{A} \\ \mathcal{A} \vee \mathcal{B} &\Leftrightarrow \mathcal{B} \vee \mathcal{A} \end{aligned} \qquad \text{(Kommutativgesetze)}$$

$$\begin{aligned} [\mathcal{A} \wedge \mathcal{B}] \wedge \mathcal{C} &\Leftrightarrow \mathcal{A} \wedge [\mathcal{B} \wedge \mathcal{C}] \\ [\mathcal{A} \vee \mathcal{B}] \vee \mathcal{C} &\Leftrightarrow \mathcal{A} \vee [\mathcal{B} \vee \mathcal{C}] \end{aligned} \qquad \text{(Assoziativgesetze)}$$

$$\begin{aligned} [\mathcal{A} \wedge \mathcal{B}] \vee \mathcal{C} &\Leftrightarrow [\mathcal{A} \vee \mathcal{C}] \wedge [\mathcal{B} \vee \mathcal{C}] \\ [\mathcal{A} \vee \mathcal{B}] \wedge \mathcal{C} &\Leftrightarrow [\mathcal{A} \wedge \mathcal{C}] \vee [\mathcal{B} \wedge \mathcal{C}] \end{aligned} \qquad \text{(Distributivgesetze)}$$

Bezüglich des Negierens gelten die folgenden Regeln.

Lemma 1.1.6.

Es seien $\mathcal{A}, \mathcal{B}$ mathematische Aussagen. Dann gelten

i. $\neg(\mathcal{A} \vee \mathcal{B}) = (\neg\mathcal{A}) \wedge (\neg\mathcal{B})$
ii. $\neg(\mathcal{A} \wedge \mathcal{B}) = (\neg\mathcal{A}) \vee (\neg\mathcal{B})$

Bemerkung 1.1.7.

Negiert man eine Aussage, die mit einem All- oder Existenzquantor beginnen, so taucht in der negierten Aussage stets der andere Quantor auf. Dies ist wichtig für den Beweis von Aussagen durch Widerspruch, hier wird in der einleitenden Widerspruchsannahme die Originalaussage negiert.

1.2. Mengen

Wir beginnen mit dem Begriff der Menge, welche an dieser Stelle aufgrund einiger Komplikationen in den Details nicht im strengen mathematischen Sinne sauber definiert werden kann. Für unsere Zwecke bedienen wir uns der (naiven) Mengendefinition von Georg Cantor (1845-1918), dem Begründer der Mengentheorie:

> *Eine Menge ist eine Zusammenfassung bestimmter wolunterschiedener Objekte unserer Anschauung oder unseres Denkens, welche Elemente genannt werden, zu einem Ganzen.*

Diese sehr einleuchtende und der alltäglichen Verwendung des Begriffs der Menge sehr nahe Umschreibung führt allerdings bei näherer Untersuchung zu Komplikationen.

Exkurs 1.2.1 (Die Russelsche Antinomie)**.**

Definiert man Mengen als “Zusammenfassung unterscheidbarer Objekte” so ergibt sich das folgende Paradoxon:

Die Menge der Mengen, welche sich nicht selbst enthalten. (1.1)

Gäbe es diese Menge, und nennen wir sie A, so stellt sich die Frage:

Enthät A sich selbst? (1.2)

- Beantworten wir Frage (1.2) mit JA so ergibt sich ein Widerspruch:
  - Wir nehmen an A enthält die Menge A (weil wir die Frage (1.2) mit JA beantworten).
  - Damit ist A (als Menge) keine jener erlesenen Mengen, die wir unter dem Titel “Mengen die sich nicht selbst enthalten” in A versammelt haben.
  - D.h. A ist nicht dabei, ergo: A ist (doch) nicht in A enthalten.
  - Ein Widerspruch!
- Beantworten wir Frage (1.2) mit NEIN so ergibt sich ein Widerspruch:
  - Wir nehmen an A enthält die Menge A nicht (weil wir die Frage (1.2) mit NEIN beantworten).
  - Damit ist A (als Menge) eine jener erlesenen Mengen, die wir unter dem Titel ”Mengen die sich nicht selbst enthalten” in A versammelt haben.
  - D.h. A ist dabei, ergo: A ist (doch) in A enthalten.
  - Ein Widerspruch!

Wir beginnen mit Konventionen und Definitionen bezüglich der Notation grundlegender Begriffe im Kontext von Mengen. Seien A und B Mengen.

Definition 1.2.2 (Mengendefinitionen und -notationen)**.**

- Mengen werden mit "{ " und " }" den *Mengenklammern* geschrieben.
- Die Schreibweise $x \in A$ bedeutet, dass x ein ***Element*** der Menge A ist.
- Ferner bedeutet $A \subset B$ (bzw. $B \supset A$), dass A eine ***Teilmenge*** von B ist, d.h. jedes Element von A ist auch ein Element von B.
- Wir nennen die Mengen A und B ***gleich***, wenn sie die gleichen Elemente enthalten.
- Eine Teilmenge A von B heißt ***echt***, wenn A nicht gleich B ist.
- Mit $A \cup B$ bezeichnen wir die ***Vereinigung*** von A und B; die Menge aller Element, die in A oder in B enthalten sind.
- Außerdem ist $A \cap B$ der ***Durchschnitt*** von von A und B; die Menge aller Elemente, die in A und B enthalten sind.
- Mit $A \setminus B$, gesprochen **"A ohne B"**, bezeichnen wir die Menge aller Elemente von A, die nicht Element von B sind (auch ***Differenz*** genannt).
- Schließlich ist $A \times B$ die ***Produktmenge*** von A und B, d.h. die Menge aller geordneten Paare (x, y) mit $x \in A$ und $y \in B$ (auch *kartesisches Produkt* genannt). Siehe auch Beispiel 1.2.3.
- Eine Menge A heißt ***endlich***, wenn A nur endlich viele Elemente besitzt.
- Die Anzahl der Elemente einer endlichen Menge A wird als die ***Kardinalität*** von A bezeichnet, und mit $|A|$ notiert (auch ***Mächtigkeit*** genannt). Ist A nicht endlich so schreibt man $|A| = \infty$.
- Die ***leere Menge*** notiert mit $\emptyset$ ist diejenige Menge, die keine Elemente enthält.
- Für eine Menge A is die ***Potenzmenge*** $\mathcal{P}(A)$ die Menge aller Teilmengen von A inklusive der leeren Menge $\emptyset$. Siehe auch Beispiel 1.2.4.
- Eine Menge ist definiert, wenn angegeben ist, welche Elemente in ihr enthalten sind. Dies kann *deskriptiv* - durch Angabe einer definierenden Eigenschaft ($A := \{n \in \mathbb{N} : n \text{ ist gerade}\}$) - und *konstruktiv* - durch Aufzählung aller in ihr enthaltenen Elemente ($B := \{2, 4, 6, 8, 10\}$) - geschehen. Wenn bei Mengen mit unendlich vielen Elementen das Bildungsgesetz klar ist, können auch unendliche Aufzählungen verwendet werden ($A := \{2, 4, 6, 8, \ldots\}$).
- Es bezeichnet $\mathbb{N} = \{1, 2, 3, \ldots\}$ die Menge der ***natürlichen Zahlen***. Es bezeichnet $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ die Menge der natürlichen Zahlen mit der Null.
- Es bezeichnet $\mathbb{Z} = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$ die Menge der ***ganzen Zahlen***.
- Es bezeichnet $\mathbb{Q}$ die Menge der ***rationalen*** und $\mathbb{R}$ die Menge der ***reellen Zahlen***.

Beispiel 1.2.3 (Produktmenge)**.**

Für $A = \{1, 2, 3\}$ und $B = \{3, 4\}$ ist

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$

Beispiel 1.2.4 (Potenzmenge)**.**

Für $A = \{1, 2, 3\}$ ist

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

In einem gewissen Sinne lässt sich mit Mengen und den ***Operatoren*** Durchschnitt und Vereinigung (Differenz und dem kartesischen Produkt) rechnen. Es gelten die folgenden "Rechenregeln".

Lemma 1.2.5.

Für beliebige Mengen A, B und C gilt:

$$\left.\begin{aligned} A \cap B &= B \cap A \\ A \cup B &= B \cup A \end{aligned}\right\} \quad \text{(Kommutativgesetze)}$$

$$\left.\begin{aligned} (A \cap B) \cap C &= A \cap (B \cap C) \\ (A \cup B) \cup C &= A \cup (B \cup C) \end{aligned}\right\} \quad \text{(Assoziativgesetze)}$$

$$\left.\begin{aligned} (A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \end{aligned}\right\} \quad \text{(Distributivgesetze)}$$

Im Folgenden Beweis stehen die Symbole "$\subset$" und "$\supset$" für folgende Textüberschriften:

" $\subset$ " entspricht: "Wir Zeigen nun: linke Menge ist enthalten in rechter Menge".

" $\supset$ " entspricht: "Wir Zeigen nun: rechte Menge ist enthalten in linker Menge".

Diese Symbole sind also Abkürzungen und nicht als mathematische Symbole zu deuten.

Beweis. [Beweis von Lemma 1.2.5] Wir beweisen exemplarisch die erste der beiden in Lemma 1.2.5 als Distributivgesetz bezeichneten Gleichungen. Zu zeigen ist:

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

Nach der Definition von Mengengleichheit müssen wir zeigen, dass die rechte menge in der linken un die linke in der rechten Menge enthalten ist.

"$\subset$": Es sei $x \in (A \cap B) \cup C$ beliebig gewählt. Für x gilt dann:

$$\begin{aligned} & x \in (A \cap B) \cup C \\ \Leftrightarrow \quad & [x \in (A \cap B) \vee x \in C] \\ \Leftrightarrow \quad & [(x \in A \wedge x \in B) \vee x \in C] \end{aligned} \tag{1.3}$$

Es gibt nun zwei Fälle:

Fall 1 $x \in C$**:** Es gilt demnach $x \in A \cup C$ und $x \in B \cup C$.
Fall 2 $x \notin C$**:** Es folgen aus (1.3) demnach sofort $x \in A$ und $x \in B$. Damit gilt auch $x \in A \cup C$ und $x \in B \cup C$.

In beiden Fällen gilt also $x \in A \cup C$ und $x \in B \cup C$ und damit $x \in (A \cup C) \cap (B \cup C)$.

Da x beliebig gewählt war gilt also allgemein für alle $x \in (A \cap B) \cup C$, dass

$$x \in (A \cap B) \cup C \qquad \Longrightarrow \qquad x \in (A \cup C) \cap (B \cup C).$$

Damit gilt nach der Defintiont von "$\subset$" also $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$.

"$\supset$": Es sei $x \in (A \cup C) \cap (B \cup C)$ beliebig gewählt. Für x gilt dann:

$$\begin{aligned} & x \in (A \cup C) && \cap && (B \cup C) \\ \Leftrightarrow\ & [x \in (A \cup C) && \wedge && x \in (B \cup C)] \\ \Leftrightarrow\ & [(x \in A \vee x \in C) && \wedge && (x \in B \vee x \in C)] \end{aligned} \tag{1.4}$$

Es gibt nun zwei Fälle:

Fall 1 $x \in C$**:** Es folgt demnach $x \in (A \cap B) \cup C$.
Fall 2 $x \notin C$**:** Es folgen aus (1.4) demnach sofort $x \in A$ und $x \in B$ und damit $x \in (A \cup C) \cap (B \cup C)$.

In beiden Fällen gilt also $x \in (A \cap B) \cup C$

Da x beliebig gewählt war, gilt also allgemein für alle $x \in (A \cup C) \cap (B \cup C)$, dass

$$x \in (A \cap B) \cup C \qquad \Leftarrow \qquad x \in (A \cup C) \cap (B \cup C).$$

Damit gilt nach der Definition von Teilmengen also $(A \cap B) \cup C \supset (A \cup C) \cap (B \cup C)$. □

Lemma 1.2.6.

Für eine endlichen Menge A mit Kardinalität n gilt: Die Potenzmenge $\mathcal{P}(A)$ hat Kardinalität 2^n.

In der Mathematik lassen sich Aussagen häufig auf unterschiedliche Weisen zeigen. Für den Satz des Pythagoras sind beispielsweise mehrere hundert verschiedene Beweise bekannt. Der Satz des Pythagoras ist damit übrigens der meistbewiesene mathematische Satz. Für Lemma 1.2.6 ist ebenfalls mehr als ein Beweis bekannt. Zum einen kann man die Menge aller Teilmengen, also die Potenzmenge, mit einer zweiten Menge in Eins-zu-eins-Relation bringt. Der Trick besteht darin, dass dabei jedem Element aus der Potenzmenge genau ein Element aus der zweiten Menge und tatsächlich jedem Element aus der zweiten Menge auch ein Element der Potenzmenge zugeordnet wird. Folglich enthalten beide Mengen also genau gleich viele Elemente. Die zweite Menge stellt sich dann schlussendlich als leicht zu zählen heraus.

Neben diesem Beweis, der die im folgenden Abschnitt erinnerten Begriff im Zusammenhang von Abbildungen verwendet, existiert ein weiterer Beweis über eine Beweistechnik mit dem Namen ***vollständige Induktion***. Wir betrachten beide Beweise im Anschluss an Abschnitt 1.3.

1.3. Abbildungen

Wir starten mit grundlegenden Definitionen von Abbildungen.

Definition 1.3.1 (Abbildungen)**.**

Eine ***Abbildung*** (oder auch ***Funktion***) $f : D \to B, x \mapsto f(x)$ bildet Werte aus dem ***Definitionsbereich*** D in den ***Bildbereich*** B ab. Jedem Element $x \in D$ wird durch f genau ein ***Bild*** $f(x) \in B$ zugeordnet. Gilt $f(x) = y$ für ein $y \in B$, so nennt man x das ***Urbild*** von y. Jedes $x \in D$ besitzt ein Bild $f(x)$, aber nicht jedes Element $y \in B$ muss ein Urbild besitzen.

Dies verallgemeinert man für eine Abbildung $f : D \to B$ und eine Teilmenge $Z \subset D$ ist

$$f(Z) = \{f(z) : z \in Z\}$$

die ***Bildmenge*** (manchmal auch einfach das Bild) von Z unter f. Umgekehrt bezeichnen wir für $C \subset B$ mit

$$f^{-1}(C) = \{x \in D : f(x) \in C\}$$

die ***Urbildmenge*** (manchmal auch einfach das Urbild) von C.

Abbildungen können drei ganz grundlegende Eigenschaften besitzen.

Definition 1.3.2 (Injektivität, Surjektivität, Bijektivität)**.**

Eine Abbildung heißt

- ***injektiv***, wenn je zwei verschiedene $x, x' \in D$ auch verschiedene Bilder besitzen, d.h. wenn gilt:

$$x \neq x' \implies f(x) \neq f(x')$$

- ***surjektiv***, wenn jeder Bildpunkt $y \in B$ tatsächlich auch ein Urbild $x \in D$ besitzt mit $y = f(x)$, d.h. wenn gilt:

$$\forall\, y \in B\ \exists\, x \in D : f(x) = y$$

- ***bijektiv***, wenn f injektiv und surjektiv ist.

Bemerkung 1.3.3.

Injektiv: Die Definition für "injektiv" kann man sich anschaulich vorstellen als: Die Definitionsmenge D wird in die Bildmenge "injiziert", d.h. man findet für jedes $x \in D$ einen eigenen Funktionswert $y \in B$ vor, "der einmal x war".

Surjektiv: Eine surjektive Abbildung dagegen "deckt die ganze Bildmenge ab", jeder Bildpunkt wird bei einer surjektiven Abbildung auch tatsächlich angenommen. Dies ist nicht selbstverständlich: Das Wort "Bildmenge" klingt zwar wie "die Sammlung aller Bilder f (x)". Tatsächlich kann die Bildmenge aber auch einfach nur eine "grobe Schätzung" sein, wie im Beispiel $g : \mathbb{R} \to \mathbb{R}$ mit $g(x) := x^2$. Dabei sind die Werte von g stets nicht-negativ, d.h. man "erreicht" mit g nicht die ganze Bildmenge $\mathbb{R}$.

Bijektiv: Eine bijektive Abbildung stellt eine Eins-zu-Eins-Relation zwischen Definitionsmenge D und Bildmenge B her. D.h. jedes $x \in D$ hat zum einen "sein eigenes(!)" Bild $f(x) \in B$, aber auch jeder Punkt $y' \in B$ hat genau(!) ein Urbild $x' \in D$. Daraus folgt: Sind D und B endliche Mengen und sind sie über eine bijektive Abbildung $f : D \to B$ verknüpft, so haben D und B gleich viele Elemente. Der Begriff einer bijektiven Abbildung ist in der Mathematik also beim Zählen von Dingen von zentraler Bedeutung.

Es folgt eine weitere sehr umfangreiche Definition.

Definition 1.3.4.

Falls f eine bijektive Abbildung ist, so hat für jedes $y \in B$ die Menge $f^{-1}(\{y\})$ genau ein Element $x \in D$ und wir schreiben einfach $x = f^{-1}(y)$. Die Abbildung $f^{-1} : B \to D, y \mapsto f^{-1}(y)$ ist in diesem Fall ebenfalls bijektiv und heißt die ***Umkehrabbildung*** von f.

Für eine Menge B und eine Zahl $k \in \mathbb{N}$ bezeichnen wir mit B^k die Menge aller Abbildungen $f : \{1, \ldots, k\} \to B$. Anstelle der Notation $f : D \to B, x \mapsto f(x)$ schreiben wir mitunter etwas lax $(f(x))_{x \in D}$. Diese Notation wird häufig verwendet, wenn $D = \{1, 2, 3, \ldots, k\}$ für eine Zahl $k \in \mathbb{N}$. Insbesondere schreiben wir die Elemente f der Menge B^k als $(f(1), \ldots, f(k))$; sie werden auch k-Tupel (und im Fall $k = 2$ Paare und im Fall $k = 3$ Tripel) genannt. Allgemeiner bezeichnen wir mit B^D die Menge aller Abbildungen $f : D \to B$. Ist $(A_i)_{i \in I}$ eine Abbildung, die Elementen einer Menge I Teilmengen A_i einer Menge A zuordnet, so bezeichnet

$$\bigcup_{i \in I} A_i = \{x \in A : \text{ es gibt ein } i \in I \text{ mit } x \in A_i\}$$

die Vereinigung aller Mengen A_i. Analog ist

$$\bigcap_{i \in I} A_i = \{x \in A : \text{ für alle } i \in I \text{ gilt } x \in A_i\}$$

der Durchschnitt aller A_i.

Sei $f : A \to \mathbb{R}$ eine Abbildung von einer endlichen Menge $A \neq \emptyset$ in die reellen Zahlen. Dann existiert eine Bijektion $g : \{1, \ldots, k\} \to A$, wobei $k \in \mathbb{N}$. Wir definieren die ***Summe***

$$\sum_{a \in A} f(a) = f(g(1)) + f(g(2)) + \ldots + f(g(k))$$

und das ***Produkt***

$$\prod_{a \in A} f(a) = f(g(1)) \cdot f(g(2)) \cdots f(g(k)).$$

Falls A die leere Menge ist, interpretieren wir die Summe als 0 und das Produkt als 1.

Wir benötigen die Beweismethode der ***Induktion***. Die Grundlage des Induktionsprinzip ist folgende Tatsache.

> *Jede nicht-leere Menge natürlicher Zahlen enthält eine kleinste Zahl.*

Aus dieser Tatsache folgt

Lemma 1.3.5 ("Induktionsprinzip")**.**

Angenommen eine Menge $A \subset \mathbb{N}$ hat die beiden folgenden Eigenschaften.

i. $1 \in A$
ii. Wenn $1, \ldots, n \in A$, dann gilt auch $n + 1 \in A$.

Dann gilt $A = \mathbb{N}$.

Beweis. Angenommen $A \neq \mathbb{N}$. Dann ist die Menge $B = \mathbb{N} \setminus A$ nicht leer. Folglich gibt es eine kleinste Zahl $x \in B$. Aufgrund von i. ist $x \neq 1$. Ferner gilt $1, \ldots, x - 1 \in A$, weil x ja die kleinste Zahl in B ist. Nach ii. gilt also $x \in A$, im Widerspruch zu unserer Annahme, dass $x \in B$. □

Das Induktionsprinzip ermöglicht es uns, Beweise nach folgendem Schema zu führen.

i. Zeige, dass die Behauptung für $n = 1$ stimmt.
ii. Weise ferner nach, dass die Behauptung für $n + 1$ gilt, wenn sie für $1, \ldots, n$ gilt.

Dann folgt die Behauptung *für alle* $n \in \mathbb{N}$. Als Beispiel zeigen wir die *gaußsche Summenformel* (auch *kleiner Gauß* genannt).

Lemma 1.3.6 ("Kleiner Gauß")**.**

Die Summe der ersten n natürlichen Zahlen ist

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

Beweis. Wir führen die Induktion über n.

Induktionsverankerung: Im Fall $n = 1$ ist die rechte Seite

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

was tatsächlich der Summe der ersten 1 vielen natürlichen Zahlen entspricht.

Induktionsannahme: Wir nehmen als Induktionsvoraussetzung nun an, dass die Formel für $n \in \mathbb{N}$ gilt, also dass

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \tag{1.5}$$

Induktionsschluss: Für den Induktionsschluss berechnen wir nun die Summe der ersten $n+1$ vielen natürlichen Zahlen

$$\begin{aligned}\sum_{i=1}^{n+1} i &= (n+1) + \sum_{i=1}^{n} i \\ &= (n+1) + \frac{n(n+1)}{2} \qquad \text{[nach Induktionsannahme (1.5)]} \\ &= \frac{2n + 2 + n^2 + n}{2} = \frac{(n+1)((n+1)+1)}{2}\end{aligned}$$

wie behauptet. □

1.3.1. Beweis von Lemma 1.2.6

Wie schon angekündigt beweisen wir Lemma 1.2.6 auf zwei unterschiedliche Wege.

Beweis. [von Lemma 1.2.6 - Variante 1] Sei A eine Menge mit n Elementen. Sei $\mathcal{W}_n$ die Menge aller "Worte" bestehend aus den Buchstaben *i* und *d* mit genau n Buchstaben.

Es sei f eine bijektive Abbildung der Elemente in A in die Menge der natürlichen Zahlen 1 bis n. Diese

Abbildung ordnet die Elemente in A. Für jedes $a \in A$ existiert also eine eindeutiges $1 \leq j \leq n$ sodass $f(a) = j$.

Sei g eine Abbildung die jedem $B \in \mathcal{P}(A)$ das Wort $w \in \mathcal{W}_n$ zuordnet, sodass für alle $a \in A$ gilt

- der $f(a)$-te Buchstabe von w ist i, wenn $a \in B$ und
- der $f(a)$-te Buchstabe von w ist d, wenn $a \notin B$.

Diese Abbildung ist bijektiv.

- **Surjektivität**
  Zu zeigen: Für jedes Wort $w \in \mathcal{W}_n$ lässt sich eine Menge $B \in \mathcal{P}(A)$ finden, sodass $g(B) = w$.
  $\forall\, w \in \mathcal{W}_n\ \exists\, B \in \mathcal{P}(A) : g(B) = w.$
  Sei Q die Menge der Positionen von w, an welchen ein i steht. Sei $B = f^{-1}(Q)$. Es ist nun der $f(a)$-te Buchstabe von w ein i, wenn $a \in B$ und ein d, wenn $a \notin B$. Demnach wird B von g auf w abgebildet.
- **Injektivität**
  Zu zeigen: Es gibt keine zwei verschiedenen Mengen $B, B' \in \mathcal{P}(A)$ mit $g(B) = g(B')$.
  $\nexists B, B' \in \mathcal{P}(A) : [B \neq B' \wedge g(B) = g(B')].$
  Angenommen, es gibt zwei verschiedene Mengen $B, B' \in \mathcal{P}(A)$ sodass $g(B) = g(B')$. Dann gibt es ***ohne Beschränkung der Allgemeinheit*** ein Element $a \in B$, dass nicht in B' enthalten ist (sonst wäre B eine Teilmenge von B' - aber beide Mengen sind verschieden und somit gäbe es dann ein Element $a \in B'$, dass nicht in B enthalten ist - Umbenennung der Mengen liefert die Behauptung). Dann ist aber der $f(a)$-te Buchstabe von $g(B)$ ein i und der $f(a)$-te Buchstabe von $g(B')$ ein d und somit ist $g(B) \neq g(B')$ - ein Widerspruch zu unserer Annahme.

Wie wir schon beobachteten, haben zwei endliche Mengen genau dann die gleiche Kardinalität, wenn es eine bijektive Abbildung zwischen ihnen gibt.

Wir müssen also nur noch zählen, wie viele Wörter bestehend aus zwei Buchstaben und von der Länge n es gibt. Für jede Position gibt es 2 Möglichkeiten: Entweder steht dort ein i oder ein d. Insgesamt gibt es also 2^n unterschiedliche Wörter und somit hat die Potenzmenge einer endlichen Menge mit Kardinalität n selbst Kardinalität 2^n. □

Beweis. [von Lemma 1.2.6 - Variante 2] Wir führen die Induktion über n.

Induktionsverankerung: Im Fall $n = 1$ ist die Aussage einfach zu Prüfen. Die Potenzmenge besteht in diesem Fall aus den beiden Mengen $\emptyset$ und A selbst.

Induktionsannahme: Wir nehmen als Induktionsvoraussetzung an, dass die Potenzmenge einer Menge mit n Elementen Kardinalität 2^n habe.

Induktionsschluss: Für den Induktionsschluss nehmen wir an A habe $n + 1$ Elemente. Nun zeichnen wir ein Element $a \in A$ aus und betrachten die Menge $A' = A \setminus \{a\}$. Es gilt $|A'| = n$. Nach Induktionsvoraussetzung ist $|\mathcal{P}(A')| = 2^n$.

Wir beobachten, dass jede Teilmenge B von A entweder eine Teilmenge von A' ist oder das Element a enthält (in diesem Fall ist aber $B \setminus \{a\}$ eine Teilmenge von A'). Also können wir jeder Teilmenge $B \subset A$ genau eine Teilmenge von A' zuordnen, nämlich $B \setminus \{a\}$. Dabei wird jede Teilmenge von A' genau zwei Teilmengen von

A zugeordnet. Es gibt also zweimal soviele Mengen in $\mathcal{P}(A)$ als in $\mathcal{P}(A')$. Demnach ist

$$|\mathcal{P}(A)| = |\mathcal{P}(A')| \cdot 2 = 2^n \cdot 2 = 2^{n+1}.$$

□

Bemerkung 1.3.7.

Mit der Formulierung ***ohne Beschränkung der Allgemeinheit (o. B. d. A.)*** wird zum Ausdruck gebracht, dass eine Einschränkung (z. B. des Wertebereichs einer Variablen) nur zur Vereinfachung der Beweisführung vorausgesetzt wird (insbesondere zur Verringerung der Schreibarbeit), ohne dass die Gültigkeit der im Anschluss getroffenen Aussagen in Bezug auf die Allgemeinheit darunter leidet. Der Beweis wird nur für einen von mehreren möglichen Fällen geführt. Dies geschieht unter der Bedingung, dass die anderen Fälle in analoger Weise bewiesen werden können (z. B. bei Symmetrie). Durch o. B. d. A. können auch triviale Sonderfälle ausgeschlossen werden.

Abschließend noch ein Wort zu Beweistechniken. Mathematische Aussagen zu beweisen erfordert neben Fleiß und Sorgfalt in der Darstellung ein hohes Maß an Kreativität. In der Beschäftigung mit mathematischen Beweisen wird man feststellen, dass es allerdings Prinzipien gibt, die immer wieder angewendet werden. Wir haben schon das Induktionsprinzip kennen gelernt. An dieser Stelle noch der Hinweis auf zwei weitere Beweisprinzipien, die zunächst ähnlich aussehen, aber zu unterscheiden sind und schon unbemerkt in obigen Beweisen auftauchten.

► **Beweis durch Kontraposition** Das logische Prinzip hinter diesem Beweisprinzip haben wir schon in Bemerkung 1.1.3 beobachtet. Um zu zeigen, dass $\mathcal{A} \Rightarrow \mathcal{B}$ kann man auch zeigen, dass $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$.

Beispiel 1.3.8.

Sei n eine gerade Quadratzahl, dann ist $\sqrt{n}$ ebenfalls gerade.

Beweis. Wir möchten zeigen:

$$\text{“}n \text{ ist gerade Quadratzahl”} \Rightarrow \text{“}\sqrt{n} \text{ ist gerade”}.$$

Die Kontraposition ist

$$\neg(\text{“}\sqrt{n} \text{ ist gerade”}) \Rightarrow \neg(\text{“}n \text{ ist gerade Quadratzahl” })$$

also

$$\text{“}\sqrt{n} \text{ ist ungerade”} \Rightarrow \text{“}n \text{ ist ungerade”}$$

Sei also $\sqrt{n}$ eine ungerade, natürliche Zahl, also gibt es ein $k_1 \in \mathbb{N}$ sodass $\sqrt{n} = 2 \cdot k_1 + 1$. Dann ist

$$\begin{aligned} n &= (\sqrt{n})^2 \\ &= (2k_1 + 1)^2 \\ &= 4k_1^2 + 4k + 1 \\ &= 2(2k_1^2 + 2k_1) + 1 \end{aligned}$$

Setzte $k_2 = 2k_1^2 + 2k_1$. Dann ist $n = 2k_2 + 1$ also ungerade, was zu zeigen war. □

▶ **Beweis durch Widerspruch** Dabei möchte man die Wahrheit einer Aussage $\mathcal{A}$ beweisen und nimmt die Negation von $\mathcal{A}$, nämlich $\neg\mathcal{A}$ als wahr an und führt dies über logische Schlüsse zu einem Widerspruch. Also kann $\neg\mathcal{A}$ nicht wahr sein, also muss $\mathcal{A}$ wahr sein.

Beispiel 1.3.9.

Ein Beispiel findet man in der Variante 1 des Beweises von Lemma 1.2.6: Nachweis der Injektivität von g.

1.4. Relationen

Objekte, die zu unterscheiden sind, können dennoch in Bezug zueinander stehen. Der mathematische Begriff der Relation misst dieses „in (einem bestimmten) Bezug zueinander stehen“, er gibt für zwei Objekte entweder die Antwort „Ja, die beiden Objekte stehen in (in diesem bestimmten) Bezug zueinander“ oder „Nein, die Objekte stehen nicht (in diesem bestimmten) Bezug zueinander“. Wir erinnern zunächst an den Begriff des Kartesisches Produkts. Für zwei Mengen A, B heißt $A \times B := \{(a, b) \ : \ a \in A \wedge b \in B\}$ das **kartesische Produkt** von A und B.

Definition 1.4.1.

Eine **(binäre) Relation** zwischen zwei Mengen A und B ist eine Teilmenge $R \subseteq A \times B$. Im Falle $A = B$ spricht man von **einer Relation auf** A.

Eine Relation zwischen A und B ist also eine Teilmenge aller *geordneten* Paare der Form (a, b) mit $a \in A$ und $b \in B$.

Beispiel 1.4.2.

- ▶ Der Begriff „größer als“ induziert eine Relation auf der Menge aller Zahlen $\mathbb{N}$:

$$R := \{(a, b) \in \mathbb{N} \times \mathbb{N} \ : \ a > b\} = \{(2, 1), \ (3, 1), (3, 2), \ (4, 1), (4, 2), (4, 3), \ (5, 1), \ldots\}$$

- ▶ Funktionen sind Relationen:
  Die Paare aus Wert $x \in \mathbb{R}$ und Funktionswert $f(x)$ einer Funktion $f : \mathbb{R} \to \mathbb{R}$ bilden eine Relation auf $\mathbb{R}$

$$R := \{(x, y) \in \mathbb{R} \times \mathbb{R} \ : \ f(x) = y\}$$

- ▶ Der Begriff „verwandt sein mit“ (engl.: „related to“) beschreibt eine Relation auf der Menge aller Menschen.

Definition 1.4.3.

Eine Relation auf A heißt

- ▶ **reflexiv**, wenn für alle $a \in A$ gilt

$$(a, a) \in R.$$

- **symmetrisch**, wenn für alle $a, b \in A$ gilt

$$(a, b) \in R \Rightarrow (b, a) \in R.$$

- **transitiv**, wenn für alle $a, b, c \in A$ gilt

$$(a, b) \in R \text{ und } (b, c) \in R \Rightarrow (a, c) \in R.$$

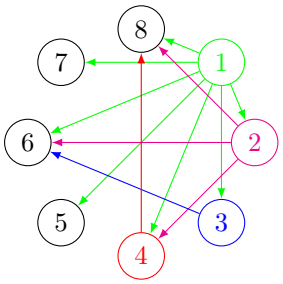
Beispiel 1.4.4.

- Wir betrachten die Teilbarkeitsrelation $R := \{(a, b) \in \mathbb{N} \times \mathbb{N} \ : \ a \text{ teilt } b\}$ auf der Menge der natürlichen Zahlen.
  Diese Relation ist reflexiv und transitiv, aber nicht symmetrisch.
- Auf $\mathbb{N}$ definiert $(a, b) \in R :\Leftrightarrow a > b$ die Relation $R := \{(a, b) \in \mathbb{N} \times \mathbb{N} \ : \ a > b\}$.
  Die Relation ist transitiv aber nicht reflexiv und nicht symmetrisch.

Bemerkung 1.4.5.

Im Fall einer endlichen Menge A kann eine Relation auf A durch einen gerichteten Graphen (mit möglichen Schlingen) visualisiert werden: Von einem Element $a \in A$ führt genau dann ein Bogen (gerichtete Kante) zu einem Element $b \in A$, wenn $(a, b) \in R$ gilt. Der gerichtete Graph in der unteren Abbildung zeigt den Graphen zur Teilbarkeitsrelation auf $\{1, \ldots 8\}$, d.h. den Graphen für

$$R := \{(a, b) \in \{1, \ldots, 8\} \times \{1, \ldots, 8\} : a \neq b \text{ und } a \text{ teilt } b\}.$$



1.4.1. Äquivalenzrelationen

Das Ziel bei der Verwendung von Äquivalenzrelationen ist, den Begriff „gleich“ (im Sinne von identisch) zu verallgemeinern auf „ähnlich“ bzw. „gleich bezüglich einer Eigenschaft“. So können z.B. zwei Gegenstände gleich sein im Bezug auf ihre Farbe (also die gleiche Farbe haben) ohne jedoch identisch zu sein.

Um den Begriff „gleich“ auf „ähnlich“ zu verallgemeinern, müssen wir sicherstellen, dass für die Verallgemeinerung weiter gilt, dass

- ein Gegenstand stets zu sich selbst ähnlich ist. (Reflexivität)
- wenn a zu b ähnlich ist, dann auch b zu a. (Symmetrie)
- wenn a ähnlich ist zu b und dies wiederum ähnlich ist zu c, so ist auch a ähnlich zu c. (Transitivität)

Definition 1.4.6 (Äquivalenzrelation)**.**

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

Wir schauen uns einige Beispiel von Relationen an.

Beispiel 1.4.7.

Es sei A die Menge aller Schüler einer Schule und

$$R := \{(a, b) \in A \times A \ : \ a \text{ ist in derselben Schulklasse wie } b\} \ .$$

Die Relation R ist eine Äquivalenzrelation

- Jeder Schüler $a \in A$ ist Schüler seiner (eigenen) Schulklasse, es gilt also $(a, a) \in R$. (Reflexivität)
- Ist $(a, b) \in R$, so ist Mitschüler a in derselben Schulklasse wie b.
  Also ist auch $(b, a) \in R$, denn b ist umgekehrt auch in derselben Schulklasse wie a. (Symmetrie)
- Wenn $(a, b) \in R$ und $(b, c) \in R$ gelten, dann gilt auch $(a, c) \in R$, denn es ist a in derselben Schulklasse wie b und b in derselben Schulklasse wie c, und das heißt a ist in der Schulklasse von c. (Transitivität)

Beispiel 1.4.8.

Es sei $R := \{(n, m) \in \mathbb{N} \times \mathbb{N} \ : \ m \text{ hat denselben Rest beim Teilen durch 2 wie } n\}$.

Die Relation R ist eine Äquivalenzrelation

- Jede Zahl $n \in \mathbb{N}$ hat einen festen Rest beim Teilen durch 2, es gilt also $(n, n) \in R$. (Reflexivität)
- Ist $(n, m) \in R$, so hat m denselben Rest beim Teilen durch 2 wie n.
  Also ist auch $(m, n) \in R$, denn n hat denselben Rest beim Teilen durch 2 wie m. (Symmetrie)
- Wenn $(n, k) \in R$ und $(k, m) \in R$ gelten, dann gilt beim Teilen durch 2:
  k hat denselben Rest wie n und m denselben Rest wie k, und das heißt m hat denselben Rest wie n. (Transitivität)

Die beiden „Schulklassen“ in den die Zahlen hier wahlweise gehen heißen „Gerade Zahlen“ oder „Ungerade Zahlen“.

Formal korrekt, aber trotzdem seltsam, ist das folgende Beispiel:

Beispiel 1.4.9 (Jede Relation über die Leere Menge ist eine Äquivalenzrelation)**.**

Es sei $A := \emptyset$ und $R \subseteq A \times A$. Dann ist R eine Äquivalenzrealtion.

Zunächst gilt besondererweise $R = \emptyset$ denn $A \times A = \emptyset \times \emptyset = \emptyset$.

- Reflexivität: Wegen $A = \emptyset$ gibt es *kein* $a \in A$.
  Also gibt es insbesondere kein $a \in A$ mit der Zusatzeigenschaft $(a, a) \notin R$.
  Kein $a \in A$ verletzt also die Reflexivität von R. R ist also reflexiv.
- Symmetrie: Wegen $R = \emptyset$ gibt es kein Paar $(a, b) \in R$.
  Also gibt es insbesondere kein Paar $(a, b) \in R$ mit der Zusatzeigenschaft $(b, a) \notin R$.
  Kein Paar $(a, b) \in R$ verletzt also die Symmetrie von R. R ist also symmetrisch.

- Transitivität: Wegen $R = \emptyset$ gibt es kein Paar $(a, b) \in R$.
  Also gibt es insbesondere kein $(a, b) \in R$ mit der Zusatzeigenschaft, dass es $(b, c) \in R$ gibt.
  Also gibt es kein Paar (a, b) für dass zwar $(b, c) \in \mathbb{R}$ gilt, aber nicht $(a, c) \in \mathbb{R}$.
  Kein Paar $(a, b) \in R$ verletzt also die Transitivität von R. R ist also transitiv.

Beispiel 1.4.10 (keine Äquivalenzrelation)**.**

Die Relation $R := \{(n, m) \in \mathbb{N} \times \mathbb{N} \ : \ n \leq m\}$ ist **nicht symmetrisch** und deswegen *keine* Äquivalenzrelation:

Es gilt zwar $(1, 2) \in R$ wegen $1 \leq 2$ aber es gilt nicht $(2, 1) \notin R$.

Die Relation R ist zwar reflexiv und transitiv, aber eben nicht symmetrisch.

Bemerkung 1.4.11.

Am Gegenbeispiel 1.4.10 sieht man:

Um zu zeigen, dass eine Relation keine *Äquivalenzrelation ist, genügt es zu zeigen, dass eine der benötigten Eigenschaften nicht gilt. Um wiederum zu zeigen, dass eine Relation z.B. nicht symmetrisch ist, genügt ein einziges Gegenbeispiel!*

Definition 1.4.12 (Äquivalenz)**.**

Es sei R eine Äquivalenzrelation auf A.

Für $(a, b) \in R$ schreibt man kurz $a \sim_R b$, und sagt: a und b sind ***äquivalent bezüglich*** R.

Wenn klar ist, welche Relation Gemeint ist, wird „$\sim_R$“ zu „$\sim$“ vereinfacht.

Das Symbol $\sim$ verallgemeinert das Symbol „$=$“, es gelten auf Ebene der logischen Operatoren die selben Regeln:

$a = b$	ist äquivalent zu	$b = a$.	(Symmetrie)	Aus $a = b$ und $b = c$	folgt $a = c$.	(Transitivität)
$a \sim b$	ist äquivalent zu	$b \sim a$.		Aus $a \sim b$ und $b \sim c$	folgt $a \sim c$.	

Definition 1.4.13 (Äquivalenzklasse)**.**

Es sei R eine Äquivalenzrelation auf A.

Für jedes Element $a \in A$ ist die ***Äquivalenzklasse***

$$[a]_R := \{b \in A \ : \ (a, b) \in R\}$$

die Menge der zu a äquivalenten (bzw. ähnlichen) Elemente aus A.

Beispiel 1.4.14 (Schul**klassen** sind Äquivalenz**klassen**)**.**

Es sei A die Menge aller Schüler einer Schule und

$$R := \{(a, b) \in A \times A \ : \ a \text{ ist in derselben Schulklasse wie } b\} \ .$$

Für jeden Schüler a bilden die Mitschüler seiner Schulklasse seine Äquivalenzklasse:

$$\begin{aligned}[a]_R &= \{b \in A \,:\, (a,b) \in R\} \\ &= \{b \in A \,:\, b \text{ ist in derselben Schulklasse wie } a\} = \big\{ \text{ Alle Schüler in der Schulkasse von } a \big\}\end{aligned}$$

Gilt $(a,b) \in R$, d.h. a und b sind in derselben (Schul-)Klasse (z.B. “6c”), so gilt $[a]_R = [b]_R$:

$$\begin{aligned}[a]_R &= \big\{ \text{ Alle Schüler in der Schulklasse von } a \big\} &= \big\{ \text{ Alle Schüler der 6c } \big\} \\ [b]_R &= \big\{ \text{ Alle Schüler in der Schulklasse von } b \big\} &= \big\{ \text{ Alle Schüler der 6c } \big\}\end{aligned}$$

Beispiel 1.4.15.

Es sei $R := \{(n,m) \in \mathbb{N} \times \mathbb{N} \,:\, m \text{ hat denselben Rest beim Teilen durch 2 wie } n\}$.

- Die Zahl 7 hat einen Rest von 1 beim Teilen durch 2, es gilt also:

$$\begin{aligned}[7]_R &= \{m \in \mathbb{N} \,:\, (7,m) \in R\} \\ &= \{m \in \mathbb{N} \,:\, m \text{ hat selben Rest beim Teilen durch 2 wie 7}\} \\ &= \{m \in \mathbb{N} \,:\, m \text{ hat Rest 1 beim Teilen durch 2}\} \\ &= \big\{ \text{ Alle ungeraden Zahlen} \big\}\end{aligned}$$

  Analog gilt $[3]_R = \big\{ \text{ Alle ungeraden Zahlen} \big\}$ und $[5]_R = \big\{ \text{ Alle ungeraden Zahlen} \big\}$ etc.
- Die Zahl 8 hat einen Rest von 0 beim Teilen durch 2, es gilt also:

$$\begin{aligned}[8]_R &= \{m \in \mathbb{N} \,:\, (8,m) \in R\} \\ &= \{m \in \mathbb{N} \,:\, m \text{ hat selben Rest beim Teilen durch 2 wie 8}\} \\ &= \{m \in \mathbb{N} \,:\, m \text{ hat Rest 0 beim Teilen durch 2}\} \\ &= \big\{ \text{ Alle geraden Zahlen} \big\}\end{aligned}$$

  Analog gilt $[2]_R = \big\{ \text{ Alle geraden Zahlen} \big\}$ und $[6]_R = \big\{ \text{ Alle geraden Zahlen} \big\}$ etc.

Die beiden „Schulklassen",’ in die die Zahlen hier wahlweise gehen, heißen „Grade Zahlen“ oder „Ungrade Zahlen“.

Anhand der Beispiele erkennt man bereits, dass zwei Äquivalenzklassen entweder „grundverschieden“ sind (leerer Schnitt) oder aber identisch sind. Dies ist einleuchtend, denn die Äquivalenzklasse $[a]_R$ besteht aus allen Elementen, die zu a äquivalent sind, d.h. gleich sind bezüglich der Eigenschaft, die R definiert.

Fordert man z.B. „1) Nenne alles, was dieselbe Länge hat wie a.“ und erhält als Antwort unter anderem b, so bekommt man auf die Aufforderung „2) Nenne alles, was dieselbe Länge hat wie b.“ dieselbe Antwort wie bei 1). Dies kann man dann mit beliebigen Eigenschaften wiederholen (Gewicht, Eckenanzahl etc.).

Diese Einsicht verallgemeinern wir zu „Zwei Elemente aus A haben bezüglich R genau dann dieselbe Äquivalenzklasse, wenn sie bezüglich R äquivalent sind“. Genauer gilt:

Lemma 1.4.16.

Es sei R eine Äquivalenzrelation über A.

i) Für $a, b \in A$ gilt dann entweder $[a]_R = [b]_R$ oder $[a]_R \cap [b]_R = \emptyset$.
ii) Es gilt $[a]_R = [b]_R$ genau dann wenn $(a, b) \in R$ gilt.

Beweis. Es sei R eine Äquivalenzrelation über A und $a, b \in R$ mit $a \neq b$.

Wir zeigen zunächst ii).

'$\Rightarrow$' Annahme: Es gelte $[a]_R = [b]_R$. Wegen $(b, b) \in R$ gilt $b \in [b]_R$ und damit $b \in [a]_R$ bzw. $(a, b) \in R$.

'$\Leftarrow$' Annahme: Es gelte $(a, b) \in R$. Wir zeigen $[a]_R \subseteq [b]_R$ und $[b]_R \subseteq [a]_R$.
Sei nun $x \in [a]_R$, so gilt $(a, x) \in R$ und da R eine Äquivalenzrelation ist gilt damit

$$(a, x), (a, b) \in R \quad \Rightarrow \quad (x, a), (a, b) \in R \quad \Rightarrow \quad (x, b) \in R \quad \Rightarrow \quad x \in [b]_R$$

Da x beliebig war folgt also $[a]_R \subseteq [b]_R$. Ganz analog beweist man $[b]_R \subseteq [a]_R$. Es gilt also: $[a]_R = [b]_R$.

Wir zeigen nun i): Es seien $a, b \in A$ mit $[a]_R \cap [b]_R \neq \emptyset$. Zu zeigen ist: $[a]_R = [b]_R$.

Sei $c \in [a]_R \cap [b]_R$ beliebig. Nach Def. der Äquivalenzklassen gilt: $(a, c), (b, c) \in R$ und da R eine Äquivalenzrelation ist gilt damit

$$(a, c), (b, c) \in R \quad \Rightarrow \quad (a, c), (c, b) \in R \quad \Rightarrow \quad (a, b) \in R$$

Aus ii) schließen wir nun: $[a]_R = [b]_R$. □

Aus Lemma 1.4.16 schließen wir, dass es genügt, ein *einziges* Element einer Äquivalenzklasse zu kennen, um die Äquivalenzklasse zu rekonstruieren:

Definition 1.4.17 (Vertreter einer Äquivalenzklasse)**.**

Es sei $M \subseteq A$ eine Äquivalenzklasse einer Äquivalenzrelation R auf der Menge A.

Ein Element $x \in M$ heißt dann ***Vertreter*** der Äquivalenzklasse M, denn es gilt $[x]_R = M$.

Beispiel 1.4.18 (Jeder Schüler ist Vertreter seiner Schul**klasse**)**.**

Es sei A die Menge aller Schüler einer Schule und

$$R := \{(a, b) \in A \times A \ : \ a \text{ ist in derselben Schulklasse wie } b\} .$$

Es sei nun Alice eine Schülerin der Schulklasse "6c". Alle Mitschüler aus der Schulklasse von Alice bilden die Äquivalenzklasse von Alice:

$$\begin{aligned} [\text{Alice}]_R &= \{b \in A \ : \ (\text{Alice}, b) \in R\} \\ &= \{b \in A \ : \ b \text{ ist in derselben Schulklasse wie Alice } \} = \{ \text{ Alle Schüler der 6c } \} \end{aligned}$$

Jeder Schüler und jede Schülerin aus der 6c ist nun ein *Vertreter* seiner (Schul-)Klasse, denn anhand des

einzelnen Schülers kann man natürlich die ganze Klasse ermitteln:

Ist Bob auch in der 6c, d.h. Alice und Bob sind in derselben (Schul-)Klasse “6c”, so gilt $[\text{Alice}]_R = [\text{Bob}]_R$:

$$[\text{Bob}]_R \quad = \quad \{ \text{ Alle Schüler in der Schulklasse von Bob } \} \quad = \quad \{ \text{ Alle Schüler der 6c } \}$$

Beispiel 1.4.19.

Es sei $R := \{(n, m) \in \mathbb{N} \times \mathbb{N} \ : \ m \text{ hat denselben Rest beim Teilen durch 2 wie } n\}$.

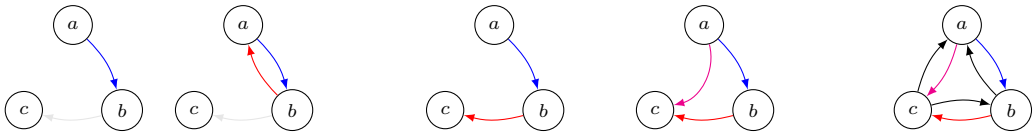
Die beiden Äquivalenzklassen von R sind:

$$\begin{array}{lll} M_g & := & \{2n \quad : \ n \in \mathbb{N}\} \quad \text{(alle graden Zahlen)} \qquad \text{und} \\ M_u & := & \{2n+1 \quad : \ n \in \mathbb{N}\} \quad \text{(alle ungraden Zahlen)} \end{array}$$

Ein Vertreter von M_g ist $x = 6 \in M_g$, und es gilt tatsächlich $[6]_R = M_g$ (s. Beispiel 1.4.15).

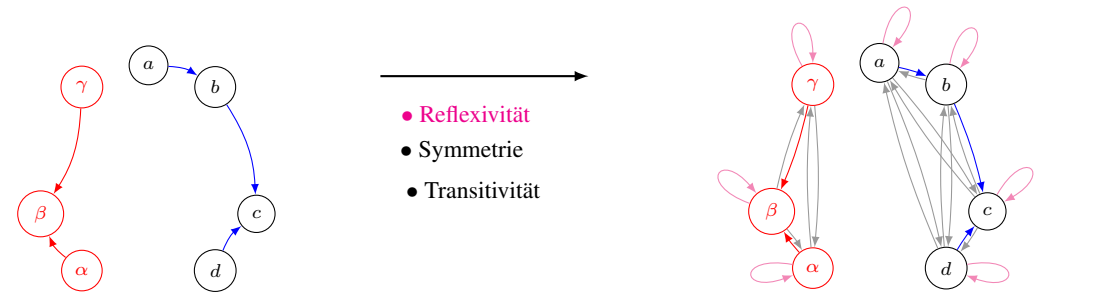
1.4.2. Äquivalenzklassen: Veranschaulichung als Graph

Die Einsichten aus Lemma 1.4.16 lassen sich leichter anhand von Graphen veranschaulichen bzw. verstehen. Ist R eine Äquivalenzrealtion so „erzeugen“ die Regeln der Symmetrie und Transitivität Bögen im zugehörigen gerichteten Graphen der Relation:



Symmetrie | Transitivität | Transitivität & Symmetrie

Aus der Skizze entnimmt man: Ist G der gerichtete Graph einer Äquivalenzrelation und sind zwei Knoten v und w *irgendwie* über einen Weg aus Bögen (und Gegenbögen) verbunden, so sind v und w in$R$ auch direkt verbunden. Dies liefert:



Bekannte Paare einer Relation

Kleinste mögliche Relation mit allen vorgegebenen Paaren.

Abbildung 1.1.: Kleinstmögliche Äquivalenzrelation mit einigen bekannte Tupeln.

Der gerichtetete Graph G einer Äquivalenzrelation zerfällt in disjunkte *Cliquen* G_i':

- Jeder dieser Untergraphen G'_i ist eine Clique (bzw. vollständig), d.h. jeder mögliche Bogen der Form (a, b) mit Knoten von G'_i ist Teil des Graphen.
- Je zwei verschiedene Untergraphen G'_i und G'_j sind disjunkt: D.h. es gibt keine Bögen von G_i nach G_j (und umgekehrt).

Jede dieser Cliquen ist eine Äquivalenzklasse der Äquivalenzrelation R. Im Falle der Relation $R = \{(a, b) \quad : b$ spielt im selben Verein wie $a\}$ sind dies grade die möglichen Vereine.

2 Rechnen mit ganzen Zahlen

2.1. Teilbarkeit

Aus der Schule bekannt ist der Begriff der Teilbarkeit für natürliche Zahlen. Zum Beispiel teilt die Zahl 3 die Zahl 15, jedoch teilt die 4 nicht die Zahl 15. Diesen Begriff müssen wir auf die ganzen Zahlen $\mathbb{Z}$ ausweiten. Kurz gesagt ist die Teilbarkeit in $\mathbb{Z}$ identisch zu der in $\mathbb{N}$, man "ignoriert" beim Prüfen von Teilbarkeit etwaige Vorzeichen.

Definition 2.1.1 (Teilbarkeit)**.**

Eine Zahl $a \in \mathbb{Z}$ ***teilt*** eine Zahl $b \in \mathbb{Z}$, falls es ein $k \in \mathbb{Z}$ gibt mit $b = k \cdot a$.

In Kurzschreibweise:

$$a|b \quad :\Leftrightarrow \quad [\ \exists k \in \mathbb{Z}\ :\ b = k \cdot a\ ]$$

Im Fall $a|b$ nennt man a einen ***Teiler*** von b und man sagt b ist ein ***Vielfaches*** von a.

Gilt zusätzlich $1 < a < |b|$ d.h. $a \neq 1$ und $a \neq \pm b$ so nennt man a einen ***echten Teiler*** von b.

Analog führt man diese Kurzschreibweise ein:

$$a \nmid b \quad :\Leftrightarrow \quad [\ \nexists k \in \mathbb{Z}\ :\ b = k \cdot a\ ]$$

Beispiel 2.1.2.

Es gelten:

$$\begin{aligned}
3|\ 12 \quad &\text{wegen} \quad 12 = 4 \cdot 3 \\
-3|\ 12 \quad &\text{wegen} \quad 12 = (-4) \cdot (-3) \\
3|-12 \quad &\text{wegen} \quad -12 = (-4) \cdot 3 \\
-3|-12 \quad &\text{wegen} \quad -12 = 4 \cdot (-3)
\end{aligned}$$

Bemerkung 2.1.3 (Teilbarkeit und die Null)**.**

Jede Zahl teilt die Null
Die Null ist Vielfaches von jeder anderen Zahl $a \in \mathbb{Z}$ denn es ist $0 = k \cdot a$ mit $k = 0$.

Es gelten also

$$1|0 \text{ wegen } 0 = 0 \cdot 1 \quad \text{und} \quad 2|0 \text{ wegen } 0 = 0 \cdot 2 \quad \text{und} \quad 3|0 \text{ wegen } 0 = 0 \cdot 3$$

Die Null teilt keine andere Zahl
Die Null teilt **keine** anderen Zahl $m \in \mathbb{Z} \setminus \{0\}$, denn $m \neq 0$ ist kein Vielfaches von Null.

Es gilt also:

$$0 \nmid 1 \text{ wegen } \nexists k \in \mathbb{Z} \,:\, 1 = k \cdot 0$$

2.2. Primzahlen

Mit Hilfe des Konzepts der Teilbarkeit kann eine wesentliche Klasse von natürlichen Zahlen, die Primzahlen, definiert werden.

Definition 2.2.1 (Primzahlen)**.**

Eine Zahl $n \in \mathbb{N}$ heißt ***Primzahl***, falls n genau 2 Teiler in $\mathbb{N}$ hat.

Beispiel 2.2.2.

Die ersten Primzahlen bis 100:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97$$

Bemerkung 2.2.3 (Die Zahl 1 ist keine Primzahl)**.**

Die 1 ist keine Primzahl, denn Sie hat genau einen Teiler in $\mathbb{N}$. Dass die Zahl 1 keine Primzahl ist, ist bei der Primzahldefinition bewußt so gehalten, damit die Primzahlzerlegung von Zahlen in den natürlichen Zahlen $\mathbb{N}$ eindeutig ist.

Bemerkung 2.2.3 motiviert den folgenden Satz, welcher die Eindeutigkeit der Primzahlzerlegung feststellt. Man findet ihn in Gauß' berühmter "Disquisitiones Arithmeticae" aus dem Jahre 1801.

Satz 2.2.4 (Fundamentalsatz der Arithmetik)**.**

Jede natürliche Zahl $n \in \mathbb{N}$ mit $n \geq 2$ besitzt eine *eindeutige* Darstellung als Produkt von Primzahlen

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} \qquad \text{(Primzahlzerlegung von } n\text{)}.$$

Dabei sind

- $m \in \mathbb{N}$,
- die Primzahlen aufsteigend sortiert, also $p_1 < \cdots < p_m$ und
- die Exponenten $k_1, \ldots, k_m \in \mathbb{N}$.

Beweis. Zum Nachweis der **Existenz** verwenden wir eine Induktion über n.

Induktionsverankerung: Für $n = 2$ ist die Aussage klar, die Primzahlzerlegung von 2 lautet $2 = 2^1$.

Induktionsannahme: Es existiere für alle Zahlen $1, \dots, n-1$ eine eindeutig Primzahlzerlegung in der gewünschten Form.

Induktionsschluss: Sei nun $n \in \mathbb{N}$ mit $n > 2$.

- Ist n eine Primzahl, so ist die Primzahlzerlegung $n = (p_1)^1$ mit $p_1 := n$.
- Ist n keine Primzahl, so gibt es einen echten Teiler k von n mit $2 \leq k \leq n-1$. Wendet man nun die Induktionsvoraussetzungen auf k und $2 \leq n/k \leq n-1$ an, so erhält man Primzahlzerlegungen von k und n/k und damit eine Zerlegung von $n = n/k \cdot k$.

Der Beweis der **Eindeutigkeit** der Zerlegung benötigt ein Hilfslemma:

Teilt eine Primzahl p das Produkt $a \cdot b$ zweier Zahlen $a, b \in \mathbb{N}$, so teilt p auch mindestens einen der Faktoren a oder b. (Beweis: Siehe Lemma **??**)

Wir nehmen an, dass es eine kleinste natürliche Zahl n mit zwei verschiedenen Primfaktorzerlegungen gibt. Es gelte also

$$n = (p_1)^{k_1} \cdots (p_m)^{k_m} = (q_1)^{\ell_1} \cdots (q_{\widetilde{m}})^{\ell_{\widetilde{m}}} \qquad (\star)$$

mit jeweils aufsteigend sortierten Primzahlen $p_1, \dots p_m$ und $q_1, \dots q_{\widetilde{m}}$.

Nach Korrolar **??** teilt jede Primzahl p_i als Teiler von n einen der Faktoren q_j, ist also identisch zu q_j. Analog ist jede Primzahl q_j identisch zu einer der Primzahlen p_i. Also müssen die beiden Primzahl-Mengen identisch sein, es gilt:

$$\{p_i \ : \ 1 \leq i \leq m\} \qquad = \qquad \{q_j \ : \ 1 \leq j \leq \widetilde{m}\}$$

Da die Zahlen p_i und die Zahlen q_j der Größe nach sortiert sind, erhalten wir $m = \widetilde{m}$ und $p_i = q_i$ für alle $1 \leq i \leq m$. Teilt man nun in $(\star)$ auf beiden Seiten durch p_1, erhält man eine kleinere Zahl $\widetilde{n} := n/p_1$ mit zwei verschiedenen Primfaktorzerlegungen. Genauer gilt:

$$\begin{aligned}
(\star) \Leftrightarrow \quad & (p_1)^{k_1} \cdot (p_2)^{k_2} \cdots (p_m)^{k_m} = (p_1)^{\ell_1} \cdot (p_2)^{\ell_2} \cdots (p_m)^{\ell_m} && \mid : p_1 \\
\Leftrightarrow \quad & \underbrace{(p_1)^{k_1-1} \cdot (p_2)^{k_2} \cdots (p_m)^{k_m}}_{=\widetilde{n}} = (p_1)^{\ell_1-1} \cdot (p_2)^{\ell_2} \cdots (p_m)^{\ell_m} && (\star\star)
\end{aligned}$$

Nach Annahme sind die Zerlegungen in $(\star)$ verschieden, die verwendeten Primzahlen jedoch identisch - es existiert also mindestens ein j mit $k_j \neq \ell_j$. Damit sind die Zerlegungen in $(\star\star)$ ebenfalls unterschiedlich.

Wir erhalten also für die natürliche(!) Zahl $\widetilde{n} := n/p_1$ zwei verschiedene Primzahlzerlegungen und wegen $p_1 > 1$ gilt $\widetilde{n} < n$. Dies ist ein Widerspruch zur Annahme dass n die kleinste solche Zahl ist. □

Beispiel 2.2.5.

Die Primzahlzerlegung für 450 ist $450 = 2 \cdot 3^2 \cdot 5^2$.

2.3. Modulo-Rechnung

In den folgenden Abschnitte werden wir beim Arbeiten mit mathematischen Gruppen das Rechnen mit sogenannten Resten betrachten. Wir beginnen mit der mathematischen sauberen Definition von Resten.

2.3.1. Reste

Definition 2.3.1 (Rest - *Patenschaft: Ina Meyer*)**.**

Es seinen $a, b \in \mathbb{Z} \setminus \{0\}$. Mit $\mathsf{Rest}(a, b)$ bezeichenen wir den ***Rest***, der beim Teilen von a durch b entsteht:

$$\mathsf{Rest}(a, b) := \min\{r \in \mathbb{N} \ : \ \exists m \in \mathbb{Z} \text{ mit } \ a = m \cdot b + r\}.$$

Bemerkung 2.3.2.

Der Rest ist nicht negativ und stets kleiner als der Modul (also $0 \leq \mathsf{Rest}(a, b) < b$).

- Die Aussage $r \geq 0$ folgt direkt aus $r \in \mathbb{N}$.
- Die Aussage $r < b$ folgt aus der "Minimalitäts-Eigenschaft" von r: Wenn $a = k \cdot b + R$ gilt, mit $R \geq b$, so kann man a darstellen als $a = (k + 1) \cdot b + (R - b)$, wobei $0 \leq R - b < R$ gilt, d.h. R ist nicht die kleinste Zahl der Form $r = a - m \cdot b$.

Der Rest $\mathsf{Rest}(a, b)$ lässt sich für $a, b \in \mathbb{N}$ leicht berechnen. Es gilt:

$$\mathsf{Rest}(a, b) = a - m \cdot b \qquad \text{mit} \qquad m := \lfloor \frac{a}{b} \rfloor$$

Beispiel 2.3.3.

Es gilt $\mathsf{Rest}(\ \ 20, 7) = 6$ wegen $20 = \ \ 2 \cdot 7 + 6$.

Es gilt $\mathsf{Rest}(-20, 7) = 1$ wegen $-20 = -3 \cdot 7 + 1$.

Beim Rechnen mit Resten können Teilreste gebildet werden, es gelten die folgenden Rechenregeln:

Lemma 2.3.4 (Rechenregeln für Reste)**.**

Es seien $a, b, n \in \mathbb{Z}$ und $k \in \mathbb{N}$.

i) $\mathsf{Rest}(a + b \ \ , n) = \mathsf{Rest}\big(a + \mathsf{Rest}(b, n) \ \ , n\big)$

ii) $\mathsf{Rest}(a \cdot \ b \ \ , n) = \mathsf{Rest}\big(a \cdot \ \mathsf{Rest}(b, n) \ \ , n\big)$

iii) $\mathsf{Rest}(\ \ b^k \ \ , n) = \mathsf{Rest}\big(\ \ \mathsf{Rest}(b, n)^k \ \ , n\big)$

Beweis. Wir führen exemplarisch den Beweis für Fall ii):

Sei $r := \mathsf{Rest}(b, n)$, d.h. es gibt m mit $b = m \cdot n + r$. Dann gilt:

$$a \cdot b = a \cdot (m \cdot n + r) = \underbrace{a \cdot m \cdot n}_{\text{fällt weg beim Teilen durch } n} + a \cdot r \quad \Rightarrow \quad \mathsf{Rest}(a \cdot b, n) = \mathsf{Rest}(a \cdot r, n)$$

□

Beispiel 2.3.5.

Es soll $\mathsf{Rest}(18 \cdot 2^{12}, 7)$ berechnet werden. Dies erreicht man am Einfachsten durch Bilden von Teilresten:

$$\mathsf{Rest}\left(18 \cdot 2^{12}, 7\right) \overset{\text{ii)}}{=} \mathsf{Rest}\left(4 \cdot 2^{12}, 7\right) = \mathsf{Rest}(4 \cdot (2^3)^4, 7) \overset{\text{iii)}}{=} \mathsf{Rest}(4 \cdot (1)^4, 7) = 4$$

$\mathsf{Rest}(18,7)=4$ $\qquad$ $\mathsf{Rest}(2^3,7)=1$

2.3.2. Von Resten und Modulo-Rechnung

Für eine gegebene Zahl m lässt sich mit den Resten, welche beim Teilen durch m entstehen, rechnen. Die Notation dafür kann mittels Resten erfolgen oder aber per Modulo-Rechnung, wie wir sie nun definieren.

Definition 2.3.6 (Äquivalenz Modulo m - *Patenschaft: Ansgar Asseburg*)**.**

Es sei $m \in \mathbb{N} \setminus \{1\}$, dann gilt für $a, b \in \mathbb{Z}$

$$a \equiv b \pmod{m} \quad :\Leftrightarrow \mathsf{Rest}(a, m) = \mathsf{Rest}(b, m)$$

Man sagt in diesem Fall „a und b sind äquivalent *mod* m“.

Die Zahl m bezeichnet man dabei als ***(den) Modul*** der *Modul-Gleichung* $a \equiv b \pmod{m}$.

Bemerkung 2.3.7.

Die Zahlen b in $a \equiv b \pmod{m}$ muss nicht kleiner als der Modul m sein.

Typischerweise nimmt man zunächst an, dass auf der rechten Seite einer Modul-Gleichung stets der Rest bzgl. Teilen durch m stehen muss (oder dass die rechte Seite zumindest kleiner sein muss als die linke). Richtig ist, dass auf der rechten Seite der Rest stehen *kann*.

$$5 \equiv 25 \pmod{10} \qquad \text{ist richtig}$$

Beispiel 2.3.8.

Für den Modul $m = 7$ gelten beispielsweise:

$$8 \equiv 1 \pmod{7} \qquad 14 \equiv 21 \pmod{7}$$

$$1 \equiv 8 \pmod{7} \qquad 14 \equiv 0 \pmod{7}$$

Lemma 2.3.9.

Für jedes $m \in \mathbb{N} \setminus \{1\}$ ist $\mathcal{R}_m := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \ : \ a \equiv b \pmod{m}\}$ eine Äquivalenzrelation.

Beweis. Der Beweis wird dem Leser überlassen. □

Als Äquivalenzrelation ist $\equiv$ reflexiv, symmetrisch und transitiv:

Korollar 2.3.10.

Es sei $m \in \mathbb{N} \setminus \{0, 1\}$ ein fester Modul, und es gelte

$$a \equiv b \pmod{m} \quad \text{und} \quad b \equiv c \pmod{m}$$

Dann gilt:

$$\underbrace{b \equiv a \pmod{m}}_{\text{Symmetrie}} \quad \text{und} \quad \underbrace{a \equiv c \pmod{m}}_{\text{Transitivität}}$$

Beweis. Der Beweis folgt direkt aus Lemma 2.3.10 und der Definition von Äquivalenzrelationen. □

Lemma 2.3.11.

Es sei $m \in \mathbb{N} \setminus \{1\}$, dann sind für $a, b \in \mathbb{Z}$ die folgenden Formulierungen äquivalent:

- Die Zahl m teilt $(a - b)$.
- Es gibt $k \in \mathbb{Z}$ mit $a = b + k \cdot m$.
- $\mathsf{Rest}(a, m) = \mathsf{Rest}(b, m)$.

Beweis. (Beweisidee) Für ein Paar $(a, b) \in \mathcal{R}_m$ gilt $m|(a - b)$ bzw. $a - b = k \cdot m$ mit $k \in \mathbb{Z}$. Mit anderen Worten: a und b unterscheiden sich um ein Vielfaches von m, bzw. $a = k \cdot m + b$.

Dies wiederum bedeutet, dass a und b den selben Rest beim Teilen durch m haben. Es gilt also:

$$\mathsf{Rest}(a, m) = \mathsf{Rest}(b + k \cdot m, m) = \mathsf{Rest}(b, m).$$

□

Lemma 2.3.12.

Es sei $m \in \mathbb{N} \setminus \{1\}$ ein fester Modul, und es gelte für $a, \widetilde{a}, c, \widetilde{c} \in \mathbb{Z}$:

$$a \equiv \widetilde{a} \pmod{m} \qquad \text{und} \qquad c \equiv \widetilde{c} \pmod{m}$$

Dann gelten auch:

$$\begin{aligned}
&\text{i)} && a + c &&\equiv \widetilde{a} + c && \pmod{m} \\
& && && \equiv \widetilde{a} + \widetilde{c} && \pmod{m} \\
&\text{ii)} && a \cdot c &&\equiv \widetilde{a} \cdot c && \pmod{m} \\
& && && \equiv \widetilde{a} \cdot \widetilde{c} && \pmod{m} \\
&\text{iii)} && a^k &&\equiv (\widetilde{a})^k && \pmod{m} \qquad \text{für } k \in \mathbb{N}
\end{aligned}$$

Beweis. Es gelte $a \equiv \widetilde{a} \pmod{m}$ und $c \equiv \widetilde{c} \pmod{m}$, d.h. $\widetilde{a} - a$ und $\widetilde{c} - c$ sind Vielfache von m.

Es gibt also $k, \ell \in \mathbb{Z}$ mit $\widetilde{a} = a + k \cdot m$ und $\widetilde{c} = c + \ell \cdot m$.

i) Für die Summe gilt:

$$\widetilde{a} + \widetilde{c} = (a + k \cdot m) + (c + \ell \cdot m) = a + c + \underbrace{k \cdot m + \ell \cdot m}_{\text{Vielfaches von } m}$$

Es folgt also $(\widetilde{a} + \widetilde{c}) \; - \; (a \cdot c)$ ist Vielfaches von m, bzw. $\widetilde{a} + \widetilde{c} \equiv a + c \pmod{m}$.

ii) Für das Produkt gilt:

$$\widetilde{a} \cdot \widetilde{c} = (a + k \cdot m) \cdot (c + \ell \cdot m) = a \cdot c + \underbrace{a \cdot \ell \cdot m + c \cdot k \cdot m + k \cdot \ell \cdot m^2}_{\text{Vielfaches von } m}$$

Es folgt also $\widetilde{a} \cdot \widetilde{c} - a \cdot c$ ist Vielfaches von m, bzw. $\widetilde{a} \cdot \widetilde{c} \equiv a \cdot c \pmod{m}$.

Die Aussagen über $\widetilde{a} + c$ und $\widetilde{a} \cdot c$ in den ersten Zeile von i) und ii) beweist man jeweils analog.

iii) Für a^k wendet man die Rechenregel aus ii) iterativ an. Es gilt

$$\begin{aligned} a^k \;=\; a \cdot (a^{k-1}) &\equiv \widetilde{a} \cdot (a^{k-1}) && \pmod{m} \\ &\equiv \widetilde{a} \cdot (a \cdot a^{k-2}) && \pmod{m} \\ &\equiv (\widetilde{a})^2 \cdot (a^{k-2}) && \pmod{m} \\ &\;\;\vdots \\ &\equiv (\widetilde{a})^k && \pmod{m}. \end{aligned}$$

□

Bemerkung 2.3.13.

Verwendet man Lemma 2.3.12 zusammen mit $a \equiv \mathsf{Rest}(a, m) \pmod{m}$ so zeigt sich: In Modul-Gleichungen kann man rechnen, in dem man Teilreste berechnet! So gelten beispielsweise:

$$\begin{aligned} a + b &\equiv \mathsf{Rest}(a, \mathbf{m}) + b && \pmod{\mathbf{m}} \\ a \cdot b &\equiv \mathsf{Rest}(a, \mathbf{m}) \cdot b && \pmod{\mathbf{m}} \\ a^{1000} &\equiv \mathsf{Rest}(a, \mathbf{m})^{1000} && \pmod{\mathbf{m}}. \end{aligned}$$

Beispiel 2.3.14.

Welchen Rest hat 29^{100} beim Teilen durch 7?

Diese Frage übersetzt sich in: Finde die kleinste, nicht negative Zahl x mit $x \equiv 29^{100} \pmod{7}$. Es gilt:

$$\begin{aligned} 29^{100} &\equiv \mathsf{Rest}(29, 7)^{100} && \pmod{7} \\ &\equiv \underbrace{1^{100}}_{} && \pmod{7} \\ &\equiv 1 && \pmod{7} \end{aligned}$$

2.3.3. Äquivalenzklassen der Äquivalenzrelation $\mathcal{R}_m$

Die Äquivalenzrelation $\mathcal{R}_m$ liefert Äquivalenzklassen.

Zwei Zahlen $a, b \in \mathbb{Z}$ sind hier äquivalent, wenn sie sich nur um ein Vielfaches von m unterscheiden, es gilt $b = a + k \cdot m$ mit $k \in \mathbb{Z}$. Die Äquivalenzklasse zu a sind also alle Zahlen b, die sich auf der Zahlengeraden von a aus in Schritten der Weite m erreichen lassen.

Lemma 2.3.15.

Für $m \in \mathbb{N} \setminus \{1\}$ sind die Äquivalenzklassen von $\mathcal{R}_m$ gerade die Mengen

$$\begin{array}{lcll} [0]_{\mathcal{R}_m} & = & \{k \cdot m & : \ k \in \mathbb{Z}\} \\ [1]_{\mathcal{R}_m} & = & \{k \cdot m + 1 & : \ k \in \mathbb{Z}\} \\ [2]_{\mathcal{R}_m} & = & \{k \cdot m + 2 & : \ k \in \mathbb{Z}\} \\ & \vdots & & \\ [m-1]_{\mathcal{R}_m} & = & \{k \cdot m + m - 1 & : \ k \in \mathbb{Z}\} \end{array}$$

Beweis. Der Beweis wird dem Leser überlassen. □

Beispiel 2.3.16.

Es sei $\mathcal{R}_3$ die Äquivalenzrelation auf $\mathbb{Z}$ mit $(m, n) \in \mathcal{R}_3$ g.d.w. $\mathsf{Rest}(m, 3) = \mathsf{Rest}(n, 3)$. Dann gibt es genau drei Äquivalenzklassen:

$$\begin{array}{lcll} [0]_{\mathcal{R}_3} & = & \{3 \cdot k & : \ k \in \mathbb{Z}\} \\ [1]_{\mathcal{R}_3} & = & \{3 \cdot k + 1 & : \ k \in \mathbb{Z}\} \\ [2]_{\mathcal{R}_3} & = & \{3 \cdot k + 2 & : \ k \in \mathbb{Z}\} \end{array}$$

Diese Äquivalenzklassen werden von den möglichen Resten beim Teilen durch 3 erzeugt.

Für $m = 7$ ist die Äquivalenzklasse $[7]_{\mathcal{R}_3}$ beispielsweise identisch mit $[1]_{\mathcal{R}_3}$:

Es gilt $7 \equiv 1 \pmod 3$ (wegen $\mathsf{Rest}(7, 3) = 1 = \mathsf{Rest}(1, 3)$)und nach Lemma 1.4.16 gilt dann $[7]_{\mathcal{R}_3} = [1]_{\mathcal{R}_3}$.

2.4. Der Euklidische Algorithmus

Der Euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers (ggT) gehört zu den ältesten bekannten Rechenverfahren. Er war schon Eudoxus (375 v. Chr.) bekannt und ist im Band 7 “der Elemente” von Euklid (300 v. Chr.) beschrieben. Er ist in der diskreten Zahlentheorie von zentraler Bedeutung und kommt in vielen Rechenprozeduren zur Anwendung.

2.4.1. Der ggT

Beim Arbeiten mit Rest-Klassen-Gruppen spielt der größte gemeinsame Teiler zweier Zahlen eine zentrale Rolle.

Definition 2.4.1 (Der ggT - *Patenschaft: Nicolaj Freyer*)**.**

Der ***größte gemeinsame Teiler*** $\mathrm{ggT}(a,b)$ zweier von Null verschiedener ganzer Zahlen $a,b \in \mathbb{Z}$ ist die größte natürliche Zahl, die sowohl a als auch b teilt. Es ist also

$$\mathrm{ggT}(a,b) := \max\{n \in \mathbb{N} \ : \ n|a \text{ und } n|b\}.$$

Bemerkung 2.4.2. Was ist $\mathrm{ggT}(a,0)$ und $\mathrm{ggT}(0,a)$?

Es gilt nach 2.1.3 für jedes $n \in \mathbb{N}$ stets, dass n die 0 teilt und damit folgt $|a| = \max\{n \in \mathbb{N} \ : \ n|a \ \text{ und } \ n|0\}$. Also ist $\mathrm{ggT}(a,0) = \mathrm{ggT}(0,a) = |a|$.

Dass $\mathrm{ggT}(a,0) = |a|$ gilt, wird im Übrigen später die Notation rund um den Euklidischen Algorithmus erleichtern.

Definition 2.4.3 (Teilerfremdheit)**.**

Zwei Zahlen $a,b \in \mathbb{Z}$ heißen ***teilerfremd***, wenn $\mathrm{ggT}(a,b) = 1$ gilt.

Man sagt auch „a und b sind relativ prim“.

Für den ggT gilt die folgende (auf den ersten Blick überraschende) Inklusion.

Lemma 2.4.4.

Es seien $a,b,n \in \mathbb{N}$ dann gilt: $\mathrm{ggT}(a \cdot b, n)$ teilt $\mathrm{ggT}(a,n) \cdot \mathrm{ggT}(b,n)$

Beweis. Der Beweis ist eine Übungsaufgabe. □

2.4.2. Naive Berechnung des ggT für kleine Zahlen

Eine Möglichkeit zur Berechnung des ggT besteht darin, a und b in Primfaktoren zu zerlegen. Seien etwa $a,b \in \mathbb{N}$ und seien $p_1,\ldots,p_\ell \in \mathbb{N}$ die Primzahlen, die in a oder b als Teiler enthalten sind. Dann gibt es Exponenten $m_1,\ldots,m_\ell \in \mathbb{N}$, und $n_1,\ldots,n_n \in \mathbb{N}$, so dass gilt:

$$\begin{aligned} a &= p_1^{m_1} \cdot p_2^{m_2} \cdots p_\ell^{m_\ell} \\ b &= p_1^{n_1} \cdot p_2^{n_2} \cdots p_\ell^{n_\ell} \end{aligned}$$

Bemerkung 2.4.5.

Die Exponenten $m_i, n_i \in \mathbb{N}$ können hier teilweise den Wert 0 haben, so dass z.B. bei $m_i = 0$ der Faktor $p_i^{m_i} = 1$ anzeigt, dass p_i in der Primzahlzerlegung von a nicht vorkommt.

Mit dieser Darstellung von a und b ist dann der ggT wie folgt zu berechnen:

$$\mathrm{ggT}(a,b) \quad = \quad p_1^{k_1} \cdot p_2^{k_2} \cdots p_\ell^{k_\ell} \qquad \text{wobei} \qquad k_i := \min\{m_i, n_i\}.$$

Beispiel 2.4.6.

Gegeben seien die Zahlen 900 und 500. Dann gilt: $900 = 2^2 \cdot 3^2 \cdot 5^2$ und $500 = 2^2 \cdot 5^3$. Die vorkommenden Primzahlen sind also $p_1 := 2$, $p_2 := 3$ und $p_3 := 5$. Für diese gilt dann:

$$\begin{aligned} 900 &= 2^2 \cdot 3^2 \cdot 5^2 \\ 500 &= 2^2 \cdot 3^0 \cdot 5^3 \\ \mathrm{ggT}(900,500) &= 2^2 \cdot 3^0 \cdot 5^2 \qquad = 4 \cdot 25 = 100 \end{aligned}$$

$$\begin{aligned} k_1 &= \min\{2,2\} &&= 2 \\ k_2 &= \min\{2,0\} &&= 0 \\ k_3 &= \min\{2,3\} &&= 2 \end{aligned}$$

Um dieses Verfahren anzuwenden, muss man zunächst die Zahlen $a, b \in \mathbb{N}$ in ein Produkt von Primzahlen zerlegen. Dies ist zwar theoretisch möglich, allerdings gibt es für diese Aufgabe bisher keinen effizienten Algorithmus, d.h. für sehr große Zahlen ist dieses Verfahren nicht umsetzbar: Die bisher bekannten Algorithmen zur Primzahlzerlegung (z.B. das Sieb des Eratosthenes) benötigen bei sehr großen Zahlen mehr Rechenzeit, als das Universum alt ist.

2.4.3. Der Euklidische Algorithmus - Vorüberlegung

Der Euklidische Algorithmus beruht auf der Division mit Rest: Zu natürlichen Zahlen $a, b \neq 0$ mit $a \geq b$ gibt es Zahlen $m, r \in \mathbb{N}$ mit

$$a = m \cdot b + r \qquad \text{und} \qquad 0 \leq r < b.$$

Die Zahlen m (der Faktor) und $r := \mathsf{Rest}(a,b)$ (der Rest) lassen sich durch Division mit Rest bestimmen, es gilt für $a = 20$ und $b = 6$ zum Beispiel $a = 3 \cdot b + 2$ also $m = 3$ und $r = 2$.

Hilfreich ist nun, dass $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$ sowie $r < b \leq a$ gelten. Man kann also die Berechnung von $\mathrm{ggT}(a,b)$ auf das Berechnen von $\mathrm{ggT}(b,r)$ zurückführen - eine Aufgabe mit kleineren Input-Zahlen!

Dies kann man nun so lange rekursiv wiederholen, bis eine der beiden Zahlen den Wert Null annimt, dann ist der ggT (nach Definition des ggT) leicht auszurechnen:

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r) = \ldots = \mathrm{ggT}(c,0) = c.$$

Lemma 2.4.7.

Es seien $a, b \in \mathbb{N}$ und $a \geq b > 0$ mit $r := \mathsf{Rest}(a,b)$. Dann gilt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(a-b,b) = \mathrm{ggT}(r,b).$$

Beweis. Es seien $a, b \in \mathbb{N}$ mit $a \geq b > 0$.

Wir zeigen $\mathrm{ggT}(a,b) = \mathrm{ggT}(a-b,b)$ und benutzen dies iterativ für den Beweis der zweiten Gleichung.

Für $c \in \mathbb{N} \setminus \{0\}$ gilt: $c|a \ \wedge \ c|b \quad \Leftrightarrow \quad c|(a-b) \ \wedge \ c|b$. Dies beweisen wir wie folgt:

$$\begin{array}{lllllll} c|a \ \wedge \ c|b & \Leftrightarrow & \exists k,\ell \in \mathbb{Z} : & b = c\cdot\ell & \wedge & a = & c\cdot k \\ & \Leftrightarrow & \exists k,\ell \in \mathbb{Z} : & b = c\cdot\ell & \wedge & a-b = & c\cdot(k-\ell) \quad (\star) \\ & \Leftrightarrow & \exists k,n \in \mathbb{Z} : & b = c\cdot\ell & \wedge & a-b = & c\cdot(n) \quad (\star\star) \\ & \Leftrightarrow & & c|b & \wedge & c|(a-b) & \end{array}$$

Um $(\star) \Rightarrow (\star\star)$ zu zeigen, wählt man $n = k - \ell$, um $(\star\star) \Rightarrow (\star)$ zu zeigen, wählt man $k = n + \ell$.

Es gilt also $\mathrm{ggT}(a,b) = \mathrm{ggT}(a-b,b)$ denn:

$$\begin{array}{lrcl} & \big(c|a \ \wedge \ c|b & \Leftrightarrow & c|(a-b) \ \wedge \ c|b\big) \\ \Rightarrow & \{c \in \mathbb{N} : c|a \ \wedge \ c|b \ \} & = & \{c \in \mathbb{N} : c|(a-b) \ \wedge \ c|b \ \} \\ \Rightarrow & \underbrace{\max\{c \in \mathbb{N} : c|a \ \wedge \ c|b \ \}}_{\mathrm{ggT}(a,b)} & = & \underbrace{\max\{c \in \mathbb{N} : c|(a-b) \ \wedge \ c|b \ \}}_{\mathrm{ggT}(a-b,b)} \end{array}$$

Es sei $r := \mathsf{Rest}(a,b)$ also $r = a - m\cdot b$ mit $m := \lfloor \frac{a}{b} \rfloor$. Dann gilt: $r = a - m \cdot b$

Zieht man nun sukzessive b von a ab, so erhält man $a-b,\ a-2b,\ a-3b$,..., $a-mb$. Aus dem ersten Teil des Beweises folgern wir, dass für diese Differenzen gilt:

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(a-b,b) = \mathrm{ggT}(a-2b,b) = \cdots = \mathrm{ggT}(a-mb,b).$$

□

Beispiel 2.4.8.

Es sei $a := 77$ und $b := 21$ mit $\mathrm{ggT}(77,21) = 7$.

Dann ist $14 = \mathsf{Rest}(77,21)$ wegen $77 = \underbrace{3\cdot 21}_{=63} + 14$

Es gilt $\mathrm{ggT}(77,21) = \mathrm{ggT}(21,14) = 7$.

2.4.4. Euklidischer Algorithmus (kompakte Notation)

Wir sind nun in der Lage die algorithmische Herangehensweise des euklidischen Algorithmus zu lesen und zu beweisen, dass der euklidische Algorithmus nach endlich vielen Schritten terminiert und die Ausgabe der korrekte ggT der Input-Zahlen ist.

Algorithmus 2.4.9 (Euklidischer Algorithmus)**.**

Input: $a, b \in \mathbb{N}$.
Output: $d = \mathrm{ggT}(a,b)$.
if $a < b$ **then**

Vertausche a und b.
end if
while $b > 0$ **do**
Setze $m := \lfloor \frac{a}{b} \rfloor$.
Setze $r := a - m \cdot b$.
Setze $a := b$ und $b := r$.
end while
return a.

Lemma 2.4.10.

Der Euklidische Algorithmus mit Input $a, b \in \mathbb{N}$ terminiert nach endlich vielen Schritten und liefert als Ausgabe $\mathrm{ggT}(a, b)$.

Beweis. Es seien $a, b \in \mathbb{N}$ der Input für den Euklidischen Algorithmus. Weiter seien a_k und b_k die Werte von a und b im k-ten Aufruf der *while*-Schleife.

Terminieren: In der *while*-Schleife berechnet der Algorithmus $r = \mathsf{Rest}(a_k, b_k)$ aus den aktuellen Werten für a_k und b_k. Außerdem wird (unter anderem) die Zuweisung $b_{k+1} = \mathsf{Rest}(a_k, b_k)$ ausgeführt, d.h. es gilt stets $0 \leq b_{k+1} < b_k$.

Da der Wert von b_1 endlich ist, liegen zwischen b_1 und 0 nur endlich viele mögliche b_k, d.h. der Algorithmus terminiert in endlich vielen Schritten.

Korrekter Output: Gilt $b_n = 0$ im n-ten Aufruf der *while*-Schleife, so terminiert der Algorithmus mit der Ausgabe von $a_n = \mathrm{ggT}(a_n, 0) = \mathrm{ggT}(a_n, b_n)$.

Wir zeigen nun, dass dann für alle $k \in \{1, \ldots, n\}$ gilt: $\mathrm{ggT}(a_k, b_k) = \mathrm{ggT}(a, b)$, also insbesondere $\mathrm{ggT}(a_n, b_n) = \mathrm{ggT}(a, b)$.

Induktionsverankerung: Für $k = 1$ gilt wegen $\{a_1, b_1\} = \{a, b\}$ sofort $\mathrm{ggT}(a_1, b_1) = \mathrm{ggT}(a, b)$.

Induktionsannahme: Es sei $1 \leq k < n$ und es gelte $\mathrm{ggT}(a_k, b_k) = \mathrm{ggT}(a, b)$.

Induktionsschluss: Zu zeigen: es gilt dann $\mathrm{ggT}(a_{k+1}, b_{k+1}) = \mathrm{ggT}(a, b)$.

Wie oben beschrieben, gilt im k-ten Aufruf der *while*-Schleife stets $r = \mathsf{Rest}(a_k, b_k)$. Damit gilt $a_{k+1} = b_k$ und $b_{k+1} = \mathsf{Rest}(a_k, b_k)$ im nachfolgenden $k+1$-ten Aufruf der *while*-Schleife. Es gilt also für alle k stets $\mathrm{ggT}(a_k, b_k) = \mathrm{ggT}(a_{k+1}, b_{k+1})$ nach Lemma 2.4.7. □

2.5. Der Satz von Bézout

Eine erweiterte Version des Euklidischen Algorithmus bietet die Möglichkeit zusätzlich (parallel) zum $\mathrm{ggT}(a, b)$ Zahlen $s, t \in \mathbb{Z}$ zu berechnen, für die $s \cdot a + t \cdot b = \mathrm{ggT}(a, b)$ gilt. Diese Zahlen s, t heißen ***Bézout-Multiplikatoren***. Sie werden im Folgenden eine wichtige Rolle im RSA-Verfaheren und im Chineschen Restsatz spielen.

Dazu berechnet man parallel zu allen im Euklidischen Algorithmus auftretenden Resten r stets zwei passende Zahlen s_r, t_r, so dass $r = s_r \cdot a + t_r \cdot b$ gilt. Da der Algorithmus am Schluss einen Rest $\tilde{r}$ ausgibt, hat man mit $s_{\tilde{r}}, t_{\tilde{r}}$ die gesuchten Faktoren, die $s_{\tilde{r}} \cdot a + t_{\tilde{r}} \cdot b = \tilde{r} = \mathrm{ggT}(a, b)$ liefern.

Den Anfang liefern $s_a := 1$ und $t_a := 0$, so dass $a = s_a \cdot a + t_a \cdot b$ gilt.
$s_b := 0$ und $t_b := 1$, so dass $b = s_b \cdot a + t_b \cdot b$ gilt.

Für den ersten zu berechnenden Rest $r := \mathrm{Rest}(a, b)$ gilt dann $r = a - m \cdot b$ mit geeignetem $m \in \mathbb{N}$. Aus dieser Gleichung lassen sich die Faktoren s_r, t_r berechnen:

$$\begin{array}{rcccc} a & = & s_a \cdot a & + & t_a \cdot b \\ m \cdot b & = & m \cdot s_b \cdot a & + & m \cdot t_b \cdot b \\ \hline r = \underbrace{a - m \cdot b}_{=r} & = & \underbrace{(s_a - m \cdot s_b)}_{=s_r} \cdot a & + & \underbrace{(t_a - m \cdot t_b)}_{=t_r} \cdot b \end{array}$$

(abziehen) (abziehen)

Hier sieht man, dass die Formel zur Berechnung des neuen Restes r und die Formeln zur Berechnung von s_r bzw. t_r sehr ähnlich sind: Sie lauten grob gesagt

"Neuer Wert = Vorvorgänger $-m\cdot$Vorgänger".

Dies halten wir in einer etwas umfangreicheren Version des Euklidischen Algorithmus fest. In dieser Version werden die Zwischenprodukte r, s und t mit einem Laufindex i abgespeichert. Dies dient lediglich dazu, später den Beweis der Korrektheit leichter führen zu können.

Algorithmus 2.5.1 (Erweiterter Euklidischer Algorithmus)**.**

Input: $a, b \in \mathbb{N}$ mit $a \geq b$.
Output: $r_{j-1} = \mathrm{ggT}(a, b)$ und die Gleichung $r_{j-1} = s_{j-1} \cdot a + t_{j-1} \cdot b$.
Setze $r_0 := a$ und $r_1 := b$.
Setze $s_0 := 1$ und $s_1 := 0$.
Setze $t_0 := 0$ und $t_1 := 1$.
Setze $j := 1$.
while $r_j > 0$ **do**
Setze $m_j := \lfloor \frac{r_{j-1}}{r_j} \rfloor$.
Setze $r_{j+1} := r_{j-1} - m_j r_j$.
Setze $s_{j+1} := s_{j-1} - m_j s_j$.
Setze $t_{j+1} := t_{j-1} - m_j t_j$.
Setze $j := j + 1$.
end while
return $(r_{j-1}, s_{j-1}, t_{j-1})$.

Lemma 2.5.2.

Es sei (r_n, s_n, t_n) der Output des Algorithmus 2.5.1 mit Input $a, b \in \mathbb{N}$ mit $a \geq b$. Dann gilt für die Zwischenergebnisse

$$r_i = s_i \cdot a + t_i \cdot b \qquad \text{für alle } i \in \{0, 1, \ldots, n\}.$$

Insbesondere gilt also $r_n = \mathrm{ggT}(a, b) = s_n \cdot a + t_n \cdot b$.

Beweis. Wir zeigen die Aussage $r_i = s_i \cdot a + t_i \cdot b$ für alle $i \in \{0, 1, \ldots, n\}$ per Induktion. Zum Berechnen eines jeden r_{j+1} wird sowohl den Vorgänger r_j als auch der Vorvorgänger r_{j-1} benötigt. Dies spiegelt sich in der Induktion wieder.

Induktionsverankerung: Für $k = 0$ gilt wegen $r_0 := a$, $s_0 := 1$ und $t_0 = 0$ sofort $r_0 = s_0 \cdot a + t_0 \cdot b$.

Für $k = 1$ gilt wegen $r_1 := b$, $s_1 := 0$ und $t_1 = 1$ sofort $r_1 = s_1 \cdot a + t_1 \cdot b$.

Induktionsannahme: Es sei $1 \leq k < n$, und es gelte

$r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$ sowie

$r_k = s_k \cdot a + t_k \cdot b$

Induktionsschluss: Zu zeigen ist: Es gilt $r_{k+1} = s_{k+1} \cdot a + t_{k+1} \cdot b$.

Mit dem in der *while*-Schleife berechneten m_k gilt: $r_{k+1} = r_{k-1} - m_k r_k$. Dies führt zu:

$$\begin{array}{rcccc} & r_{k-1} & \overset{\text{I.Vor.}}{=} & s_{k-1} \cdot a + t_a \cdot b & \\ \text{abziehen}\downarrow & m_k \cdot r_k & \overset{\text{I.Vor.}}{=} & m_k \cdot s_k \cdot a + m_k \cdot t_b \cdot b & \downarrow\text{abziehen} \\ \hline r_{k+1} = & r_{k-1} - m_k \cdot r_k & = & \underbrace{(s_{k-1} - m \cdot s_k)}_{=s_{k+1}} \cdot a + \underbrace{(t_{k-1} - m \cdot t_k)}_{=t_{k+1}} \cdot b & \end{array}$$

Es gilt also $r_{k+1} = s_{k+1} \cdot a + t_{k+1} \cdot b$

□

Satz 2.5.3 (Satz von Bézout)**.**

Für zwei Zahlen $a, b \in \mathbb{N}$ gibt es Zahlen $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot b = \text{ggT}(a, b)$.

Beweis. Der Beweis ist eine direkte Konsequenz von Lemma 2.5.2, man konstruiert s und t mittels Algorithmus 2.5.1. □

Beispiel 2.5.4.

Es gilt zum Beispiel für $a = 60 = 5 \cdot 12$ und $b = 25 = 5 \cdot 5$ mit $\text{ggT}(60, 25) = 5$:

$$\underbrace{(-2) \cdot 60}_{-120} + \underbrace{5 \cdot 25}_{125} = 5$$

Der Eukidischen Algorithmus in Form von Algorithmus 2.5.1 lässt sich angenehm übersichtlich in Tabellenform durchführen.

Init

Laufindex j	Faktor m_j (VorVor-r / Vor-r)	aktueller Rest r_j	Faktor vor a s_j	Faktor vor b t_j
0	/	a	1	0
1		b	0	1

Berechnen von m_1 in Zeile 1

Laufindex j	Faktor m_j (VorVor-r / Vor-r)	aktueller Rest r_j	Faktor vor a s_j	Faktor vor b t_j
0	/	a	1	0
1	$\lfloor \frac{a}{b} \rfloor$	b	0	1

Berechnen von r_2, s_2, t_2 in Zeile 2

Laufindex j	Faktor m_j (VorVor-r / Vor-r)	aktueller Rest r_j	Faktor vor a s_j	Faktor vor b t_j
0	/	a	1	0
1	$\lfloor \frac{a}{b} \rfloor$	b	0	1
2		r_2	1	$-\lfloor \frac{a}{b} \rfloor$

a	1	0
$-\lfloor \frac{a}{b} \rfloor \cdot b$	$-\lfloor \frac{a}{b} \rfloor \cdot 0$	$-\lfloor \frac{a}{b} \rfloor \cdot 1$
$= r_2$	$= 1$	$-\lfloor \frac{a}{b} \rfloor$

$r_2 = a - \lfloor \frac{a}{b} \rfloor \cdot b$

$s_2 = 1 - \lfloor \frac{a}{b} \rfloor \cdot 0 = 1$

$t_2 = 0 - \lfloor \frac{a}{b} \rfloor \cdot 1 = -\lfloor \frac{a}{b} \rfloor$

Berechnen von m_2 in Zeile 2

Laufindex j	Faktor m_j (VorVor-r / Vor-r)	aktueller Rest r_j	Faktor vor a s_j	Faktor vor b t_j
0	/	a	1	0
1	$\lfloor \frac{a}{b} \rfloor$	b	0	1
2	$\lfloor \frac{b}{r_2} \rfloor$	r_2	1	$-\lfloor \frac{a}{b} \rfloor$

...

Berechnen von m_1 in Zeile 1

Laufindex j	Faktor m_j = Vor-Vor-r / Vor-r	aktueller Rest r_j	Faktor vor a $= 84$ s_j	Faktor vor b $= 35$ t_j
0	/	84	1	0
1	2	35	0	1

$m_1 = \lfloor \frac{85}{35} \rfloor = 2$

denn $\underbrace{70}_{2\cdot 35} \leq 84 < \underbrace{105}_{3\cdot 35}$

Berechnen von r_2, s_2, t_2 in Zeile 2

j	m_j	r_j	s_j	t_j			
0	/	84	1	0	84	1	0
1	2	35	0	1	$-2 \cdot 35$	$-2 \cdot 0$	$-2 \cdot 1$
2		14	1	-2	$= 14$	$= 1$	-2

$r_2 = 84 - 2 \cdot 35 = 14$

$s_2 = 1 - 2 \cdot 0 = 1$

$t_2 = 0 - 2 \cdot 1 = -2$

Berechnen von m_2 in Zeile 2

j	m_j	r_j	s_j	t_j
0	/	84	1	0
1	2	35	0	1
2	2	14	1	-2

$m_2 = \lfloor \frac{35}{14} \rfloor = 2$

denn $\underbrace{28}_{2\cdot 14} \leq 35 < \underbrace{42}_{3\cdot 14}$

Berechnen von r_3, s_3, t_3 in Zeile 3

j	m_j	r_j	s_j	t_j			
0	/	84	1	0			
1	2	35	0	1	35	0	1
2	2	14	1	-2	$-2 \cdot 14$	$-2 \cdot 1$	$-2 \cdot (-2)$ $=+4$
3		7	-2	5	$= 7$	$= -2$	$+5$

Berechnen von m_3 in Zeile 3

j	m_j	r_j	s_j	t_j
0	/	84	1	0
1	2	35	0	1
2	2	14	1	-2
3	2	7	-2	5

$m_3 = \lfloor \frac{14}{7} \rfloor = 2$

denn $\underbrace{14}_{2\cdot 7} \leq 14 < \underbrace{21}_{3\cdot 7}$

Berechnen von r_4, s_4, t_4 in Zeile 4

j	m_j	r_j	s_j	t_j			
0	/	84	1	0			
1	2	35	0	1			
2	2	14	1	-2	14	1	-2
3	2	7	-2	5	$-2 \cdot 7$	$-2 \cdot (-2)$ $=+4$	$-2 \cdot 5$
4		0	5	-12	$= 0$	$= 5$	-12

Der Algorithmus terminiert in Schritt $j = 4$ wegen $r_j = r_4 = 0$.

Output: $\mathrm{ggT}(84, 35) = r_{j-1} = 7$ und $s_{j-1} = -2$, $t_{j-1} = 5$. Es gilt: $\underbrace{(-2) \cdot 84}_{-168} + \underbrace{(5) \cdot 35}_{175} = 7$

2.6. Die Eulersche Phi-Funktion

In diesem Abschnitt untersuchen wir eine im Folgenden wichtige Funktion auf den natürlichen Zahlen: Die Eulersche φ-Funktion. Diese Funktion wird bei der späteren Behandlung von Anwendungen wie dem RSA-Schema eine zentrale Rolle spielen.

Definition 2.6.1 (Eulersche φ-Funktion - *Patenschaft: Ralf aka Bier Samuel <3*)**.**

Für $n \in \mathbb{N}$ ist die Eulersche φ-Funktion definiert als

$$\varphi(n) := |\{m \in \{1, \ldots, n\} \ : \ \mathrm{ggT}(m, n) = 1\}|$$

Die φ-Funktion $\varphi(\mathbf{n})$ **zählt** die zu n **teilerfremden Reste**, die beim Teilen durch n entstehen.

Bemerkung 2.6.2.

In der Definition von $\varphi(n)$ scheint die Bedingung $m \in \{1, \ldots, n\}$ etwas ungeschickt gewählt, da bei $m = n$ sofort $\mathrm{ggT}(m, n) = n$ gilt. Könnte man hier nicht also besser gleich $m \in \{1, \ldots, n-1\}$ schreiben? Dies *scheint* aber nur "richtiger" zu sein, denn für $n = 1$ gilt $\{1, \ldots, n\} = \{1\}$ aber $\{1, \ldots, n-1\} = \emptyset$.

Satz 2.6.3.

Für eine Primzahl $p \in \mathbb{N}$ gilt:

- $\varphi(p) = (p-1)$
- $\varphi(p^k) = p^{k-1}(p-1)$ mit Exponenten $k \in \mathbb{N}$, $k \neq 0$.

- Ist $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_\ell^{k_\ell}$ die Primzahlzerlegung von n mit $p_1 < p_2 < \ldots < p_\ell$ und $k_1, k_2 \ldots, k_\ell \neq 0$, so gilt:

$$\varphi(n) = p_1^{k_1-1} \cdot (p_1 - 1) \ \cdot p_2^{k_2-1} \cdot (p_2 - 1) \ \cdots \ p_\ell^{k_\ell-1} \cdot (p_\ell - 1)$$

Satz 2.6.3 liefert nun die Grundlage, um $\varphi(n)$ zu berechen: Zunächst muss n in seine Primzahlzerlegung zerlegt werden, und dann kann mittels Regel iii) die Berechnung von $\varphi(n)$ erfolgen:

Beispiel 2.6.4.

Es gelten:

$$\begin{aligned}
\varphi(8) &= \varphi\left(2^3\right) &&= 2^2 \cdot (2-1) &&= 4 \\
\varphi(12) &= \varphi\left(2^2 \cdot 3\right) &&= 2^1 \cdot (2-1) \cdot (3-1) &&= 4 \\
\varphi(360) &= \varphi\left(2^3 \cdot 3^2 \cdot 5\right) &&= 2^2 \cdot (2-1) \cdot 3^1 \cdot (3-1) \cdot (5-1) && \\
& &&= 2^2 \cdot 1 \cdot 3 \cdot 2 \cdot 4 = 96 && \\
\varphi(3^4 \cdot 5^4) &= 3^3 \cdot 2 \cdot 5^3 \cdot 4 &&= 27 \cdot 2 \cdot 125 \cdot 4 = \ldots &&
\end{aligned}$$

Beweis. (Satz 2.6.3) Wir beweisen Aussage i) und ii) "in einem Abwasch", in dem wir $\varphi(p^k)$ berechnen und $k = 1$ (also $p^k = p$) zulassen.

Es sei $p \in \mathbb{N}$ eine Primzahl und $k \in \mathbb{N}$, $k \neq 0$.

Die Zahl p^k hat als Teiler nur 1 und Vielfache von p.

Gilt für ein $m \in \mathbb{N}$ also $\mathrm{ggT}(m, p^k) \neq 1$, so muss $\mathrm{ggT}(m, p^k)$ (als Teiler von p^k) ein Vielfaches von p sein. In diesem Fall teilt p also die Zahl m, d.h. m ist ein Vielfaches von p.

Das heißt, die Zahlen $m \in \{1, \ldots, p^k\}$ mit $\mathrm{ggT}(m, p^k) \neq 1$ sind genau sie Vielfachen von p, d.h. es gilt

$$m \in \{\underbrace{1{\cdot}p,\ 2{\cdot}p,\ 3{\cdot}p,\ \ldots,\ p^{k-1}{\cdot}p}_{p^{k-1}-\text{viele}}\}.$$

Innerhalb der Menge $\{1, \ldots, p^k\}$ gibt es p^{k-1}-viele solcher p-Vielfachen, die Anzahl $\varphi(p^k)$ der restlichen Zahlen $\ell \in \{1, \ldots, p^k\}$ mit $\mathrm{ggT}(\ell, p^k) = 1$ ist also

$$\varphi(p^k) = \quad p^k - p^{k-1} = p^{k-1} \cdot (p-1).$$

Es gilt also $\varphi(p^k) = p^{k-1} \cdot (p-1)$.

Teil iii) von Satz 2.6.3 folgt mit Teil ii) direkt aus dem folgenden Lemma 2.6.5. □

Lemma 2.6.5.

Es seien $n, m \in \mathbb{N}$. Es gilt genau dann $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, wenn $\mathrm{ggT}(m, n) = 1$.

Beweis. Der Beweis zu Lemma 2.6.5 ist nicht sehr angenehm, und daher wird dieser Beweis für den interssierten Leser im Anhang geführt. □

Bemerkung 2.6.6 (Typischer Flüchtigkeitsfehler)**.**

Beim Berechnen von $\varphi(n)$ unter Klausurbedingungen ist der folgende Flüchtigkeitsfehler typisch.

Oft ist man so glücklich (endlich) die Primfaktorzerlegung von n berechnet zu haben, dass es passieren kann, dass man bei der abschließenden Berechnung/Notation schusselt:

Falsch ist:

$$\varphi(375) = \varphi(5 \cdot 5 \cdot 5 \cdot 3) \overset{\text{Falsch}}{=} \cancel{\varphi(5) \cdot \varphi(5) \cdot} \varphi(5) \cdot \varphi(3) = 4 \cdot 4 \cdot 4 \cdot 2 = 128$$

Richtig ist:

$$\varphi(375) = \varphi(5 \cdot 5 \cdot 5 \cdot 3) = \varphi(5^3) \cdot \varphi(3) = 5^2 \cdot 4 \cdot 2 = 200$$

In der folgenden Zeile steht zwar das richtige Ergebnis am Ende,

aber die Rechnung enhält zwei falsche Gleichheitszeichen:

$$\varphi(375) = \varphi(5 \cdot 5 \cdot 5 \cdot 3) \overset{\text{Falsch}}{=} \varphi(5) \cdot \varphi(5) \cdot \varphi(5) \cdot \varphi(3) \overset{\text{nochmal Falsch}}{=} 5 \cdot 5 \cdot 4 \cdot 2 = 200$$

3 Algebraische Strukturen - Gruppen, Ringe, Körper und Vektorräume

3.1. Gruppen

Eine Gruppe ist die mathematische Abstraktion von Rechnen mit einer einzelnen *umkehrbaren* Operation wie zum Beispiel die “Addition in $\mathbb{Z}$” oder die “Multiplikation in $\mathbb{Q} \setminus \{0\}$”.

Eine Gruppe $(G, \circ)$ besteht stets aus einer Menge (oft “G” genannt) auf der mit einer einzelnen Operation (oft mit “$\circ$” bezeichnet) gerechnet werden kann. Ein typisches Beispiel ist die Gruppe $(\mathbb{Z}, +)$ der Ganzen Zahlen zusammen mit der Addition. Die Überrschrift in diesem Kapitel könnte also auch lauten: "Gruppen: Abstraktes Rechnen mit einem Operator".

3.1.1. Axiomatische Definition einer Gruppe

Gruppen mittels Gruppen-Axiome einzuführen liefert eine sehr knappe Formulierung für eine Menge in der man lineare Gleichungen lösen kann:

Definition 3.1.1 (Gruppe)**.**

Eine Gruppe $(G, \circ)$ ist ein Tupel aus

- einer Menge G und
- einer Verknüpfung $\circ : \ G' \times G' \to G'$, wobei $G \subset G'$ ist,

so dass gelten:

G1.	$a \circ b \in G$	$\forall a, b \in G$	(Abgeschlossenheit)
G2.	$a \circ (b \circ c) = (a \circ b) \circ c$	$\forall a, b, c \in G$	(Assoziativität)
G3.	$\exists\, e \in G : \forall a \in G : e \circ a = a$		(Neutrales Element)
G4.	$\forall a \in G : \exists\, \bar{a} \in G : \bar{a} \circ a = e$		(Inverses Element)

Bemerkung 3.1.2 (Das neutrale Element)**.**

Das Neutrale Element e ist dasjenige Element $e \in G$, das jedes Element $a \in G$ unverändert lässt, wenn man e mit a verknüpft. In einer Gruppe mit einer additiven Verknüpfung übernimmt e die Rolle der Null, in einer Gruppe mit einer multiplikativen Verknüpfung übernimmt e die Rolle der 1.

Beispiel 3.1.3.

Das Tupel $(\mathbb{Z}, +)$ aus der Menge $\mathbb{Z}$ zusammen mit der gewöhnlichen Addition bildet eine Gruppe:

G1 Für alle $m, n \in \mathbb{Z}$ gilt $m + n \in \mathbb{Z}$.
G2 Für alle $m, n, k \in \mathbb{Z}$ gilt $m + (n + k) = (m + n) + k$.

G3 Das Neutrale Element ist hier die Zahl $e = 0$, sie erfüllt: $0 + x = x$ für alle $x \in \mathbb{Z}$.
G4 Das Inverse zu einer Zahl $m \in \mathbb{Z}$ ist die zugehörige Zahl $-m$ mit entgegengesetztem Vorzeichen.

Beispiel 3.1.4.

Die Menge $\mathbb{Q} \setminus \{0\}$ bildet zusammen mit der gewöhnlichen Multiplikation eine Gruppe:

G1 Für alle $x, y \in \mathbb{Q} \setminus \{0\}$ gilt $x \cdot y \in \mathbb{Q} \setminus \{0\}$.
G2 Für alle $x, y, z \in \mathbb{Z}$ gilt $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
G3 Das Neutrale Element ist hier die Zahl $e = 1$, sie erfüllt: $1 \cdot x = x$ für alle $x \in \mathbb{Q} \setminus \{0\}$.
G4 Das Inverse zu einer Zahl $x \in \mathbb{Q} \setminus \{0\}$ ist die zugehörige Zahl $\frac{1}{x} \in \mathbb{Q} \setminus \{0\}$.

Für das nächste Beispiel brauchen wir die folgenden Definitionen.

Definition 3.1.5.

Für Zahlen $s, t, n \in \mathbb{N}$ sei

$$s \odot_n t := \mathsf{Rest}(s \cdot t, n)$$

$$s \oplus_n t := \mathsf{Rest}(s + t, n).$$

Definition 3.1.6.

Für eine Zahl $n \in \mathbb{N}$ sei

$$\mathbb{Z}_n^* := \{k \in \mathbb{N} : k \leq n \text{ und } \mathrm{ggT}(k, n) = 1\}.$$

Beispiel 3.1.7.

Die Menge $(\mathbb{Z}_5^*, \odot_5)$ bildet eine Gruppe (wobei $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$):

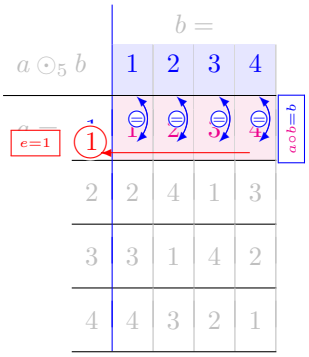
G1 Für alle $a, b \in \{1, 2, 3, 4\}$ gilt $a \odot_5 b \in \{1, 2, 3, 4\}$, dies kann man der unten angefügten Verknüpfungstabelle entnehmen.
G2 Muss man nachrechnen - geht auf die Assozitivität der natürlichen Zahlen zurück.
G3 Das Neutrale Element ist hier die Zahl $e = 1$, sie erfüllt: $1 \odot_5 b = b$ für alle $b \in \{1, 2, 3, 4\}$.
G4 Das Inverse zu den Zahlen $b \in \{1, 2, 3, 4\}$ liest man aus der Verknüpfungstabelle ab:

$b =$	1	2	3	4
Inverses $\overline{b} =$	1	3	2	4

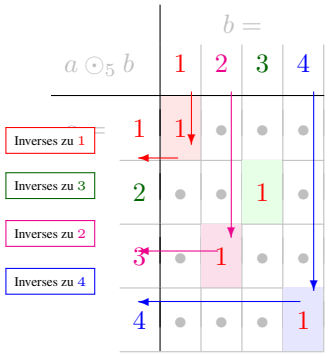
Verknüpfungstabelle

$a \odot_5 b$	$b=1$	$b=2$	$b=3$	$b=4$
$a=1$	1	2	3	4
$a=2$	2	4	1	3
$a=3$	3	1	4	2
$a=4$	4	3	2	1

Auslesen: Neutrales Element



Auslesen: Inverse Elemente



3.1.2. Rechenregeln in Gruppen

In jeder Gruppe gelten die folgenden Regeln:

Lemma 3.1.8.

Es sei $(G, \circ)$ eine Gruppe.

i. Es gibt in $(G, \circ)$ genau ein neutrales Element e.
ii. Es gilt $e \circ a = a \circ e$ für alle $a \in G$.
iii. Für jedes $a \in G$ gibt es genau ein Inverses $\overline{a}$.
iv. Es gilt $a \circ \overline{a} = \overline{a} \circ a$ für alle $a \in G$.
v. Das Inverse zu $\overline{a}$ ist a, d.h. es gilt $\overline{(\overline{a})} = a$ für alle $a \in G$.

Beweis. Exemplarisch führen wir hier die Beweise für i. und ii. sowie iv..

- **Zu iv.** Es sei $a \in G$ beliebig.
  Nach Axiom **G4** hat a ein Inverses $\overline{a}$ mit $\overline{a} \circ a = e$. Das Element $\overline{a}$ hat wiederum ein Inverses $\widetilde{a} := \overline{(\overline{a})}$
  Es gilt dann für $a \circ \overline{a}$:

$$a \circ \overline{a} \overset{\text{G3}}{=} e \circ (a \circ \overline{a}) \overset{\text{G4}}{=} (\widetilde{a} \circ \overline{a}) \circ (a \circ \overline{a}) \overset{\text{G2}}{=} \widetilde{a} \circ \Big(\underbrace{(\overline{a} \circ a)}_{e} \circ \overline{a} \Big) \overset{\text{G4}}{=} \widetilde{a} \circ (e \circ \overline{a}) \overset{\text{G3}}{=} \widetilde{a} \circ \overline{a} \overset{\text{G4}}{=} e$$

  Es gilt also $a \circ \overline{a} = e$. Wegen $\overline{a} \circ a = e$ gilt also $\overline{a} \circ a = a \circ \overline{a}$.
- **Zu ii.** Es sei $a \in G$ beliebig.
  Nach Axiom **G2** hat a ein Inverses $\overline{a}$ mit $\overline{a} \circ a = e$. Es gilt dann:

$$a \circ e \overset{\text{G3}}{=} a \circ (\overline{a} \circ a) \overset{\text{G2}}{=} \underbrace{(a \circ \overline{a})}_{=e} \circ a \overset{\text{iv.}}{=} e \circ a$$

- **Zu i.** Es seien $e, \widetilde{e} \in G$ zwei neutrale Elemente, d.h. sie erfüllen

$$e \circ a = a$$

$$\widetilde{e} \circ a = a \tag{3.1}$$

für alle $a \in G$. Dann gilt $\widetilde{e} \circ e = e$ nach (3.1) für $a = e$, sowie $\widetilde{e} \circ e \overset{\text{ii.}}{=} e \circ \widetilde{e} \overset{\textbf{G4}}{=} \widetilde{e}$. Insgesamt gilt also $\widetilde{e} = e$.

□

Lösen von Gleichungen

Die Gruppe ist die kleinste Recheneinheit der Mathematik, in der lineare Gleichungen stets lösbar sind:

In einer Gruppe $(G, \circ)$ sind Gleichungen der Form $a \circ x = b$ bei gegebenem $a, b \in G$ lösbar mit einem $x \in G$.

Um dies garantieren zu können, muss der Vorgang "a *mit* x *mittels* $\circ$ *verknüpfen*" rückgängig zu machen sein. Rechnet man zum Beispiel in $\mathbb{Q} \setminus \{0\}$ mit der Verknüpfung $\cdot$ so kann man die Gleichung $2 \cdot x = 7$ durch Multiplikation mit $1/2$ bzw. $0,5 \in \mathbb{Q}$ wie folgt lösen:

$$\begin{array}{rrrcl} & & 2 \cdot\ x & = & 7 \\ \Leftrightarrow & (0,5) \cdot & 2 \cdot\ x & = & 0,5 \cdot 7 \\ \Leftrightarrow & & x & = & 3,5 \end{array}$$

Die Zahl $0,5 \in \mathbb{Q} \setminus \{0\}$ nennt man das "multiplikative Inverse zu 2". Die Zahl $0,5$ kann also das ungeschehen machen, was die Multiplikation mit 2 "angerichtet hat", denn es gilt: $0,5 \cdot 2 = 1$ und die Zahl 1 benimmt sich bei der Multiplikation neutral.

Lemma 3.1.9.

Es sei $(G, \circ)$ eine Gruppe und $a, b \in G$.

Die Gleichung der Form $a \circ x = b$ hat stets eine Lösung $x \in G$, nämlich $x = \overline{a} \circ b$.

Beweis. In der Gruppe G gibt es ein zu a inverses Element $\overline{a}$. Verknüpfung mit $\overline{a}$ "entfernt " a auf der linken Seite der Gleichung. Beachten Sie, dass beim Umformen der Gleichung $a \circ x = b$ *alle* Gruppenaxiome **G1** bis **G4** verwendet werden müssen:

$$\begin{array}{rrrcll} & & a \circ\ x & = & b & \\ \Leftrightarrow & \overline{a} \circ & (a \circ\ x) & = & \overline{a} \circ b & \\ \overset{\textbf{G2}}{\Leftrightarrow} & (\overline{a} \circ & a) \circ\ x & = & \overline{a} \circ b & \text{Assoziativität: } \textbf{G2} \\ \overset{\textbf{G4}}{\Leftrightarrow} & e & \circ\ x & = & \overline{a} \circ b & \text{Eigenschaften des Inversen: } \textbf{G4} \\ \overset{\textbf{G3}}{\Leftrightarrow} & & x & = & \overline{a} \circ b & \text{Eigenschaften des Neutralen: } \textbf{G3} \end{array}$$

Dass die Lösung $x = \overline{a} \circ b$ wieder in G ist, liegt an Axiom **G1**. □

Beispiel 3.1.10 (Rechnen in der Gruppe $(\mathbb{Q} \setminus \{0\}, \cdot)$)**.**

Eine Gleichung der Form $a \cdot x = b$ mit $a, b \in \mathbb{Q} \setminus \{0\}$ hat immer eine Lösung $x = \frac{1}{a} \cdot b$.

Hier ist $\frac{1}{a}$ das Multiplikativ-Inverse zu $a \in \mathbb{Q} \setminus \{0\}$, das Inverse $\frac{1}{a}$ zu bilden ist immer möglich, da $a \neq 0$ gilt.

Beispiel 3.1.11 (Rechnen in der Gruppe $(\mathbb{Z}, +)$)**.**

Eine Gleichung der Form $a + x = b$ mit $a, b \in \mathbb{Z}$ hat immer eine Lösung $x = (-a) + b$.

Hier ist $-a$ das Additiv-Inverse zu $a \in \mathbb{Z}$.

Beispiel 3.1.12 (Rechnen in $(\mathbb{N}_0, +)$)**.**

Das Paar $(\mathbb{N}_0, +)$ ist **keine** Gruppe. Es gibt also Gleichungen der Form $a + x = b$ mit $a, b \in \mathbb{N}_0$, die keine Lösung in $\mathbb{N}_0$ besitzen:

Ein Beispiel für eine solche Gleichung ist $5 + x = 0$ die "Lösung" $x = -5$ liegt nicht in $\mathbb{N}_0$, d.h. man verlässt beim Lösen der Gleichung die vorgegbene Menge.

Beispiel 3.1.13 (Rechnen in $(\mathbb{Q}, \cdot)$)**.**

Das Paar $(\mathbb{Q}, \cdot)$ ist **keine** Gruppe. Es gibt also Gleichungen der Form $a \cdot x = b$ mit $a, b \in \mathbb{Q}$, die keine Lösung in $\mathbb{N}$ besitzen:

Ein Beispiel für eine solche Gleichung ist $0 \cdot x = 5$, diese Gleichung besitzt keine Lösung in $\mathbb{Q}$.

3.1.3. Abelsche Gruppen

Für die meisten bisher betrachteten Gruppen ist die Verknüpfungsreihenfolge in $a \circ b$ gleichgültig. Das gilt aber nicht allgemein für Grupppen:

Definition 3.1.14.

Eine Gruppe $(G, \circ)$ heißt abelsch, wenn zusätzlich zu den Gruppenaxiomen **G1** bis **G4** gilt:

GS. $a \circ b = b \circ a \quad \forall a, b \in G$ (Kommutativität (Symmetrie))

Abelsche Gruppen sind beispielsweise $(\mathbb{Z}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ (s. Beispiel 3.1.3, 3.1.4 und 3.1.7).

Beispiel 3.1.15.

Die Menge $\mathbb{O}(n)$ der orthogonalen Matrizen (s. Kapitel "Lineare Abbildungen" - Mathe für Informatik I) bildet zusammen mit der Matrix-Multiplikation eine nicht-abelsche Gruppe.

3.1.4. Isomorphe Gruppen

Es ist möglich, ein und dieselbe Gruppe auf verschiedene Arten und Weisen zu notieren:

Die Gruppe $(\{0, 1\}, \oplus_2)$ kann man abstrakt auffassen als eine Gruppe mit zwei Elementen, dem neutralen Element $e = 0$ und einem weiteren Element $x = 1$ mit den Rechenregeln $e \oplus_2 x = x \oplus_2 e = x$ und $e \oplus_2 e = x \oplus_2 x = e$.

Beispiel 3.1.16.

Augenscheinlich sind die Gruppen

- $(\{0,1\}, \oplus_2)$
- $(\{1,2\}, \odot_3)$
- $(\{\text{Falsch}, \text{Wahr}\}, \dot{\vee})$

"strukturell gleich", wenn man die jeweiligen Verknüpfungstabelle anschaut:

$a \oplus_2 b$	$b=$ 0	1
$a=$ 0	0	1
1	1	0

$a \odot_3 b$	$b=$ 1	2
$a=$ 1	1	2
2	2	1

$a \mathbin{\mathring{\vee}} b$	$b=$ F	W
$a=$ F	F	W
W	W	F

Ersetzt man in einer Gleichung $a \oplus_2 b = c$ in $(\{0,1\}, \oplus_2)$ ...

- jede 0 durch F,
- jede 1 durch W
- und $\oplus_2$ durch $\mathring{\vee}$

so erhält man wieder eine korrekte Gleichung.

Diesen Umstand wollen wir mathematisch formalisieren. Um zwei Gruppen $(G, \circ)$ und $(H, *)$, die prinzipiell gleich (also "isomorph" $\sim$ "gleich geformt") sind als solche auszuweisen, muss angegeben werden, welche Elemente der beiden Gruppen einander entsprechen:

Hierzu verwendent man eine bijektive Abbildung, d.h. eine Abbildung $f : G \to H$, die jedem $g \in G$ ein $h \in H$ zuordnet, so dass

- je zwei verschiedene $g, \widetilde{g} \in G$ auch verschiedene Bilder $f(g) \neq f(\widetilde{g}) \in H$ haben und
- es für jedes $h \in H$ ein $g \in G$ gibt mit $f(g) = h$.

Mit dieser Zuordnung f wird nun einem $g \in G$ sein Gegenstück $h := f(g)$ in H zugeordnet, so dass sich h in $(H, *)$ genauso, wie g sich in $(G, \circ)$ verhält.

Definition 3.1.17 (Isomorphe Gruppen)**.**

Zwei Gruppen $(G, \circ)$ und $(H, *)$ heißen ***isomorph***, wenn es eine bijektive Abbildung $f : G \to H$ gibt, so dass gilt:

$$f(g) * f(\widetilde{g}) \;=\; f(g \circ \widetilde{g}) \quad \forall g, \widetilde{g} \in G$$

Die Gleichung in der Definition lässt sich wie folgt lesen:

Für das Element $g \circ \widetilde{g} = c \in G$ müssen die zu $g, \widetilde{g}$ und c zugeordneten Elemente $f(g), f(\widetilde{g}), f(c) \in H$ folgende Identität erfüllen:

$$f(g) * f(\widetilde{g}) \;=\; f(c)$$

Kurz gesagt, $f(g), f(\widetilde{g})$ verhalten sich innerhalb von $H = f(G)$ wie $g, \widetilde{g}$ innerhalb von G. Es gilt:

$$g \circ \widetilde{g} = c \quad \Rightarrow \quad f(g) * f(\widetilde{g}) \; = \; f(c)$$

Beispiel 3.1.18.

Die Gruppen $(\{0,1\}, \oplus_2)$ und $(\{1,2\}, \odot_3)$ sind isomorph.

Mit $f : \{0,1\} \to \{1,2\}$ definiert durch $f(0) := 1$ und $f(1) := 2$ erhält man:

$$\begin{array}{lcll} a \oplus_2 b & = & c \quad \text{für } a,b,c \in \{0,1\} & \Longrightarrow \quad f(a) \odot_3 f(b) \; = \; f(c) \\ 0 \oplus_2 0 & = & 0 & \Longrightarrow \quad 1 \odot_3 1 \; = \; 1 \\ 0 \oplus_2 1 & = & 1 & \Longrightarrow \quad 1 \odot_3 2 \; = \; 2 \\ 1 \oplus_2 0 & = & 1 & \Longrightarrow \quad 2 \odot_3 1 \; = \; 2 \\ 1 \oplus_2 1 & = & 0 & \Longrightarrow \quad \underbrace{2}_{f(1)} \odot_3 \underbrace{2}_{f(1)} \; = \; \underbrace{1}_{f(0)} \end{array}$$

3.1.5. Die Gruppenordnung

Im Folgenden werden wir zeigen, was beim mehrfachen Verknüpfen ein und desselben Gruppenelements passiert. Interessanterweise kommt man in einer abelschen Gruppe immer wieder am neutralen Element "vorbei". Um dies zu zeigen benötigen wir die Eigenschaften einer Funktion $f_a : G \to G$, die ein Element $x \in G$ einfach mit einem (festen!) Element a verknüpft: $f_a(x) = a \circ x$. Diese Abbildung wird ***Translation*** um das Element a genannt.

Für eine Gruppe $(G, \circ)$ kann man die Mehrfach-Verknüfung eines Elementes mit a^n abkürzen:

Definition 3.1.19.

Für ein Element $a \in G$ einer Gruppe $(G, \circ)$ und eine natürliche Zahl $n \in \mathbb{N}$ ist definiert:

$$a^n = \underbrace{a \circ a \circ \ldots \circ a}_{n-\text{oft}} \circ e$$

Es gilt also $\quad a^0 = e \quad , \quad a^1 = a \quad , \quad a^2 = a \circ a \quad$ etc.

Die Gruppenordnung zählt die Elemente der Gruppe:

Definition 3.1.20 (Ordnung einer Gruppe)**.**

Für eine Gruppe $(G, \circ)$ ist die Anzahl $|G|$ der Elemente in G die ***Ordnung*** von G.

Hat G ***endlich*** / ***unendlich*** viele Elemente, so nennt man $(G, \circ)$ eine ***endliche*** Gruppe. / so sagt man: Die Gruppenordnung von $(G, \circ)$ ist ∞.

Satz 3.1.21.

Es sei $(G, \circ)$ eine endliche abelsche Gruppe mit neutralem Element e.

Für alle $a \in G$ gilt dann: $a^{|G|} = e$ ($|G|$ = Anzahl der Elemente von G).

Um diesen Satz zu beweisen benötigen wir das folgende Lemma:

Lemma 3.1.22.

Es sei $(G, \circ)$ eine Gruppe und $a \in G$ sei ein fest gewähltes Element. Dann ist die Abbildung $f_a : G \to G$ mit $f_a(x) := a \circ x$ bijektiv.

Beweis.

- **Surjektivität:** Zu zeigen ist: für jedes $y \in G$ gibt es ein $x \in G$ mit $f_a(x) = y$.
  Sei $y \in G$ beliebig. Wähle $x := \overline{a} \circ y$, dann gilt: $f_a(x) = a \circ (\overline{a} \circ y) \overset{\text{GI}}{=} (a \circ \overline{a}) \circ y = y$.

- **Injektivität:** Zu zeigen ist: für jedes Paar $x, x' \in G$ mit $x \neq x'$ gilt: $f_a(x) \neq f_a(\widetilde{x}')$.
  Es seien $x, x' \in G$ beliebig mit $x \neq x'$. Annahme es gelte: $f_a(x) = f_a(x')$. Dann gilt:

$$\begin{array}{lllllll} f_a(x) = f_a(x') & \Leftrightarrow & a \circ x & = & a \circ x' & |\overline{a} \circ & \\ & \Leftrightarrow & \overline{a} \circ (a \circ x) & = & \overline{a} \circ (a \circ x') & & \\ & \Leftrightarrow & (\overline{a} \circ a) \circ x & = & (\overline{a} \circ a) \circ x' & \Leftrightarrow \quad x = x' & \end{array}$$

  Die letzte Gleichung ist ein Widerspruch zu $x \neq x'$.

□

Nun können wir mit Lemma 3.1.22 den Satz 3.1.21 beweisen:

Beweis. [Satz 3.1.21] Es sei $(G, \circ)$ eine endliche abelsche Gruppe mit $n := |G|$ Elementen $g_1, \ldots, g_n \in G$. Weiter sei $a \in G$ beliebig (d.h. es gilt $a = g_i$ für ein i).

Da $f_a : G \to G$ mit $f_a(x) = a \circ x$ nach Lemma 3.1.22 eine bijektive Abbildung ist, gilt:

$$G = \{g_1, g_2, \ldots, g_n\} = \{a \circ g_1,\ a \circ g_2,\ \ldots,\ a \circ g_n\}$$

Die Gruppe $(G, \circ)$ ist abelsch. Bildet man also die Verknüpfung aller Elemente in G, so spielt die Reihenfolge keine Rolle. Es gilt also

$$\overbrace{g_1 \circ \cdots \circ g_n}^{\text{Verknüpfung aller } g_j \text{ sortiert}} = \overbrace{(a \circ g_1) \circ (a \circ g_2) \circ \cdots \circ (a \circ g_n)}^{\text{Verknüpfung aller } g_j \text{ “durcheinander”}}$$

Da $(G, \circ)$ abelsch ist, dürfen wir umsortieren, es gilt zum Beispiel $\overset{\curvearrowleft}{a} \circ g_1 \circ a \circ g_2 = g_1 \circ a \circ a \circ g_2$.
Wiederholt man dies immer wieder, so erhält man aus der letzen Gleichung schließlich:

$$\begin{array}{lll} g_1 \circ \cdots \circ g_n & = & g_1 \circ \cdots \circ g_n \ \circ \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ Stück}} \\ g_1 \circ \cdots \circ g_n & = & g_1 \circ \cdots \circ g_n \ \circ \ a^n \end{array}$$

Nun “kürzt” man durch sukzessives Multiplizieren auf beiden Gleichungsseiten mit $\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_n$. Dieses Kürzen liefert: $e = a^n$ bzw. $a^{|G|} = e$.

Eine zweite Möglichkeit dies einzusehen, folgt aus **G1**, der Abgeschlossenheit der Gruppenoperation. Die Verknüpfung aller Gruppenelemente ist wieder in G, es gibt also ein $g' \in G$ mit $g' = g_1 \circ \cdots \circ g_n$. Somit ist

$$\begin{aligned} & g_1 \circ \cdots \circ g_n = g_1 \circ \cdots \circ g_n \circ a^n \\ \Leftrightarrow \quad & g' = g' \circ a^n \\ \Leftrightarrow \quad & \bar{g}' \circ g' = \bar{g}' \circ g' \circ a^n \\ \Leftrightarrow \quad & e = e \circ a^n \\ \Leftrightarrow \quad & e = a^n \end{aligned}$$

was zu zeigen war. □

Beispiel 3.1.23 (Lemma 3.1.22)**.**

Dass die Abbildung $f_a : x \mapsto a \circ x$ bijektiv ist, hat zur Folge, dass die Verknüpungstabelle einer Gruppe $(G, \circ)$ immer ein kleines "Sudoku" ist:

In jeder Zeile (und in jeder Spalte) kommt jedes Element aus G *genau einmal* vor.

Dies veranschaulichen wir am Beispiel der Gruppe $(\mathbb{Z}_9^*, \odot_9)$. Es gilt für $a := 5$:

Element	g	1	2	4	5	7	8
Bild	$f_5(g) = 5 \odot_9 g$	5	1	2	7	8	4

$\leftarrow$ Jedes Element taucht genau einmal auf.

Hier ist die zweite Zeile "$f_5(g)$" eine Zeile aus der Verknüpfungstabelle von $\odot_9$:

		b=					
$a \odot_9 b$		1	2	4	5	7	8
a=	1	1	2	4	5	7	8
	2	2	4	8	1	5	7
	4	4	8	7	2	1	5
	5	5	1	2	7	8	4
	7	7	5	1	8	4	2
	8	8	7	5	4	2	1

Beispiel 3.1.24 (Satz 3.1.21)**.**

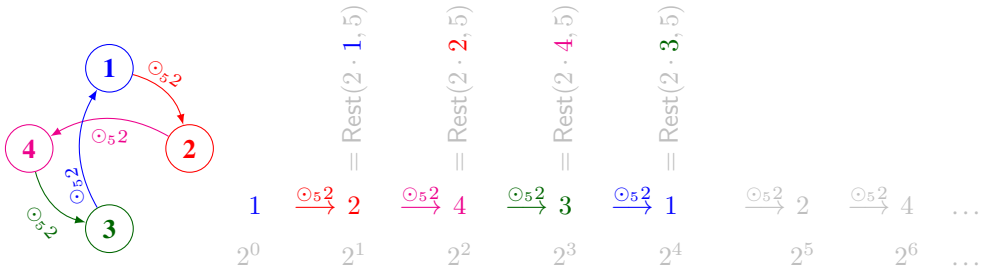
Wir untersuchen die Aussage $a^{|G|} = e$ am Beispiel der Gruppe $(\mathbb{Z}_5^*, \odot_5)$.

Hier ist $e = 1$. Weiter gilt $|G| = 4$ wegen $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Wir untersuchen also nun a^4 für $a \in \{1, 2, 3, 4\}$:

$$\begin{aligned} 1^4 &= \mathsf{Rest}(1^4, 5) = \mathsf{Rest}(1, 5) = 1 \\ 2^4 &= \mathsf{Rest}(2^4, 5) = \mathsf{Rest}(16, 5) = 1 \\ 3^4 &= \mathsf{Rest}(3^4, 5) = \mathsf{Rest}(81, 5) = 1 \\ 4^4 &= \mathsf{Rest}(4^4, 5) = \mathsf{Rest}(256, 5) = 1 \end{aligned}$$

Berechnet man alle Werte von 2^k in $\mathbb{Z}_5^*$ durch sukzessive Multiplikation "$\odot_5 2$", so erhält man nach und nach

alle Elemente aus $\mathbb{Z}_5^*$: Man startet bei $1 = 2^0$ und nach einem Zyklus von $4 = |\mathbb{Z}_5^*|$-oft "mal-zwei-nehmen" erreicht man zwangsläufig wieder die 1:



3.1.6. Die Gruppe $\mathbb{Z}_n^*$

In diesem Abschnitt beschäftigen wir uns ausgiebig mit der multiplikativen Gruppe $(\mathbb{Z}_n^*, \odot_n)$ (kurz $\mathbb{Z}_n^*$ genannt). Diese Gruppe spielt eine wichtige Rolle im Kontext des "RSA-Schemas" (ein Verschlüsselungsverfahren aus der Kryptographie), welches wir uns in der Vorlesung "Mathe für die Informatik IIänschauen werden. Nebenbei liefert diese Gruppe für den Fall, dass n eine Primzahl ist ein wichtiges Beispiel für endliche Körper.

Die wesentlichen Punkte im Arbeiten mit $\mathbb{Z}_n^*$ sind:

1. Die Inversen mittels des Satzes von Bézout zu bestimmen.
2. Die Arbeit mit Potenzen der Form $a^k := a \odot_n a \odot_n \cdots \odot_n a$ für $a \in \mathbb{Z}_n^*$.

Mittels des ersten Punkts werden wir beweisen, dass $(\mathbb{Z}_n^*, \odot_n)$ in der Tat eine Gruppe ist, und mittels des zweiten Punkts werden wir den Satz von Fermat und den Satz von Euler beweisen.

Bemerkung 3.1.25 (Warum mit teilerfremden Zahlen arbeiten?)**.**

Wir betrachten noch einmal das Rechnen mit Resten am Beispiel von Resten der Form $\mathsf{Rest}(n, 12)$ mit $n \in \mathbb{N}$. Die möglichen Zahlen, die als Rest beim Teilen durch 12 auftreten können sind $\mathbb{Z}_{12} := \{0, 1, 2, 3, \ldots, 11\}$.

Rechnet man nun auf diesen Zahlen mit einer Multiplikation modulo 12, also $a \odot_{12} b := \mathsf{Rest}(a \cdot b, 12)$, so gilt stets $a \odot_{12} b \in \mathbb{Z}_{12}$. Trotzdem ist $(\mathbb{Z}_{12}, \odot_{12})$ leider keine Gruppe:

- Man findet mit $e = 1$ schnell ein neutrales Element in $(\mathbb{Z}_{12}, \odot_{12})$, denn es gilt $1 \odot_{12} a = a$ für alle $a \in \mathbb{Z}_{12}$ wegen $\mathsf{Rest}(1 \cdot a, 12) = \mathsf{Rest}(a, 12) = a$.
- Aber die Zahl 0 kann in $(\mathbb{Z}_{12}, \odot_{12})$ kein Inverses besitzen:
  Es gilt $a \odot_{12} 0 = 0 \neq 1 = e$ für alle $a \in \mathbb{Z}_{12}$ wegen $\mathsf{Rest}(0 \cdot a, 12) = \mathsf{Rest}(0, 12) = 0$. Deswegen kommt kein $a \in \mathbb{Z}_{12}$ als Inverses für 0 in Frage.
  (Das "Inverse zu 0" $\overline{0}$ müsste erfüllen: $\overline{0} \odot_{12} 0 = e$.)

Lässt man die 0 weg, so zeigt sich, dass $(\{1, 2, 3, \ldots, 11\}, \odot_{12})$ ebenfalls keine Gruppe ist:

- Für die die Zahl $8 \in \{1, \ldots, 11\}$ gilt $3 \odot_{12} 8 = 0 \notin \{1, \ldots, 11\}$
  (wegen $\mathsf{Rest}(3 \cdot 8, 12) = \mathsf{Rest}(24, 12) = 0$).
  Also ist die Menge $\{1, \ldots, 11\}$ nicht abgeschlossen unter $\odot_{12}$.

Das Problem ist hier, dass $8 = 2 \cdot 4$ den Teiler 4 mit $12 = 3 \cdot 4$ gemeinsam hat, so dass die Gleichung $a \cdot 8 = k \cdot 12$

lösbar wird, mit $a = 3$ und $k = 2$.

Wir erinnern uns für $n \in \mathbb{N}$ an die Definition 3.1.5 der Menge

$$\mathbb{Z}_n^* := \{k \in \mathbb{N} \ : \ k \leq n \ \text{ mit } \ \mathrm{ggT}(k, n) = 1\}$$

der teilerfremden Zahlen zu n.

Bemerkung 3.1.26.

Es gilt $\mathrm{ggT}(1, n) = 1$, und deswegen gilt $1 \in \mathbb{Z}_n^*$ für alle $n \in \mathbb{N}$.

In Definition 3.1.5 scheint die Formulierung "$k \leq n$" etwas "unnütz", und "$k < n$" scheint naiv gedacht "richtiger" zu sein: Da $\mathrm{ggT}(n, n) = n$ gilt, sollte doch immer $n \notin \mathbb{Z}_n^*$ gelten, oder? - Nein, denn für $n = 1$ gilt nämlich (wegen $\mathrm{ggT}(1, 1) = 1$): $\mathbb{Z}_1^* = \{1\}$.

Damit Definition 3.1.5 auch auf $\mathbb{Z}_1^* = \{1\}$ passt, muss in der Definition tatsächlich "$k \leq n$" stehen und nicht $k < n$: Denn für $n = 1$ ist $\{k \in \mathbb{N} : \ 1 \leq k \leq n\} = \{1\}$ und $\{k \in \mathbb{N} : \ 1 \leq k < n\} = \emptyset$.

Beispiel 3.1.27.

Um zu der Zahl $n = 12 = 2^2 \cdot 3$ teilerfremd zu sein, muss eine Zahl $k \in \mathbb{N}$ erfüllen:

[2 teilt nicht k] und [3 teilt nicht k]

Um die Zahlen in $\mathbb{Z}_{12}^*$ zu erhalten muss man also aus $\{1, \ldots, 12\}$ alle echten Vielfachen von 2 und alle echten Vielfachen von 3 streichen. Es bleibt dann übrig:

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\} = \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}\}$$

Analog gilt für $n = 9 = 3^2$: $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

Satz 3.1.28.

Es sei $n \in \mathbb{N}$ und $n \geq 2$, dann ist $(\mathbb{Z}_n^*, \odot_n)$ eine abelsche Gruppe.

Beweis.

G1 Abgeschlossenheit von "$\odot_n$": Zu zeigen ist, dass aus $a, b \in \mathbb{Z}_n^*$ auch $a \odot_n b \in \mathbb{Z}_n^*$ folgt.

Es seien $a, b \in \mathbb{Z}_n^*$, d.h. $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n) = 1$. Wegen Lemma 2.4.4 teilt $\mathrm{ggT}(a \cdot b, n)$ das Produkt $\mathrm{ggT}(a, n) \cdot \mathrm{ggT}(b, n) = 1$, d.h. es gilt $\mathrm{ggT}(a \cdot b, n) = 1$.

Es sei nun $c := a \odot_n b$. Da $c = \mathsf{Rest}(a \cdot b, n)$ von der Form $c = a \cdot b - k \cdot n$ ist (mit $k \in \mathbb{N}$) folgt $\mathrm{ggT}(c, n) = \mathrm{ggT}(a \cdot b, n) = 1$ und damit $c \in \mathbb{Z}_n^*$.

Klar ist, dass die Verknüpfung $\odot_n$ symmetrisch und assoziativ ist. Denn es gilt:

G2
$$\begin{aligned} a \odot_n (b \odot_n c) &= \mathsf{Rest}\left(a \cdot \mathsf{Rest}(b \cdot c, n)\right), n) \\ &= \mathsf{Rest}(a \cdot b \cdot c, n) \\ &= \mathsf{Rest}\left(\mathsf{Rest}(a \cdot b, n) \cdot c, n\right) \quad = \quad (a \odot_n b) \odot_n c \end{aligned}$$

GS
$$\begin{aligned} a \odot_n b &= \mathsf{Rest}\left(a \cdot b, n\right) \\ &= \mathsf{Rest}(\, b \cdot a, n) = b \odot_n a \end{aligned}$$

G3 Das Neutrale Element in $(\mathbb{Z}_n^*, \odot_n)$ ist das Element 1, es gilt: $1 \odot_n a = \mathsf{Rest}(1 \cdot a, n) = a$ für alle $a \in \mathbb{Z}_n^*$.

G4 Berechnen der Inversen Elemente: Es sei $n \in \mathbb{N}$ mit $n \geq 2$ und $a \in \mathbb{Z}_n^*$, dann gilt $\mathrm{ggT}(a, n) = 1$.

Nach dem Satz von Bézout gibt es $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot n = \mathrm{ggT}(a, n) = 1$. Es gilt dann $s \cdot a = 1 - t \cdot n$ bzw. $s \odot_n a = \mathsf{Rest}(s \cdot a, n) = 1$. Die Zahl s ist also ein guter Kandidat für das Inverse zu a, allerdings kann es passieren, dass $s < 0$ oder $s > n$ gilt, und damit s nicht in $\mathbb{Z}_n^*$ liegt.

Setzt man $r := \mathsf{Rest}(s, n)$, so gilt: r ist das Inverse zu a. Dies beweisen wir nun. Es gilt:

$$\begin{aligned} r \odot_n a &= \mathsf{Rest}(r \cdot a, n) \\ &= \mathsf{Rest}\left(\mathsf{Rest}(s, n) \cdot a, n\right) \\ &= \mathsf{Rest}\left(s \cdot a, n\right) \qquad\qquad = 1 \end{aligned}$$

Es gilt also: r ist das Inverse zu a, denn $r \odot_n a = 1$.

□

3.1.7. Berechnen von Inversen in $\mathbb{Z}_n^*$ (per Satz von Bézout)

Will man für ein $a \in \mathbb{Z}_n^*$ das passende Inverse $\overline{a}$ berechnen, so liefert der Beweis von Satz 3.1.28 unter Punkt **G4** eine Berechnungsvorschrift:

1. Berechne via Euklidischem Algorithmus Bézout-Multiplikatoren $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot n = \mathrm{ggT}(a, n) = 1$.
2. Berechne $\overline{a} = \mathsf{Rest}(s, n)$.

Beispiel 3.1.29 (Inversenberechnung in $\mathbb{Z}_n^*$)**.**

Gegeben sei $n := 20$ und $k := 7 \in \mathbb{Z}_{20}^*$ dann erhält man via E.A.: $3 \cdot 7 - 1 \cdot 20 = 1$.

Das Inverse zu 7 ist also $3 = \mathsf{Rest}(3, 20)$.

Probe: Es gilt $7 \odot_{20} 3 = \mathsf{Rest}(21, 20) = 1$

Gegeben sei $n := 15$ und $k := 2 \in \mathbb{Z}_{15}^*$ dann erhält man via E.A.: $-7 \cdot 2 + 1 \cdot 15 = 1$.

Das Inverse zu 2 ist also $8 = \mathsf{Rest}(-7, 15)$.

(Die Zahl 8 erhält man durch sukzessives Adddieren von 15 zu $s = -7$.)

Probe: Es gilt $2 \odot_{15} 8 = \mathsf{Rest}(16, 15) = 1$

3.2. Ringe und Körper

In diesem Kapitel haben wir Gruppen als algebraische Struktur kennen gelernt. Das Wort Algebra kommt aus dem Arabischen von *al-dschabr* was mit "das Zusammenfügen gebrochener Teile" ins Deutsche zu übersezten ist. Es geht um das Rechnen mit Elementen einer festen Menge - abstrakter, wie schon bekannt, um Verknüpfungen auf einer Menge. Das Wort "Struktur" konkretisiert, dass diese Verknüpfung bestimmten Regeln folgt - die Gruppenaxiome (**G1**-**G4**). Neben Gruppen gibt es noch eine Vielzahl weiterer algebraischer Strukturen, sie sind durch die Verknüpfungen und entsprechenden "Rechenregeln" charakterisiert. Zwei weitere algebraische Strukturen lernen wir nun noch kurz kennen: Ringe und Körper.

3.2.1. Ringe

Zumindest die einfachen algebraischen Strukturen sind durch eine "bekannte Rechenstruktur"motiviert, beschreiben Sie. Für Ringe standen die ganzen Zahlen $\mathbb{Z}$ mit ihrer Addition und Multiplikation Modell.

Eine Ring ist also die mathematische Abstraktion vom Rechnen mit einer *umkehrbaren* Operation wie zum Beispiel die "Addition in $\mathbb{Z}$" und einer *nicht notwendigerweise umkehrbaren* Operation wie zum Beispiel die "Multiplikation in $\mathbb{Z}$".

Eine Ring $(R, +, \cdot)$ besteht stets aus einer Menge (oft "R" genannt) auf der mit zwei Operationen (oft mit "$+$" und "$\cdot$" bezeichnet) gerechnet werden kann.

Axiomatische Definition eines Rings

Bevor wir Ringe definieren, konkretisieren wir, was wir mit einer *nicht umkehrbaren* Operation meinen. Dazu führen wir die algebraische Struktur der Halbgruppe ein.

Definition 3.2.1 (Halbgruppe)**.**

Eine ***Halbgruppe*** $(H, \circ)$ ist ein Tupel aus

- einer Menge H und
- einer Verknüpfung $\circ : \ H' \times H' \to H'$ wobei $H \subset H'$ ist,

so dass gelten:

H1.	$a \circ b \in H$	$\forall a, b \in H$	(Abgeschlossenheit)
H2.	$a \circ (b \circ c) = (a \circ b) \circ c$	$\forall a, b, c \in H$	(Assoziativität)

Das kanonische Beispiel ist die Menge der ganzen Zahlen $\mathbb{Z}$ mit der Multiplikation.

Beispiel 3.2.2.

Das Tupel $(\mathbb{Z}, \cdot)$ der ganzen Zahlen $\mathbb{Z}$ und der gewöhnlichen Multiplikation bildet eine Halbgruppe aber keine Gruppe. Ein neutrales Element lässt sich mit der 1 noch finden, allerdings besitzen die meisten Elemente (alle bis auf die 1) kein Inverses. Für die 7 beispielsweise gibt es nämlich keine ganze Zahl $\bar{a} \in \mathbb{Z}$ mit $7 \cdot \bar{a} = 1$.

Beispiel 3.2.3.

Das Tupel $(\mathbb{N}, +)$ der natürlichen Zahlen $\mathbb{N}$ und der gewöhnlichen Addition bildet eine Halbgruppe aber keine Gruppe. Je nach Definition der natürlichen Zahlen (mit oder ohne 0) lässt sich nicht mal ein neutrales Element finden. Selbst wenn man die 0 bei der Definition der natürlichen Zahlen hinzunimmt, ist es nicht möglich für die meisten Elemente (alle bist auf die 0) ein Inverses zu finden. Für die 7 beispielsweise gibt es nämlich keine natürliche Zahl $\bar{a} \in \mathbb{Z}$ mit $7 + \bar{a} = 0$.

Beispiel 3.2.4.

Betrachtet man für eine endliche Menge von Vektoren $v_1, \ldots, v_s \in \mathbb{R}^n$ die Menge aller Positivkombinationen

$$\mathcal{K}(v_1, \ldots, v_s) = \left\{ v \in \mathbb{R} : v = \sum_{i=1}^{s} a_i \cdot v_i \text{ mit } a_1, \ldots, a_s \in \mathbb{R}^+ \right\}$$

wobei $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$ ist, so wird $\mathcal{K}(v_1, \ldots, v_s)$ auch als der von $v_1, \ldots, v_s$ aufgespannte ***Kegel*** bezeichnet. Kegel bilden zusammen mit der Addition von Vektoren in $\mathbb{R}^n$ Halbgruppen.

Bemerkung 3.2.5.

Wie in Beispiel (3.2.2) gesehen, kann es in Halbgruppen neutrale Elemente im Sinne von **G3** geben. Die Multiplikation der ganzen Zahlen $\mathbb{Z}$ besitzt ein neutrales Element (die 1). Häufig ist jedoch Axiom **G4** nicht erfüllt und es gibt keine Inversen Elemente.

Definition 3.2.6 (Ring)**.**

Ein ***Ring*** $(R, +, \cdot)$ ist ein Tripel aus

- einer Menge R und
- einer Verknüpfung $+ : \ R' \times R' \to R'$ und
- einer Verknüpfung $\cdot : \ R' \times R' \to R'$ wobei $R \subset R'$ ist,

so dass gelten:

R1.	$(R, +)$ bildet eine abelsche Gruppe		(Addition)
R2.	$(R, \cdot)$ bildet eine Halbgruppe		(Multiplikation)
R3.	$a \cdot (b + c) = a \cdot b + a \cdot c$	$\forall a, b, c \in R$	(Distributivgesetz I)
R4.	$(a + b) \cdot c = a \cdot c + b \cdot c$	$\forall a, b, c \in R$	(Distributivgesetz II)

Ein Ring ist also eine Menge mit zwei Verknüpfungen, wobei die eine Verknüpfung auf der Menge eine Gruppenstruktur, die andere Verknüpfung auf der Menge eine Halbgruppenstruktur erzeugt. Die Distributivgesetze regeln die Verträglichkeit der beiden Verknüpfungen.

Bemerkung 3.2.7.

Wir halten noch etwas zusätzliche Notation fest.

- Ist $(R, \cdot)$ eine abelsche Gruppe, so sagt man auch, dass $(R, +, \cdot)$ ein ***kommutativer Ring*** ist. In kommutativen Ringen sind die beiden Distributivgesetze äquivalent.
- Gibt es in der Halbgruppe $(R, \cdot)$ ein neutrales Element (oft als 1 bezeichnet) spricht man auch von einem ***unitären Ring***.

Beispiel 3.2.8.

Die ganzen Zahlen $\mathbb{Z}$ mit der gewöhnlichen Addition und Multiplikation bilden einen kommutativen Ring.

R1 Die ganzen Zahlen bilden mit der gewöhnlichen Addition eine abelsche Gruppe.

R2 Die ganzen Zahlen bilden nach Beispiel 3.2.2 mit der gewöhnlichen Multiplikation eine Halbgruppe.

R3 & R4 Bleiben die Distributivgesetze zu prüfen. In Bemerkung 3.2.7 haben wir festgehalten, dass in kommutativen Ringen die beiden Distributivgesetze äquivalent sind. Man vergewissert sich schnell, das in den ganzen Zahlen gilt

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{für alle } a, b, c \in \mathbb{Z}.$$

Analog zur Definition von $\mathbb{Z}_n^*$ definieren wir nun eine ähnliche Menge.

Definition 3.2.9.

Für eine Zahl $n \in \mathbb{N}$ sei

$$\mathbb{Z}_n := \{k \in \mathbb{N} \cup \{0\} : k < n\}.$$

Offensichtlich beinhatlet die Menge $\mathbb{Z}_n$ alle natürlichen Zahlen kleiner n und die Null. Es handelt sich dabei um eine Meng von Representanten der Restklassen modulo n - mit anderen Worten: Alle möglichen Reste modulo n. Es gilt im übrigen $\mathbb{Z}_n^* \subset \mathbb{Z}_n$.

Beispiel 3.2.10 (Restklassenringe)**.**

Das Tripel $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ bildet einen kommutativen unitären Ring auch als Restklassenring zum Parameter n bezeichnet.

R1 Man prüft leicht nach, dass $(\mathbb{Z}_n, \oplus_n)$ eine abelsche Gruppe ist (Abgeschlossenheit - Rechnen modulo n; Assozitivität und Kommutativität - Rechnenregeln in $\mathbb{Z}$ mit Resten verträglich; Inverses - für $a \in \mathbb{Z}_n$ ist $\mathsf{Rest}(-a, n)$ das inverse Element; Neutrales Element - die 0).

R2 Die Multiplikation $\otimes_n$ liefert als Ergebnis eine natürliche Zahl zwischen 0 und $n - 1$ und ist Assoziativ, wie wir gezeigt haben.

R3 & R4 Bleiben die Distributivgesetze zu prüfen. In Bemerkung 3.2.7 haben wir festgehalten, dass in kommutativen Ringen die beiden Distributivgesetze äquivalent sind. Mit Lemma 2.3.4 lässt sich die Distributivität der natürlichen Zahlen auf $\mathbb{Z}_n$ übertragen.

3.2.2. Körper

Wir beenden unseren kurzen Ausflug in die Welt der Algebra und ihrer Strukturen mit der Definition von Körpern. Modell standen die rationalen oder auch die reellen Zahlen mit der gewöhnlichen Addition und Multiplikation.

Definition 3.2.11 (Körper)**.**

Ein ***Körper*** $(K, +, \cdot)$ ist ein Tripel aus

- einer Menge K und
- einer Verknüpfung $+ : \ K' \times K' \to K'$ und
- einer Verknüpfung $\cdot : \ K' \times K' \to K'$ wobei $K \subset K'$ ist,

so dass gelten:

K1.	$(K, +)$ bildet abelsche Gruppe mit neutralem Element 0		(Addition)
K2.	$(K \setminus \{0\}, \cdot)$ bildet abelsche Gruppe mit neutralem Element 1		(Multiplikation)
K3.	$a \cdot (b + c) = a \cdot b + a \cdot c$	$\forall a, b, c \in K$	(Distributivgesetz)

Ein Körper ist also mit einer sich vertragenden kommutativen Addition und Multiplikation ausgestattet. Ein Körper ist also ein Ring, ein kommutativer unitärer Ring mit multiplikativem neutralem Element und multiplikativen Inversen.

Beispiel 3.2.12.

Die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ bilden mit der gewöhnlichen Addition und der gewöhnlichen Multiplikation ein Körper. Auch die komplexen Zahlen $\mathbb{C}$ bilden mit der komplexen Addition und Multiplikation ein Körper.

Beispiel 3.2.13.

Restklassenringe $\mathbb{Z}_n$ sind keine Körper. Ihnen fehlt für manche n für manche Elemente bei der Multiplikation das inverse Element, wie wir schon in Bemerkung 3.1.25 gesehen haben. Selbst wenn man zu $\mathbb{Z}_n^*$ übergeht (da können wir multiplikativ inverse Elemente berechnen) hat man keinen Körper in der Hand. Die Addition macht den Strich durch die Rechnung, denn erstens ist das neutrale Element der Addition $0 \notin \mathbb{Z}_n^*$ und außerdem ist (im Allgemeinen) die Addition nicht abgeschlossen, wie das folgende Beispiel zeigt: Sei $n = 8$, dann ist $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ - aber $1 + 3 = 4 \notin \mathbb{Z}_n^*$.

Endliche Körper

Beispiel 3.2.13 wirft die Frage auf, ob es endliche Körper gibt. Die Antwort ist ja und die Antwort ist überraschend, wir kennen schon endliche Körper: $\mathbb{Z}_n$ ist ein Körper, wenn n eine Primzahl ist. Des Weiteren gibt es für jede Primzahlpotenz p^k einen endlichen Körper dieser Ordnung (meint Anzahl der Elemente - Ordnung der abelschen Gruppe der Addition). Die Konstruktion dieser Körper mit Ordnung p^k ist allerdings nicht leicht zu skizieren, es handelt sich dabei um Gallois-Erweiterungen von $\mathbb{Z}_n$. Wir beobachten zunächst, dass die Menge $\mathbb{Z}_2 = \{0, 1\}$ ein Körper ist.

Beispiel 3.2.14.

Dazu betrachten wir die Verknüpfungstafeln der Addition und erinnern uns, dass die Addition in $\mathbb{Z}_2$ eine abelsche Gruppenstruktur entfaltet.

$a \oplus_2 b$		$b=$ 0	1
$a=$	0	0	1
	1	1	0

Die Multiplikation in $\mathbb{Z}_2 \setminus \{0\} = \{1\}$ ist bestechend einfach, sicherlich handelt es sich bei der multiplikativen Gruppe, die aus der $\{1\}$ besteht um eine abelsche Gruppe. Das Distributivgesetzt gelten dank der Rechenoperationen mit Rest aufgrund des Distributivgesetzes in den natürlichen Zahlen.

Der Knackpunkt scheint die Existenz von multiplikativen Inversen in $\mathbb{Z}_n \setminus \{0\}$ zu sein. Tatsächlich ist aber für eine Primzahl n

$$\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$$

und wir wissen, dass $\mathbb{Z}_n^*$ eine abelsche Gruppe ist. Wir halten also fest:

Lemma 3.2.15.

Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist der Restklassenring $\mathbb{Z}_p$ eine Körper.

Beweis. In Beispiel 3.2.10 haben wir gezeigt, dass Restklassenringe kommutative unitäre Ringe sind. Bleibt zu zeigen, dass $\mathbb{Z}_p \setminus \{0\}$ eine abelsche Gruppe ist und dass das Distributivgesetz gilt. Letzteres überträgt sich von den natürlichen Zahlen (über das Rechnen mit Resten). Man beobachtet, dass für Primzahlen $\mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*$ gilt und wir wissen schon, dass $\mathbb{Z}_p^*$ eine abelsche Gruppe ist. □

Analog zur Gruppenisomorphie definieren wir nun Isomorphie von Körpern.

Definition 3.2.16 (Isomorphe Körper)**.**

Zwei Körper $(K, +, \cdot)$ und $(K', \oplus, \otimes)$ heißen ***isomorph***, wenn es eine bijektive Abbildung $f : K \to K'$ gibt, so dass gilt:

$$f(0_K) = 0_{K_1}$$
$$f(a+b) = f(a) \oplus f(b) \quad \forall a, b \in K$$
$$f(1_K) = 1_{K_1}$$
$$f(a \cdot b) = f(a) \otimes f(b) \quad \forall a, b \in K$$

Endliche Körper spielen eine wichtige Rolle in der Zahlentheorie, algebraischer Geometrie, Kryptographie und Codierungstheorie, wie wir im nächsten Kapitel sehen werden. Wir halten nun noch einige Aussagen über endliche Körper fest, ohne die komplizierten Beweise zu betrachten.

Satz 3.2.17.

Sei $n \in \mathbb{N}$. Alle endlichen Körper der Ordnung n sind isomorph.

Satz 3.2.18.

Für jede Primzahl p und jede positive natürliche Zahl n existiert (bis auf Isomorphie) genau ein Körper mit p^n Elementen.

Definition 3.2.19 (Endliche Körper)**.**

Sei $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N}$. Dann bezeichnen wir den (bis auf Isomorphie) eindeutigen Körper mit p^n Element als $\mathbb{F}_p^n$. Dabei heißt p die ***Charakteristik*** von $\mathbb{F}_{p^n}$. Für unendliche Körper haben Charakteristik 0.

Wir halten noch eine amüsante Beobachtung zum Schluss fest.

Lemma 3.2.20.

In endlichen Körpern mit der Chrakteristik p gilt die *falsche binomische Formel*

$$(x+y)^p = x^p + y^p.$$

Beweis. Wir beweisen die Aussage nur für endliche Körper $\mathbb{F}_p$ wobei p eine Primzahl ist. Nach Satz 3.2.17 sind können wir von dem endlichen Körper $\mathbb{F}_p$ sprechen, der insbesondere isomorph zu $\mathbb{Z}_p$ ist. Rechnen wir also in $\mathbb{Z}_p$ dann ist nach dem binomischen Lehrsatz für alle $x, y \in \mathbb{Z}_p$

$$\begin{aligned}
(x+y)^p &\equiv \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} \pmod{p} \\
&\equiv \binom{p}{0} x^0 y^p + \binom{p}{1} x^1 y^{p-1} + \ldots + \binom{p}{p-1} x^{p-1} y^1 + \binom{p}{p} x^p y^0 \pmod{p} \\
&\equiv y^p + \binom{p}{1} x^1 y^{p-1} + \ldots + \binom{p}{p-1} x^{p-1} y^1 + x^p \pmod{p} \qquad (3.2)
\end{aligned}$$

weil $\binom{p}{0} = \frac{p!}{(p-p)!\cdot 0!} = 1$ und $\binom{p}{p} = \frac{p!}{(p)!\cdot(p-p)!} = 1$ (da $0! = 1$ definiert ist).

Wir beobachten nun, dass $\binom{p}{i} \equiv 0 \pmod{p}$ ist für $0 < i < p$, denn

$$\begin{aligned}
& \binom{p}{i} = \frac{p!}{(p-i)! \cdot i!} \\
\Leftrightarrow \qquad & (p-i)! \cdot i! \cdot \binom{p}{i} = p!
\end{aligned}$$

Die rechte Seite ist durch p teilbar, also muss auch die linke Seite durch p teilbar sein. Die linke Seite enthält drei Faktoren wobei gilt

$$p \nmid (p-i)! \qquad \text{und} \qquad p \nmid (i)!$$

da alle Zahlen in dem Produkt $(p-i)! = 1 \cdot 2 \cdots ((p-i)-1) \cdot (p-i)$ echt kleiner sind als p und p als Primzahl nur die Teiler 1 und p hat - gleiches gilt für $i!$ (das Argument funktioniert nicht für $i = p$ und $i = 0$).

Demnach muss $\binom{p}{i}$ durch p teilbar sein.

Es gilt also nach (3.2), dass

$$(x+y)^p \equiv y^p + \underbrace{\binom{p}{1} x^1 y^{p-1}}_{\equiv 0 \pmod p} + \ldots + \underbrace{\binom{p}{p-1} x^{p-1} y^1}_{\equiv 0 \pmod p} + x^p \equiv y^p + x^p \pmod p.$$

□

3.3. Vektorräume

Das Hauptziel der ersten Hälfte dieser Vorlesung ist das Verständnis *linearer Abbildungen*. Dies ist ein Typ von Abbildungen, den wir in der Tat sehr gut verstehen. Deshalb befasst sich die zweite Hälfte der Vorlesung in etwa damit, wie man Abbildungen, die nicht linear sind, durch lineare Abbildungen annähern kann.

Um den Begriff der linearen Abbildung einzuführen, müssen wir beschreiben, was sie wohin abbildet. Diese Objekte sind "Vektoren".

3.3.1. Die Vektorräume $\mathbb{R}^n$

In diesem Skript erinnern wir *zunächst* an die aus der Schule bekannten Vektoren aus dem $\mathbb{R}^n$. Eine genaue Definition dafür, was ein allgemeiner Vektor ist, findet sich im nachfolgenden Abschnitt. Ein Vektor in der Schulmathematik ist zunächst einmal ein Vektor aus $\mathbb{R}^3$ oder $\mathbb{R}^2$, d.h. eine Spalte mit Zahleneinträgen. Diese Vektoren haben eine geometrische Bedeutung, die sich auf zwei verschiedene Weisen verstehen lässt:

- Ein Vektor kann als Punkt in einem Raum aufgefasst werden. Wählt man beispielsweise einen festen Bezugspunkt im uns umgebenden dreidimensionalen Raum, so lässt sich jeder Punkt in unserem Universum durch einen Vektor mit drei Einträgen (Höhe, Breite, Länge) relativ zu diesem Punkt beschreiben.
- Andererseits repräsentieren Vektoren in der Physik Kräfte, also eine Messgröße die mit einer Richtung einhergeht: Im Gegensatz zu *skalaren* Messgrößen wie Temperatur oder Masse, muss man um eine Kraft vollständig zu beschreiben nicht nur angeben wie groß die Kraft ist, sondern auch in welche Richtung sie wirkt.

Konkret wurde ein mehrdimensionaler reeller Vektor definiert wie im Folgenden:

Erinnerung
Für ein festes $n \in \mathbb{N}$ ist $\mathbb{R}^n$ ein n-dimensionaler Vektorraum.

Ein Vektor $\vec{x} \in \mathbb{R}^n$ ist ein Tupel mit n reellen Zahleneinträgen $x_1, x_2, \ldots x_n \in \mathbb{R}$. Die allgemeine Form eines solchen Vektors $\vec{x}$ lautet:

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Die Zahlen $x_1, \ldots, x_n$ heißen die Komponenten des Vektors.

Es ist zwischen dem $\mathbb{R}^n$ als Vektorraum und dem n-dimensionalen Raum, der mit Koordinaten (zum Beispiel den kartesischen Koordinaten $(x_1, \ldots, x_n)$) beschrieben wird, zu unterscheiden. Im n-dimensionalen Raum wird jeder Punkt eindeutig durch seine Koordinaten beschrieben. Bettet man den Vektorraum $\mathbb{R}^n$ in den n-dimensionalen Raum ein, dann gibt es für jeden Punkt im Raum einen Stützvektor, der vom Ursprung auf

diesen Punkt deutet (die entsprechende Einbettung diskutieren wir nachdem wir das Konzept der Basis eines Vektorraums kennengelernt haben). Die Komponenten dieses Stützvektors entsprechen den kartesischen Koordinaten des Punktes.

Sage-Box (Vektor)**.**

```
sage: x = vector([0, -4, -1])
(0, -4, -1)
```

3.3.2. Rechnen im $\mathbb{R}^n$

Wir führen zwei Rechenregeln für Vektoren ein:

Definition 3.3.1.

Es sei $n \in \mathbb{N}$. Für zwei Vektoren $\vec{a}, \vec{b} \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gelten:

$$\vec{a} + \vec{b} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} := \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} \qquad \lambda \cdot \vec{a} = \lambda \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} := \begin{pmatrix} \lambda \cdot a_1 \\ \vdots \\ \lambda \cdot a_n \end{pmatrix}$$

Sage-Box (Rechnen mit Vektoren)**.**

```
sage: a = vector([1, 2, 3])
sage: b = vector([4, 5, 6])
sage: s = 2
sage: a + b
(5, 7, 9)
sage: s * a
(2, 4, 6)
```

Bemerkung 3.3.2.

Man kann Vektoren mit *gleich vielen* Einträgen addieren oder voneinander abziehen (Dies geht mit Vektoren mit verschieden vielen Einträgen nicht!).

Für die Addition von Vektoren und die Multiplikation mit einer Zahl gelten die selben Rechenregeln, die man schon von "normalen Zahlen" kennt:

Korollar 3.3.3.

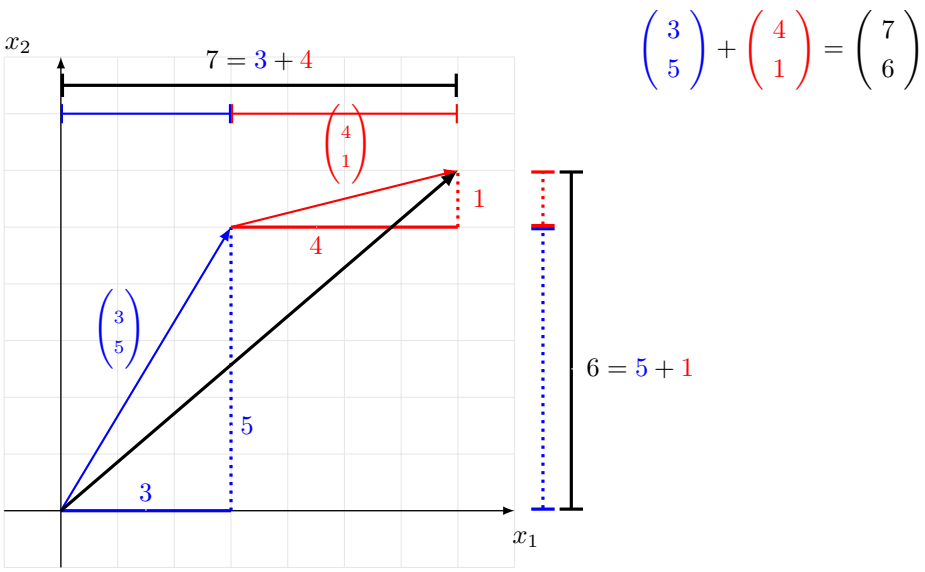
Für $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^n$ und $\lambda, \mu \in \mathbb{R}$ gelten:

$$\begin{aligned} \vec{a} + \vec{b} &= \vec{b} + \vec{a} && && && \text{(Kommutativgesetz)} \\ \left(\vec{a} + \vec{b}\right) + \vec{c} &= \vec{a} + \left(\vec{b} + \vec{c}\right) && && && \text{(Assoziativgesetz)} \\ (\lambda + \mu) \cdot \vec{a} &= \lambda \cdot \vec{a} + \mu \cdot \vec{a} && \text{und} && \lambda \cdot \left(\vec{a} + \vec{b}\right) &= \lambda \cdot \vec{a} + \lambda \cdot \vec{b} && \text{(Distributivgesetze)} \end{aligned}$$

Geometrische Interpretation des Rechnens im $\mathbb{R}^n$

Sei $n \in \mathbb{N}$ und seinen $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^n$.

► **Addition** Die *Addition* zweier Vektoren $\vec{a}$ und $\vec{b}$ entspricht geometrisch dem Aneinanderhängen der entsprechenden Vektoren. In der folgenden Abbildung für $n = 2$:

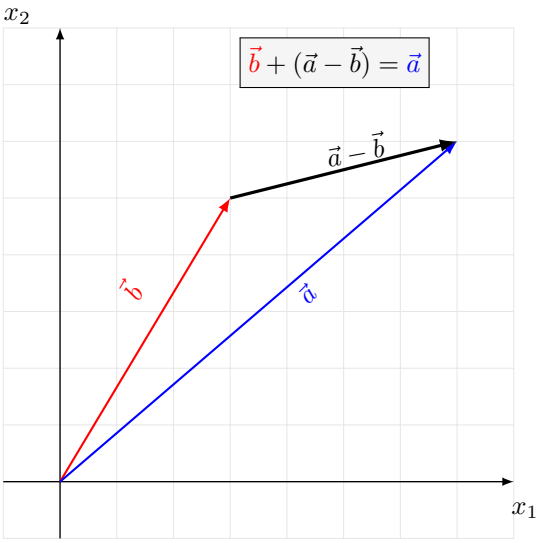


► **Subtraktion** Die *Subtraktion* zweier Vektoren, $\vec{a} - \vec{b}$, wird einfach als Addition von $\vec{a}$ und $-\vec{b}$ aufgefasst. Geometrisch kann man dies als das umgekehrte Anhängen des Vektors $\vec{b}$ an den Vektor $\vec{a}$ verstehen.

Eine deutlich bessere Anschauung erhält man jedoch, wenn man $\vec{c} = \vec{a} - \vec{b}$ liest als "$\vec{c}$ ist derjenige Vektor, der von $\vec{b}$ zu $\vec{a}$ führt". Denn es gilt:

$$\vec{c} = \vec{a} - \vec{b} \qquad \Leftrightarrow \qquad \vec{b} + \vec{c} = \vec{a}$$

Dies liefert dann das folgende Bild:



$$\vec{a} - \vec{b} = \begin{pmatrix} 7 \\ 6 \end{pmatrix} - \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$$

► **Multiplikation mit einer Zahl** Die *Multiplikation* eines Vektors mit einer *Zahl* ist *verträglich* mit der Vektor-Addition. Dies bedeutet, dass beispielsweise $2 \cdot \vec{a} = \vec{a} + \vec{a}$ gilt:

$$2 \cdot \vec{a} = 2 \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 2 \cdot a_1 \\ \vdots \\ 2 \cdot a_n \end{pmatrix} = \begin{pmatrix} a_1 + a_1 \\ \vdots \\ a_n + a_n \end{pmatrix} = \vec{a} + \vec{a}.$$

Geometrisch entspricht die Multiplikation eines Vektors mit einer Zahl $\lambda \in \mathbb{R}$ also einer Streckung bzw. einer Stauchung von $\vec{a}$ um den Faktor λ,

für $0 < |\lambda| < 1$ ist $\lambda \cdot \vec{a}$ *kürzer* als $\vec{a}$. für $1 < |\lambda|$ ist $\lambda \cdot \vec{a}$ *länger* als $\vec{a}$.

Ist λ negativ, so kehrt sich die Richtung eines Vektors $\vec{a}$ beim Multiplizieren mit λ um, der Vektor $-\vec{a} = (-1) \cdot \vec{a}$ zeigt also genau entgegengesetzt zu $\vec{a}$.

3.3.3. Allgemeine Vektorräume

Im weiteren Verlauf werden wir uns nun zunächst mit abstrakteren Vektorräumen beschäftigen zum Beispiel dem Vektorraum der Polynome. Die bereits bekannten Rechengesetze aus dem $\mathbb{R}^n$ wollen wir dabei "mitnehmen" also auf ein abstrakteres Niveau anheben. Im Wesentlichen verlangen wir also einfach, dass die beiden Rechenoperationen "Addition von Vektoren" und "Multiplikation eines Vektors mit einer Zahl" *sinnvoll* funktionieren:

Bei genauerem Hinsehen entdeckt man, dass $(\mathbb{R}^n, +)$ eine Gruppe ist, dass also die Elemente aus $\mathbb{R}^n$ beliebig addiert und subtrahiert werden können, und dass es ein Neutrales Element (eine Null, in diesem Fall der Nullvektor) gibt. Die Multiplikation mit Zahlen $\lambda \in \mathbb{R}$ kommt dann als "Extra" hinzu. Die Addition innerhalb der Gruppe und die Multiplikation mit Elementen "von außen" aus $\mathbb{R}$ müssen bestimmte Verträglichkeitsregeln erfüllen.

Wiederholung - Eigenschaften des $\mathbb{R}^n$
In der Menge $V := \mathbb{R}^n$ sind die folgenden Eigenschaften erfüllt:

► $(V, +)$ ist eine *abelsche* Gruppe. Also gelten

RA1.	$\vec{v}+\vec{w}\in V$	$\forall \vec{v},\vec{w}\in V$	(Abgeschl. der Addition)
RA2.	$\vec{v}+(\vec{w}+\vec{x})=(\vec{v}+\vec{w})+\vec{x}$	$\forall \vec{v},\vec{w},\vec{x}\in V$	(Assoziativität)
RA3.	$\exists\, \vec{e}\in V:\forall \vec{v}\in V:\vec{e}+\vec{v}=\vec{v}$		(Neutrales Element)
RA4.	$\forall \vec{v}\in V:\exists\ -\vec{v}\in V:-\vec{v}+\vec{v}=e$		(Inverses Element)
RA5.	$\vec{v}+\vec{w}=\vec{w}+\vec{v}$	$\forall \vec{v},\vec{w}\in V$	(Kommutativität)

- Abgeschlossenheit bezüglich der Multiplikation mit Elementen in $\mathbb{R}$:

RM1.	$\lambda\cdot\vec{v}\in V$	$\forall\lambda\in\mathbb{R},\vec{v}\in V$	(Abgeschl. der Multiplikation)

- Es gelten Verträglichkeitsregeln für alle $\vec{v},\vec{w}\in V$ und $\lambda,\mu\in\mathbb{R}$:

RV1.	$\lambda\cdot(\mu\cdot\vec{v})$	$=$	$(\lambda\cdot\mu)\cdot\vec{v}$	(Assoziativität)
RV2.	$(\lambda+\mu)\cdot\vec{v}$	$=$	$\lambda\cdot\vec{v}+\mu\cdot\vec{v}$	(Distributivgesetz I)
RV3.	$\lambda\cdot(\vec{v}+\vec{w})$	$=$	$\lambda\cdot\vec{v}+\lambda\cdot\vec{w}$	(Distributivgesetz II)
RV4.	$1\cdot\vec{v}$	$=$	$\vec{v}$	(Neutralität der 1)

Diese Eigenschaften wollen wir verallgemeinern, doch zunächst noch ein Hinweis bezüglich der Notation.

Bemerkung 3.3.4 (Verwendung der Operatoren)**.**

Um dabei die Definition korrekt und so allgemein wie möglich zu halten, verwenden wir für die "neuen" Operationen (Vektoraddition & skalare Multiplikation) hervorgehobene Symbole $\oplus$ und $\odot$. Im normalen mathematischen Alltag schreibt man aber statt dessen einfach "+" und "·". Dies werden wir nach diesem Abschnitt auch so tun und haben wir bisher auch schon für die Vektorräume $\mathbb{R}^n$ gentan. Im Prinzip sind nämlich die beiden Additionen $\begin{pmatrix}1\\1\end{pmatrix}\oplus\begin{pmatrix}2\\2\end{pmatrix}$ und $1+2$ tatsächlich unterschiedliche Operationen.

Wir definieren nun allgemeine Vektorräume.

Definition 3.3.5.

Eine Menge V zusammen mit

- einer inneren Verknüpfung $\oplus : V'\times V'\to V'$ ("Vektor-Addition")
- einer äußeren Verknüpfung $\odot : \mathbb{K}\times V'\to V'$, wobei $V\subset V'$ ist, ("Multiplikation mit einem Skalar")

nennt man einen *Vektorraum über* $\mathbb{K}$, falls gelten

- $(V,\ \oplus\ )$ ist eine *abelsche* Gruppe. Also gelten

VA1.	$\vec{v}\oplus\vec{w}\in V$	$\forall \vec{v},\vec{w}\in V$	(Abgeschl. der Addition)
VA2.	$\vec{v}\oplus(\vec{w}\oplus\vec{x})=(\vec{v}\oplus\vec{w})+\vec{x}$	$\forall \vec{v},\vec{w},\vec{x}\in V$	(Assoziativität)
VA3.	$\exists\,\vec{e}\in V:\forall\vec{v}\in V:\vec{e}\oplus\vec{v}=\vec{v}$		(Neutrales Element)
VA4.	$\forall\vec{v}\in V:\exists\ -\vec{v}\in V:-\vec{v}\oplus\vec{v}=\vec{e}$		(Inverses Element)
VA5.	$\vec{v}\oplus\vec{w}=\vec{w}\oplus\vec{v}$	$\forall\vec{v},\vec{w}\in V$	(Kommutativität)

- Abgeschlossenheit bezüglich der Multiplikation mit Elementen in $\mathbb{K}$:

VM1.	$\lambda\odot\vec{v}\in V$	$\forall\lambda\in\mathbb{K},\vec{v}\in V$	(Abgeschl. der Multiplikation)

- Es gelten Verträglichkeitsregeln für alle $\vec{v},\vec{w}\in V$ und $\lambda,\mu\in\mathbb{K}$:

VV1.	$\lambda\odot(\mu\odot\vec{v})$	$=$	$(\lambda\odot\mu)\odot\vec{v}$	(Assoziativität)
VV2.	$(\lambda+\mu)\odot\vec{v}$	$=$	$\lambda\odot\vec{v}+\mu\odot\vec{v}$	(Distributivgesetz I)
VV3.	$\lambda\odot(\vec{v}+\vec{w})$	$=$	$\lambda\odot\vec{v}+\lambda\odot\vec{w}$	(Distributivgesetz II)
VV4.	$1\odot\vec{v}$	$=$	$\vec{v}$	(Neutralität der 1)

In der Gruppe $(V, \oplus)$ bezeichnet man ...

- das neutrale Element mit $\vec{0}$.
- das zu $\vec{v} \in V$ inverse Element mit $-\vec{v}$.

Bemerkung 3.3.6.

Ein Vektorraum ist eine abelsche, additive Gruppe $(V, \oplus)$ zusammen mit einer *äußeren* Multiplikation "$\odot$" mit Elementen aus einem Körper $\mathbb{K}$. Die Addition innerhalb der Gruppe und die Multiplikation mit Elementen "von außen" aus $\mathbb{K}$ müssen bestimmte *Verträglichkeitsregeln* erfüllen.

Aus der Definition des Vektorraumes ergeben sich sofort Konsequenzen:

Korollar 3.3.7.

In einem Vektorraum V gelten:

a. Die Menge V ist nicht leer.

b. Für $\lambda \in \mathbb{K}$ und $\vec{v} \in V$ gelten die Rechenregeln:

i. $0 \odot \vec{v} = \vec{0}$

ii. $(-1) \odot \vec{v} = -\vec{v}$

iii. $\lambda \odot \vec{0} = \vec{0}$

iv. $\lambda \odot \vec{v} = \vec{0} \iff \Big((\lambda = 0) \vee (\vec{v} = \vec{0}) \Big)$

Beweis.

zu a. Folgt direkt aus der Definition einer Gruppe, also aus Axiom **VA3**.

zu b. zu i. Wegen $\vec{v} \overset{\text{Trick}}{=} (0+1) \odot \vec{v} \overset{\text{VV2}}{=} 0 \odot \vec{v} \oplus \vec{v}$ folgt: $0 \odot \vec{v}$ ist das neutrale Element $\vec{0}$ in $(V, \oplus)$.

zu ii. Für $\lambda = 0$ gilt wegen **i.** sofort $\lambda \odot \vec{0} = \vec{0}$.

Es sei nun $\lambda \neq 0$ und $\vec{v} \in V$ beliebig. Dann gilt:

$$\begin{aligned} \vec{v} = 1 \odot \vec{v} &\overset{\text{Trick}}{=} (\lambda \cdot \tfrac{1}{\lambda}) \odot \vec{v} \overset{\text{VV1}}{=} \lambda \odot (\tfrac{1}{\lambda} \odot \vec{v}) \\ &\overset{\text{Trick}}{=} \lambda \odot (\tfrac{1}{\lambda} \odot \vec{v} \oplus \vec{0}) \\ &\overset{\text{VV3}}{=} (\lambda \cdot \tfrac{1}{\lambda}) \odot \vec{v} \oplus \lambda \odot \vec{0} = \vec{v} \oplus \lambda \odot \vec{0} \end{aligned}$$

Wegen $\vec{v} = \lambda \odot \vec{0} \oplus \vec{v}$ folgt: $\lambda \odot \vec{0}$ ist das neutrale Element $\vec{0}$ der Gruppe $(V, \oplus)$.

zu iii. Den Beweis für **iii.** überlassen wir dem Leser.

zu iV. Die Richtung "$\Leftarrow$" folgt direkt aus **i.** und **ii.**.

"$\Rightarrow$": Sei $\lambda \odot \vec{v} = \vec{0}$ und gelte $\lambda \neq 0$ zu zeigen ist: Dann gilt $\vec{v} = \vec{0}$.

$$\vec{v} = 1 \odot \vec{v} \overset{\text{Trick}}{=} (\frac{1}{\lambda} \cdot \lambda) \odot \vec{v} \overset{\text{VV1}}{=} \frac{1}{\lambda} \odot (\lambda \odot \vec{v}) = \frac{1}{\lambda} \odot \vec{0} = \vec{0}$$

□

Bemerkung 3.3.8.

Begründung der scheinbar trivial-offensichtlichen Bedingung VV4
Wieso steht in **VV4** die scheinbar offensichtliche Bedingung "$1 \cdot \vec{v} = \vec{v}$"?

Lässt man **VV4** weg, so bilden Vektor-Addition und Multiplikation mit einem Skalar auf V zwei völlig voneinander losgelöste Operationen. Es wäre zum Beispiel denkbar, den uns bekannten $\mathbb{R}^2$ mit einer *"y-weglassen-Multiplikation"* der Form

$$\lambda \odot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda \cdot x \\ 0 \end{pmatrix}$$

zu versehen. Diese Form der Multiplikation erfüllt alle Regeln **VM1** und **VV1** bis **VV3** nur nicht **VV4**. Diese Dann ist aber

$$2 \odot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 0 \end{pmatrix} \quad \neq \quad \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x \\ y \end{pmatrix}.$$

Die Bedingung **VV4** stellt also sicher, dass *Vektoraddition* $+$ in V und äußere Multiplikation "sinnvoll" mit einander funktionieren.

Dank $1 \cdot \vec{v} = \vec{v}$ kann man zum Beispiel auf $2 \cdot \vec{v} = \vec{v} + \vec{v}$ schließen und entdeckt, dass die Multiplikation $\lambda \cdot \vec{v}$ *tatsächlich* das tut was man erwartet:

$$2 \cdot \vec{v} = (1+1) \cdot \vec{v} \overset{\text{VV2}}{=} 1 \cdot \vec{v} + 1 \cdot \vec{v} \overset{\text{VV4}}{=} \vec{v} + \vec{v}$$

Beispiel 3.3.9.

- Die bekannte Menge
$$\mathbb{R}^3 := \left\{ \begin{pmatrix} a \\ b \\ c \end{pmatrix} \; : \; a, b, c \in \mathbb{R} \right\}$$
bildet mit der üblichen Vektor-Addition und Skalarmultiplikation einen Vektrorraum.
- Die Menge $\mathbb{R}[x]_2 := \left\{ ax^2 + bx + c \; : \; a, b, c \in \mathbb{R} \right\}$ aller Polynome vom Grad höchstens 2 bildet einen Vektorraum zusammen mit der üblichen Addition von Polynomen und der üblichen Multiplikation mit einer Zahl. Der Nullvektor ist hier das Polynom 0 (bzw. das Polynom $0x^2 + 0x^1 + 0$).
- Die Menge *aller* reellen Polynome $\mathbb{R}[x]$ bildet einen Vektorraum mit der üblichen Addition von Polynomen und der üblichen Multiplikation mit einer Zahl. Der Nullvektor ist hier das Polynom $p(x) := 0$.
- Die Menge aller reellen Funktionen $\mathcal{C} := \{f : \mathbb{R} \to \mathbb{R}\}$ ist ein Vektorraum mit der üblichen Addition von Funktionen und der üblichen Multiplikation mit einer Zahl.

Bemerkung 3.3.10 (Notation)**.**

In den folgenden Kapiteln werden wir den Vektorpfeil, der bisher Variablen aus einem Vektorraum kennzeichnete, einsparen. Wir schreiben also für einen Vektor aus einem Vektorraum V in Zukunft $v \in V$ statt $\vec{v} \in V$.

3.3.4. Untervektorräume

Der Vektorraumbegriff gibt Anlaß zur folgenden Kennzeichung besonderer Teilmengen eines Vektorraumes V, die ebenfalls mit den Operationen + und $\cdot$ verträglich sind.

Definition 3.3.11.

Es sei V ein Vektorraum. Wir nenne eine Teilmenge $W \subset V$ *Untervektorraum* von V, falls gelten:

UV0.	$\emptyset \neq W \subset V$		
UV1.	$v + w \in W$	$\forall v, w \in W$	(Abgeschl. bez. der Addition)
UV2.	$\lambda \cdot v \in W$	$\forall \lambda \in \mathbb{K}, \forall v \in W$	(Abgeschl. bez. der Skalarmultiplikation)

Korollar 3.3.12.

Für einen Untervektorraum $W \subset V$ des Vektrorraums V gelten:

i. Es ist $0 \in W$.
ii. Für alle $v \in W$ ist auch $-v \in W$.

Beweis.

zu i. Da W nach **UV0** nicht leer ist, gibt es ein Element $v \in W$. Da ebenfalls nach **UV0** $W \subset V$ ist auch $v \in V$. Da V ein Vektorraum ist, gilt nach Korollar 3.3.7 **b) i.**, dass $0 \cdot v = 0$. Also ist nach **UV2** auch $0 \in W$.

ii. Sei $v \in W$ beliebig gewählt. Dann gilt nach **UV0** $W \subset V$ ist auch $v \in V$. Da V ein Vektorraum ist, gilt nach Korollar 3.3.7 **b) i.**, dass $-1 \cdot v = -v$. Also ist nach **UV2** auch $-v \in W$.

□

Eine Teilmenge $W \subset V$ "*erbt*" vom Vektorraum V (automatisch) die Rechenregeln.

Dies bedeutet, dass in W zum Beispiel weiterhin das Assoziativgesetz gilt, d.h. $(v+w)+z = v+(w+z)$ gilt für alle $v, w, z \in W$. Ebenso gelten auch weiterhin alle Verträglichkeitsregeln **VV1** bis **VV4** aus den Vektorraumaxiomen in W.

Bleibt nur noch die Existenz des neutralen Elements der Addition und der additiven Inversen Elemente zu zeigen. Beides folgt jedoch direkt aus Korollar 3.3.12 und es gilt

Korollar 3.3.13.

Jeder Untervektorraum ist ein Vektorraum.

Bemerkung 3.3.14.

Zu erkennen, ob eine Teilmenge $W \subset V$ ein Untervektorraum eines Vektorraumes V ist, erfordert also per Definition zu prüfen, ob W abgeschlossen ist unter Addition und skalarer Multiplikation. Ein erster Anhaltspunkt ist das "Enthaltensein der Null":

Gilt $0 \notin W$ so ist W *kein* Vektorraum und damit auch kein Untervektorraum.

Beispiel 3.3.15.

- Der Vektorraum $\mathbb{R} = \mathbb{R}^1$ hat nur zwei Untervektorräume: sich selbst und die Menge $\{0\}$, die nur den Nullvektor enthält.
- Die Untervektorräume von $\mathbb{R}^2$ sind genau

- die Menge $\{0\}$,
- alle Mengen der Form $V_a = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \ : \ y = a \cdot x \right\}$ mit $a \in \mathbb{R}$,
- die Menge $V_\infty = \left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} \ : \ y \in \mathbb{R} \right\}$ und
- der gesamte Vektorraum $\mathbb{R}^2$ selbst.

Geometrisch ist eine Menge V_a mit festem a eine Gerade durch den Ursprung $0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (genauso auch V_∞).

► Die Untervektorräume des $\mathbb{R}^3$ sind entsprechend die Mengen $\{0\}$ und $\mathbb{R}^3$ selbst sowie die Geraden und Ebenen durch 0.

Teil II.

Lineare Algebra

4 Lineare Abbildungen

Wir kommen nun zum Hauptbegriff, um den sich der erste Teil der Vorlesung dreht.

Die Beispiele in 3.3.9 sehen sich überraschend ähnlich und auch die Operationen (Addition und skalare Multiplikation) laufen weitestgehend gleich ab:

$$\begin{array}{rcccc} & (ax^2 & +bx & +c) \\ + & (\alpha x^2 & +\beta x & +\gamma) \\ \hline + & ((a+\alpha)x^2 & +(b+\beta)x & +(c+\gamma)) \end{array} \quad \left| \quad \begin{pmatrix} a \\ b \\ c \end{pmatrix} + \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} a+\alpha \\ b+\beta \\ c+\gamma \end{pmatrix} \right.$$

Der Vektorraum $\mathbb{R}[x]_2$ ist also quasi nichts anderes als ein "hingelegter" $\mathbb{R}^3$, die Koeffizienten der Polynome benehmen sich identisch zu den Koeffizienten der Vektoren des $\mathbb{R}^3$. Den $\mathbb{R}[x]_2$ als Vektorraum zu betrachten bringt also auch im Sinne von Vektorräumen nichts wirklich neues. Den Umstand, dass diese Vektorräume die gleiche Form haben, werden wir in Definition 4.1.5 abstrakt fassen, nachdem wir in diesem Kapitel Abbildungen zwischen Vektorräumen eingeführt haben.

4.1. Lineare Abbildungen von Vektorräumen

Definition 4.1.1.

Seien V, V' Vektorräume. Eine Abbildung $f : V \to V'$ heißt linear, falls sie die folgenden Bedingungen erfüllt.

L1.	$f(v+w)$	$=$	$f(v)+f(w)$	$\forall v, w \in V$	("Additivität")
L2.	$f(\lambda \cdot v)$	$=$	$\lambda \cdot f(v)$	$\forall v \in V, \lambda \in \mathbb{K}$	("Homogenität")

Salopp gesagt ist eine Abbildung f also linear, wenn man f mit $+$ und $\cdot$ "vertauschen kann". Es gibt einige offensichtliche Beispiele linearer Abbildungen. Für je zwei Vektorräume V, V' ist die Abbildung $f : V \to V', v \mapsto 0$, die also alle Vektoren auf den Nullvektor abbildet, linear. Außerdem ist für jeden Vektorraum V die Abbildung $id : V \to V, v \mapsto v$, die einfach v auf sich selbst abbildet, linear. Ist allgemeiner λ eine reelle Zahl, so ist die Abbildung $f_\lambda : V \to V : v \mapsto \lambda \cdot v$ linear. Kommen wir zu einigen vielleicht weniger offensichtlichen Beispielen.

Beispiel 4.1.2.

- Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -y \end{pmatrix}$ ist, geometrisch gesprochen, die Spiegelung an der x-Achse.
- Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -y \\ x \end{pmatrix}$ ist die Rotation um $90°$.
- Allgemeiner ist $f : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos(\alpha)x - \sin(\alpha)y \\ \sin(\alpha)x + \cos(\alpha)y \end{pmatrix}$ die Rotation um den Winkel α.

Aus gegebenen linearen Abbildungen kann man neue basteln. Für eine lineare Abbildung $f : V \to V'$ und $\lambda \in \mathbb{K}$ definieren wir eine neue Abbildung $\lambda \cdot f : V \to V'$ durch $x \mapsto \lambda \cdot f(x)$. Außerdem definieren wir für lineare $f, g : V \to V'$ die Abbildung $f + g : V \to V'$ durch $x \mapsto f(x) + g(x)$.

Korollar 4.1.3.

Seien $f, g : V \to V'$ und $h : V' \to V''$ lineare Abbildungen.

i. Für jede Zahl $\lambda \in \mathbb{K}$ ist $\lambda \cdot f$ linear.
ii. Die Abbildung $f + g$ ist linear.
iii. Die Abbildung $h \circ f : V \to V''$ ist linear.

Beweis. Man rechnet die Eigenschaften **L1** und **L2** nach. Details werden dem Leser überlassen. □

Proposition 4.1.4.

Sei $f : V \to V'$ eine bijektive lineare Abbildung. Dann ist auch ihre Umkehrabbildung $f^{-1} : V \to V'$ linear.

Beweis. Seien $v', w' \in V'$ Vektoren. Dann gibt es $v, v \in V$ mit $v' = f(v)$ und $w = f(w)$. Weil f linear ist, gilt also $v' + w' = f(v + w)$. Weil f außerdem bijektiv ist, folgt

$$f^{-1}(v' + w') = f^{-1}(f(v + w)) = v + w = f^{-1}(v) + f^{-1}(w).$$

Ist ferner $\lambda \in \mathbb{K}$, so gilt

$$f^{-1}(\lambda \cdot v') = f^{-1}(\lambda \cdot f(v)) = \lambda \cdot v = \lambda \cdot f^{-1}(v).$$

Also erfüllt f^{-1} die Bedingungen **L1** und **L2**. □

Lineare Abbildungen werden auch oft als ***Homomorphismen*** bezeichnet. Eine bijektive lineare Abbildung heißt ein ***Isomorphismus***.

Definition 4.1.5.

Zwei Vektorräume V und V' heißen *isomorph*[1], wenn es eine *bijektive* linear Abbildung (Isomorphismus) von V nach V' gibt.

Beispiel 4.1.6.

Die Vektorräume $(\mathbb{R}^3, +, \cdot)$ und $(R[x]_2, \ + \ , \ \cdot \ )$ sind isomorph, der Isomorphismus lautet:

$$f : \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto ax^2 + bx + c$$

5 Basen und Dimension

Bis auf weiteres sprechen wir von einem Vektorraum über einem Körper $\mathbb{K}$, wenn nicht anders angegeben.

5.1. Lineare Unabhängigkeit

Wir führen ein Maß für die Größe eines Vektorraums ein, die *Dimension*. Die Dimension ist grob gesagt ein Maß für die Bewegungsmöglichkeiten in einem Vektorraum, sogenannte Freiheitsgrade.

Motivation 5.1.1.

Es ist leicht zu sehen, dass man für die Wahl eines Punktes im $\mathbb{R}^3$ drei Freiheitsgrade hat, während es für einen Punkt im $\mathbb{R}^2$ nur zwei Freiheitsgrade sind. Dies hat direkte Konsequenzen beim Bau von ferngesteuertem Spielzeug:

- Eine Spielzeugeisenbahn muss nur vor oder zurück fahren. Mathematisch gesehen fährt die Lok auf einer Geraden, hat also nur einen Freiheitsgrad und benötigt deswegen auch nur einen Motor.
- Ein Modellauto dagegen benötigt mindestens *zwei Kontrollmöglichkeiten*, weil es sich abstrakt gesehen im $\mathbb{R}^2$ (alias "der Fußboden") frei bewegen können muss.
- Ein Modellflugzeug muss mindestens *drei Kontrollmöglichkeiten* besitzen, weil es sich frei im $\mathbb{R}^3$ bewegen können muss.

Um die Dimension definieren zu können müssen wir zunächst definieren, was es bedeutet "mit bestimmten Laufrichtungen mittels Vektoren durch einen von den Vektoren aufgespannten Raum zu laufen". Dazu definieren wir:

Definition 5.1.2.

Es seien $v_1, \ldots, v_k \in V$ Vektoren in einem Vektorraum V.

Eine Summe der Form $\mu_1 \cdot v_1 + \ldots + \mu_k \cdot v_k$ mit $\mu_1, \ldots, \mu_k \in \mathbb{K}$ nennt man *eine Linearkombination* der Vektoren $v_i, \ldots, v_k$. Die Menge aller Linearkombinationen dieser Vektoren nennt man den Spann von $v_1, \ldots, v_k$ bezeichnet mit

$$\mathsf{span}(v_1, \ldots, v_k) := \left\{ \sum_{i=1}^{k} \mu_i v_i \quad : \quad \mu_1, \ldots, \mu_k \in \mathbb{R} \right\}.$$

Es ist $\mathsf{span}(\emptyset) = \{0\}$.

Anschauung 5.1.3.

Die Addition von Vektoren entspricht dem "Hintereinanderhängen" der entsprechenden Vektoren. Geometrisch ist eine Linearkombination $\mu_1 \cdot v_1 + \ldots + \mu_k \cdot v_k$ also eine "Laufanweisung" der Form "Folge dem Vektor v_1, dann v_2 etc. ". Dabei geben die μ_i jeweils (grob gesagt) an, wie weit jeweils zu laufen ist.

Der Spann ist dann die Menge an Punkten, die über solche Laufwege erreichbar ist.

Beispiel 5.1.4.

- Für die Vektoren $v_1 := \begin{pmatrix}1\\0\\0\end{pmatrix}, v_2 := \begin{pmatrix}0\\1\\0\end{pmatrix}$ ist der Spann:

$$\mathsf{span}(v_1, v_2) := \left\{ \mu_1 \begin{pmatrix}1\\0\\0\end{pmatrix} + \mu_2 \begin{pmatrix}0\\1\\0\end{pmatrix} \;:\; \mu_1, \mu_2 \in \mathbb{R} \right\} = \left\{ \begin{pmatrix}\mu_1\\\mu_2\\0\end{pmatrix} \;:\; \mu_1, \mu_2 \in \mathbb{R} \right\}$$

- Fügt man den Vektor $v_3 = \begin{pmatrix}1\\1\\0\end{pmatrix}$ hinzu, ändert sich der Spann nicht, da sich v_3 bereits als Summe von v_1 und v_2 schreiben lässt (Die "Zutat" v_3 liefert also keine "echt neue" Laufrichtung, das Verwenden von v_3 lässt sich durch das Verwenden von v_1 und v_2 ersetzen:

$$\begin{aligned}\mathsf{span}(v_1, v_2, v_3) &:= \left\{ \mu_1 \begin{pmatrix}1\\0\\0\end{pmatrix} + \mu_2 \begin{pmatrix}0\\1\\0\end{pmatrix} + \mu_3 \begin{pmatrix}1\\1\\0\end{pmatrix} \;:\; \mu_1, \mu_2, \mu_3 \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix}\mu_1+\mu_3\\\mu_2+\mu_3\\0\end{pmatrix} \;:\; \mu_1, \mu_2, \mu_3 \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix}x\\y\\0\end{pmatrix} \;:\; x, y \in \mathbb{R} \right\}\end{aligned}$$

  Um das letzte Gleichheitszeichen einzusehen macht man sich klar, dass hier "$\subset$" stets gilt: Die letzte Menge enthält *alle* Vektoren mit drittem Eintrag 0 (und jeder Vektor der vorletzten Menge ist ein solcher). Umgekehrt gilt: Ist $w := \begin{pmatrix}x\\y\\0\end{pmatrix}$ ein beliebiger Vektor mit $x, y \in \mathbb{R}$, so ist w auch ein Element der vorletzten Menge: Setze im Vektor $\begin{pmatrix}\mu_1+\mu_3\\\mu_2+\mu_3\\0\end{pmatrix}$ einfach $\mu_1 = x$, $\mu_2 = y$, $\mu_3 = 0$ und erhalte w.

Das letzte Beispiel zeigt: Geht es darum eine Menge als Spann von Vektoren zu beschreiben, so ist es nicht hilfreich "überflüssige" Vektoren zu verwenden. Um solche Mengen von Vektoren zu vermeiden, führen wir den folgenden Begriff ein (das Lemma 5.1.8 klärt dann, was dieser für den Spann bedeutet):

Definition 5.1.5.

Eine Menge von Vektoren $\{v_1, \ldots, v_k\} \subset V$ in einem Vektorraum V heißt *linear **un**abhängig* falls gilt:

$$\mu_1 \cdot v_1 + \ldots + \mu_k \cdot v_k = 0 \quad \Rightarrow \quad \mu_1 = \mu_2 = \ldots = \mu_k = 0$$

Gilt dies nicht, nennt man die Vektoren *linear abhängig* (oder auch kurz abhängig).

Bemerkung 5.1.6.

ür die Gleichung $\mu_1 \cdot v_1 + \ldots + \mu_k \cdot v_k = 0$ ist $\mu_1 = \ldots = \mu_k = 0$ *immer* eine Lösung, es kann aber noch weitere Lösungen geben. Die Vektoren $\{v_1, \ldots, v_k\}$ sind also linear unabhängig, wenn $\mu_1 = \mu_2 = \ldots = \mu_k = 0$ die *einzige* Lösung der Gleichung $\mu_1 \cdot v_1 + \ldots + \mu_k \cdot v_k = 0$ ist.

Beispiel 5.1.7.

- Die Vektoren $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^3$ sind linear **un**abhängig, denn:

$$\mu_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mu_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \mu_3 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = 0 \quad \Leftrightarrow \quad \begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad \mu_1 = \mu_2 = \mu_3 = 0$$

- Die Vektoren $v_1 := \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, v_2 := \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, v_3 := \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3$ sind linear **ab**hhängig, denn es gilt:

$$1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

- In jedem Vektorraum V gilt:
  Die Menge $\{0\} \subset V$ ist linear **ab**hängig, denn für $\lambda_1 \cdot 0 = 0$ ist jedes $\lambda_1 \in \mathbb{R}$ eine Lösung.
  Ganz genauso ist jede andere Menge der Form $\{0, v_1, \ldots, v_k\} \subset V$ linear abhängig.

In einer Menge von linear **ab**hängigen Vektoren ist beim Bilden des Spanns immer (mindestens) ein Vektor überflüssig, weil er sich aus den anderen herstellen lässt:

Lemma 5.1.8.

Die Vektoren $\{v_1, \ldots, v_k\}$ sind genau dann linear **ab**hängig, wenn es einen Vektor $v_j \in \{v_1, \ldots, v_k\}$ gibt, der sich als Linearkombination der anderen Vektoren schreiben lässt, wenn also gilt:

$$\exists \mu_1, \ldots, \mu_{j-1}, \ \mu_{j+1}, \ldots \mu_k \in \mathbb{K} \ : \ v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} \mu_i v_i \tag{5.1}$$

Beweis.

"⇒" Annahme: Die Vektoren $v_1, \ldots, v_k$ seien linear **ab**hängig. Dann hat $\sum_{i=1}^{k} \lambda_i v_i = 0$ mehr als nur die triviale Lösung $\lambda_1 = \ldots = \lambda_k = 0$, d.h. eine Lösung mit mindestens einem $\lambda_j \neq 0$. Es gilt also:

$$\lambda_j \cdot v_j + \sum_{\substack{i=1 \\ i \neq j}}^{k} \lambda_i v_i = 0 \quad \Longrightarrow \quad v_j = \sum_{\substack{i=1 \\ i \neq j}}^{k} \frac{-\lambda_i}{\lambda_j} \cdot v_i$$

Setzt man nun $\mu_i := \frac{-\lambda_i}{\lambda_j}$ für alle $i \in \{1, \ldots, k\} \setminus \{j\}$, so hat man die gewünschte Darstellung von v_j.

"⇐" Annahme: Es gilt (5.1), d.h. $v_j = \sum_{\substack{i=1 \\ i \neq j}}^{k} \mu_i \cdot v_i$ mit $\mu_i \in \mathbb{K}$. Setzt man zusätzlich $\mu_j := -1$ so gilt:

$$v_j = \sum_{\substack{i=1 \\ i \neq j}}^{k} \mu_i \cdot v_i \quad \Longrightarrow \quad 0 = -v_j + \sum_{\substack{i=1 \\ i \neq j}}^{k} \mu_i \cdot v_i \quad \Longrightarrow \quad 0 = \sum_{i=1}^{k} \mu_i \cdot v_i \quad \text{mit } \mu_j \neq 0$$

Die Gleichung $\sum_i^k \mu_i v_i = 0$ hat also mehr als nur die Lösung $\mu_1 = \ldots = \mu_k = 0$, die Vektoren sind also linear **ab**hängig.

□

Beispiel 5.1.9.

- Die Vektoren $v_1 := \begin{pmatrix}1\\0\\0\end{pmatrix}, v_2 := \begin{pmatrix}0\\1\\0\end{pmatrix}, v_3 := \begin{pmatrix}0\\0\\1\end{pmatrix}, v_4 := \begin{pmatrix}5\\7\\0\end{pmatrix}$ aus $\mathbb{R}^3$ sind linear **ab**hängig, denn es gilt $v_4 = 5 \cdot v_1 + 7 \cdot v_2$.
- Es sei $\mathbb{R}[x]$ der Vektorraum aller Polynome. Die Vektoren $p_1 := x$, $p_2 := x^2 + x$, $p_3 := x^2 + 5x$ aus $\mathbb{R}[x]$ sind linear abhängig, denn es gilt $p_3 = 4 \cdot p_1 + p_2$.

Exkurs 5.1.10 (Lineare Unabhängigkeit)**.**

Betrachtet man Lemma 5.1.8 so bedeutet "$v_1, \ldots v_k$ sind linear unabhängig", dass *kein* Vektor aus der Menge $\{v_1, \ldots, v_k\}$ durch die anderen "hergestellt" werden kann.

Frage: Wieso verwendet man dies nicht als Definition für den Begriff "linear unabhängig"?

Antwort: Man verwendet dies nicht als Definition, weil diese Aussage kein praktisches Prüfkriterium bietet: Um zu Zeigen, dass $v_1, \ldots v_k$ linear **un**abhängig sind, müsste man für jeden der k Vektoren ein eigenes lineares Gleichungssystem aufstellen und zeigen, dass *jedes* davon unlösbar ist.

5.2. Basis

Der Kernbegriff den wir benötigen, um die Dimension eines Vektorraums zu definieren ist der einer Basis.

Definition 5.2.1.

Seien $v_1, \ldots, v_n \in V$ Vektoren in einem Vektorraum V. Wir nennen $\{v_1, \ldots, v_n\}$ eine ***Basis*** von V, wenn erfüllt sind:

B1. Die Vektoren $\{v_1, \ldots, v_n\}$ sind linear unabhängig.
B2. $V = \mathsf{span}(v_1, \ldots, v_n)$.

Geometrisch bedeutet dies: Mit den "Laufrichtungen" v_i kann man jeden Punkt in V erreichen, und die "Wegbeschreibung" ist eindeutig:

Proposition 5.2.2.

Ist $\{v_1, \ldots, v_n\}$ eine Basis des Vektorraums V, so gibt es zu jedem Vektor $w \in V$ *genau ein* n-tupel $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit $w = \sum_{i=1}^n \lambda_i \cdot v_i$.

Beweis. Es sei $\{v_1, \dots, v_n\}$ eine Basis des Vektorraums V und sei $w \in V$ beliebig. Wegen $V = \mathsf{span}(v_1, \dots, v_n)$ gibt es (mindestens) ein Tupel $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ mit

$$w = \sum_{i=1}^{n} \lambda_i \cdot v_i.$$

Nehmen wir nun an, es gäbe noch ein anderes n-Tupel $\mu_1, \dots, \mu_n \in \mathbb{K}$ für welches $w = \sum_{i=1}^{n} \mu_i \cdot v_i$ ist, dann gilt:

$$0 = w - w = \sum_{i=1}^{n} (\lambda_i - \mu_i) \cdot v_i$$

Weil nach **B1** die Vektoren $v_1, \dots, v_n$ linear **un**abhängig sind, *muss* $\lambda_i - \mu_i = 0$ für alle $i \in \{1, \dots n\}$ gelten, d.h. die beiden n-Tupel sind identisch, ein Widerspuch zur Annahme, dass $\mu_1, \dots, \mu_n$ ein anderes n-Tupel als $\lambda_1, \dots, \lambda_n$ sei. □

Proposition 5.2.3.

Seien $v_1, \dots, v_n \in V$ Vektoren in einem Vektorraum V. Dann ist $\mathsf{span}(v_1, \dots, v_n)$ ein Vektorraum.

Beweis. Übungsaufgabe. □

Definition 5.2.4.

Es sei $\mathbb{K}^n$ der Vektorraum, der von den n ***Einheitsvektoren***

$$e^{(1)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e^{(2)} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e^{(n)} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

aufgespannt wird.

5.2.1. Dimension

Wir würden gerne die Dimension eines Vektorraums V definieren als die Anzahl der Vektoren in einer Basis von V. Dazu müssen wir uns allerdings noch zwei Dinge überlegen:

- Jeder Vektorraum hat eine Basis.
- Alle Basen bestehen aus gleichvielen Vektoren.

Dazu benötigen wir die beiden Sätze

Satz 5.2.5.

Sind $v_1, \dots, v_n$ und $w_1, \dots, v_k$ Basen des Vektorraums V, so gilt: $k = n$.

Satz 5.2.5 folgt direkt aus Lemma 5.2.11, dessen Beweis ist allerdings etwas technisch, weswegen wir ihn am Ende dieses Abschnittes führen. Satz 5.2.5 motiviert die folgende Definition:

Definition 5.2.6.

Hat ein Vektorraum V eine Basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ mit $n \in \mathbb{N}$ so sagt man die Dimension von V ist n. Ist es nicht möglich, eine (endliche) Basis von V zu finden, so sagt man die Dimension von V ist unendlich.

Beispiel 5.2.7.

- Die Menge
$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$
ist eine Basis des $\mathbb{R}^3$,
d.h. der Vektorraum $\mathbb{R}^3$ hat die Dimension 3.
- Die Menge $\left\{1, x, x^2\right\}$ ist eine Basis von $\mathbb{R}[x]_2 := \left\{ax^2 + bx + c \ : \ a, b, c \in \mathbb{R}\right\}$,
d.h. der Vektorraum $\mathbb{R}[x]_2$ hat die Dimension 3.
- Die Menge $\mathbb{R}[x]$ aller Polynome ist ein Vektorraum, der *keine* endliche Basis besitzt,
d.h. der Vektorraum $\mathbb{R}[x]$ hat die Dimension unendlich.

Folgender Satz lässt sich mit einem Gedicht von James Whitcomb Riley umschreiben:

“When I see a bird that walks like a duck and swims like a duck and quacks like a duck, I call that bird a duck.”

(Wenn ich einen Vogel sehe, der wie eine Ente läuft, wie eine Ente schwimmt und wie eine Ente schnattert, dann nenne ich diesen Vogel eine Ente.)

Satz 5.2.8.

Jeder n-dimensionale Vektorraum ist isomorph zu $\mathbb{R}^n$ (wobei $n \in \mathbb{N}$).

Beweis. Es sei V ein n-dimensionaler Vektorraum, dann besitzt V eine Basis $\{v_1, \ldots, v_n\}$. Zu jedem Vektor $w \in V$ gibt es genau ein n-Tupel $(a_{w,1}, \ldots, a_{w,n}) \in \mathbb{R}^n$ mit $w = a_{1,w}v_1 + \ldots + a_{n,w}v_n$.

Die Abbildung $f : V \to \mathbb{R}^n$ mit $w \mapsto f(w) := (a_{w,1}, \ldots, a_{w,n})$ ist bijektiv:

Injektivität: Klar ist - Für $w \neq \widetilde{w}$ ist $(a_{w,1}, \ldots, a_{w,n}) \neq (a_{\widetilde{w},1}, \ldots, a_{\widetilde{w},n})$.

Surjektivität: Umgekehrt gilt - Für jeden Vektor $a \in \mathbb{R}^n$ ist $u := a_1v_1 + \ldots + a_nv_n$ ein Vektor mit $u \in V$ und $f(u) = a$.

□

Bemerkung 5.2.9 (Basis des Nullvektorraums”)**.**

Der ***Nullvektorraum*** besteht nur aus dem Nullvektor 0 und hat eine leere Basis. Nach Beispiel 5.1.7 ist nämlich die Menge bestehend alleine aus dem Nullvektor $\{0\}$ nicht linear unabhängig. Nach der Definition gilt $\mathsf{span}(\emptyset) = \{0\}$.

5.2.2. Basisaustauschsätze

Die folgenden zwei Lemmata sind von Ihren Aussagen nur scheinbar rein technische Hilfssätze. Das Lemma 5.2.11 zeigt insbesondere:

- dass es Sinn macht von "n-dimensionalen" Vektorräumen zu sprechen und
- dass im n-dimensionalen Vektorraum eine Menge von linear unabhängigen Vektoren höchstens n Elemente haben kann.

Insgesamt beweist Lemma 5.2.11 den Satz 5.2.5.

Lemma 5.2.10.

Sei $\{v_1, \ldots, v_k\}$ eine Basis des Vektorraumes V, und $z = a_1 v_1 + \ldots + a_k v_k$ eine Linearkombination mit $a_j \neq 0$. Dann ist auch $\{v_1, \ldots, v_{j-1}, z, v_{j+1}, \ldots, v_n\}$ eine Basis von V.

Beweis. Nach Umnummerierung der v_i dürfen wir annehmen, dass in $z = a_1 v_1 + \ldots + a_k v_k$ gilt: $a_1 \neq 0$.

Wir zeigen, dass in diesem Fall $\{z, v_2, \ldots, v_k\}$ eine Basis von V ist:

- **Lineare Unabhängigkeit:** Angenommen es gäbe Zahlen $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ so dass gilt

$$\lambda_1 z + \lambda_2 v_2 + \ldots + \lambda_k v_k = 0.$$

  Setzt man hier $\lambda_1 z = \lambda_1 a_1 v_1 + \ldots + \lambda_1 a_k v_k$ ein, so erhält man

$$\lambda_1 a_1 v_1 + (\lambda_2 + \lambda_1 a_2) v_2 + \ldots + (\lambda_k + \lambda_1 a_k) v_k = 0.$$

  Da $\{v_1, \ldots v_k\}$ linear unabhängig sind, sind hier alle Koeffizienten Null, d.h. insbesondere gilt $\lambda_1 a_1 = 0$. Wegen der Annahme $a_1 \neq 0$ folgt sofort $\lambda_1 = 0$, und dies liefert

$$\lambda_2 v_2 + \ldots + \lambda_k v_k = 0.$$

  und damit $\lambda_2 = \ldots = \lambda_k = 0$, da $\{v_1, \ldots v_k\}$ linear unabhängig sind. Folglich sind $\{z, v_1, \ldots, v_k\}$ linear unabhängig.
- **Spann ist ganz V:** Es gibt Zahlen $c_1, \ldots, c_k \in \mathbb{K}$ mit $v_1 = c_1 z + c_2 v_2 + \ldots + c_k v_k$, denn löst man $z = a_1 v_1 + a_2 v_2 + \ldots a_k v_k$ nach v_1 auf, so erhält man

$$v_1 = \frac{1}{a_1} z - \frac{a_2}{a_1} v_2 - \ldots - \frac{a_k}{a_1} v_k.$$

  Da $\{v_1, \ldots, v_k\}$ eine Basis von V ist, lässt sich jedes $w \in V$ darstellen als Linearkombination:

$$w = \mu_1 v_1 + \mu_2 v_2 \ldots + \mu_k v_k \quad \text{mit } \mu_1, \ldots \mu_k \in \mathbb{K}$$

  Ersetzt man hier $v_1 = c_1 z + c_2 v_2 + \ldots + c_k v_k$, so erhält man für w eine Linearkombination aus $z, v_2, \ldots v_k$, nämlich

$$w = \mu_1 (c_1 z + c_2 v_2 + \ldots + c_k v_k) + \mu_2 v_2 \ldots + \mu_k v_k.$$

  Es gilt also $w \in \mathsf{span}(z, v_2, \ldots v_k)$.

□

Lemma 5.2.11 (Basisaustauschsatz von Steinitz)**.**

Es seien $\{w_1, \ldots, w_k\} \subset V$ linear unabhängig und es sei $\{v_1, \ldots, v_n\}$ eine Basis von V.

Dann gilt $k \leq n$, und es gibt $n-k$ paarweise verschiedene $\widetilde{v}_{k+1}, \ldots, \widetilde{v}_n \in \{v_1, \ldots, v_k\}$, so dass gilt:

$$\{\, w_1, \ldots, w_k,\ \ \widetilde{v}_{k+1}, \ldots, \widetilde{v}_n \,\} \quad \text{ist eine Basis von } V$$

Beweis. Wir führen eine Induktion über k, beginnend bei $k = 1$.

Induktionsverankerung: Es sei $\{w_1\}$ linear unabhängig. Der Vektor w_1 lässt sich darstellen als $w_1 = a_1 v_1 + \ldots + a_n v_n$ mit $a_1, \ldots, a_n \in \mathbb{R}$. Es gilt $w_1 \neq 0$, weil $\{w_1\}$ linear unabhängig ist. Also gibt es ein $a_i \neq 0$. Lemma 5.2.10 beweist: $\{v_1, \ldots, v_{i-1}, w_1, v_{i+1}, \ldots v_k\}$ ist eine Basis.

Induktionsannahme: Die Aussage gelte für ein ℓ mit $1 \leq \ell$.

Induktionsschluss: Es sei $\{w_1, \ldots, w_\ell, w_{\ell+1}\}$ linear unabhängig, entsprechend sind $\{w_1, \ldots, w_\ell\}$ linear unabhängig. Nach Induktionsannahme gibt es $u_i \in \{v_1, \ldots, v_n\}$, so dass $\{w_1, \ldots w_\ell,\ \ u_{\ell+1}, \ldots, u_n\}$ eine Basis von V ist. Insbesondere lässt sich der Vektor $w_{\ell+1}$ darstellen als

$$w_{\ell+1} = a_1 w_1 + \ldots + a_\ell w_\ell \ \ + \ \ b_{\ell+1} u_{\ell+1} + \ldots + b_n u_n$$

Da $\{w_1, \ldots, w_\ell, w_{\ell+1}\}$ linear unabhängig sind, ist $w_{\ell+1}$ *keine* Linearkombination der restlichen w_i nach Lemma 5.1.8. D.h. es gibt ein $j \geq \ell + 1$ mit $b_j \neq 0$.

Nummeriert man die Vektoren u_i so, dass $b_{k+1} \neq 0$ gilt, so zeigt Lemma 5.2.10, dass

$$\{w_1, \ldots w_\ell,\ \ w_{\ell+1},\ u_{\ell+2}, \ldots, u_n\}$$

eine Basis von V ist.

Es bleibt zu zeigen: $k \leq n$. Dazu nehmen wir an, es seien $W := \{w_1, \ldots, w_k\} \subset V$ linear unabhängig. Per Induktion haben wir bewiesen: Weil die Vektoren in W linear **un**abhängig sind, lässt sich W zu einer Basis der Länge n *auffüllen*[2] . Es folgt also insbesondere $|W| \leq n$, d.h. es folgt $k \leq n$. □

Bemerkung 5.2.12.

Frage: Eine Induktion über k welches beschränkt wird?!
Eine Induktion über k beweist doch eine Aussage für *alle* $k \in \mathbb{N}$. Hier kommt im zweiten Teil des Beweises aber eine Einschränkung $k < n$. Geht das überhaupt?

Antwort: Die Induktion beweist eine "Wenn-Dann-Aussage", deren "Wenn-Teil" für $k > n$ einfach nicht mehr eintritt:

"*Wenn* $W := \{w_1, \ldots w_k\}$ linear unabhängig sind,

dann lässt sich W zu einer Basis der Länge n ergänzen."

Diese "Wenn-Dann-Aussage" ist *tatsächlich* richtig für *alle* $k \in \mathbb{N}$, und das beweist die Induktion.

Allerdings gibt es einen kleinen "Twist": Die Aussage gilt ab $k > n$ *trivialerweise*, weil die Voraussetzung

"$\{w_1, \dots w_k\}$ ist linear unabhängig" unerfüllbar (also immer falsch) ist. Dies ist dann die Aussage des zweiten Teils des Beweises:

Ab $k > n$ gilt für eine Menge mit k-vielen Vektoren: Die Vektoren sind *nicht* linear unabhängig.

Lemma 5.2.11 beweist also:

- für $1 \leq k \leq n-1$:
  Eine (tatsächlich) linear unabhängige Menge $W = \{w_1, \dots w_k\}$ lässt sich *tatsächlich* zu einer Basis der Länge n auffüllen.
- für $k = n$:
  Eine (tatsächlich) linear unabhängige Menge $W = \{w_1, \dots w_n\}$ *ist bereits* eine Basis der Länge n, denn "zu einer Basis der Länge n auffüllen" bedeutet hier: *keinen* Vektor aus $\{v_1, \dots, v_n\}$ dazufügen, weil die Länge n bereits erreicht ist.
- für $k > n$:
  Jede *hypothetisch* linear unabhängige Menge $W = \{w_1, \dots w_k\}$, *ließe* sich zu einer Basis der Länge n auffüllen. Da W aber schon mehr als n Elemente hat, kann dies nicht gehen, d.h. es gibt solche Mengen W nicht.

6 Matrizen

6.1. Einführung

Im den vorherigen Abschnitten haben wir gezeigt, dass ein endlich-dimensionaler $\mathbb{K}$-Vektorraum V stets isomorph ist zu einem $\mathbb{K}^n$. Wir verlassen nun jedoch die Welt der allgemeinen Vektorräume und werden von nun an nur noch Vektorräume über den reelen Zahlen $\mathbb{R}$ betrachten. Viele der Aussagen, die wir treffen werdem, gelten auch für allgemeine Vektorräume.

Im Folgenden werden wir uns dennoch vorerst mit linearen Abbildungen der Form $f : \mathbb{R}^n \to \mathbb{R}^m$ beschäftigen. Diese linearen Abbildungen lassen sich sehr kurz und knapp durch eine Matrix beschreiben.

Definition 6.1.1 (Allgemeine Form einer Matrix)**.**

Sei S eine Menge. Eine $m \times n$-Matrix (sprich „m-Kreuz-n-Matrix“) A ist eine Abbildung

$$A : \{1, \dots, m\} \times \{1, \dots, n\} \to S, \qquad (i, j) \mapsto A_{ij}.$$

Die Menge aller $m \times n$-Matrizen bezeichnen wir mit $S^{n \times n}$.

- Wir schreiben eine Matrix in der Form

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & A_{1,3} & \cdots & A_{1,\mathbf{n}} \\ A_{2,1} & A_{2,2} & A_{2,3} & \cdots & A_{2,\mathbf{n}} \\ A_{3,1} & A_{3,2} & A_{3,3} & \cdots & A_{3,\mathbf{n}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{\mathbf{m},1} & A_{\mathbf{m},2} & A_{\mathbf{m},3} & \cdots & A_{\mathbf{m},\mathbf{n}} \end{pmatrix}.$$

- Wir nennen das n-Tupel $A_{(i)} = (A_{i1}, \dots, A_{in})$ die ***i-te Zeile*** von A.
- Entsprechend heißt der Vektor

$$A^{(j)} = \begin{pmatrix} A_{1j} \\ \vdots \\ A_{mj} \end{pmatrix}$$

  die ***j-te Spalte*** von A.
- Die einzelnen Zahlen A_{ij} heißen die ***Einträge*** von A.
- Falls $m = n$, nennen wir M eine ***quadratische*** Matrix.

Sage-Box (Matrix)**.**

- Alternative I

```
sage: A = Matrix([[1,2,3],[3,2,1]])
sage: A
[1 2 3]
[3 2 1]
```

- Alternative II

```
sage: M = MatrixSpace(QQ,2,3)
sage: # MatrixSpace - Menge von Matrizen - Erstes Argument: Die den
Einträgen der Matrix zugrundeliegende Menge - Zweites Argument: Anzahl
der Zeilen - Drittes Argument: Anzahl der Spalten
sage: A = M([1,2,3,3,2,1])
[1 2 3]
[3 2 1]
```

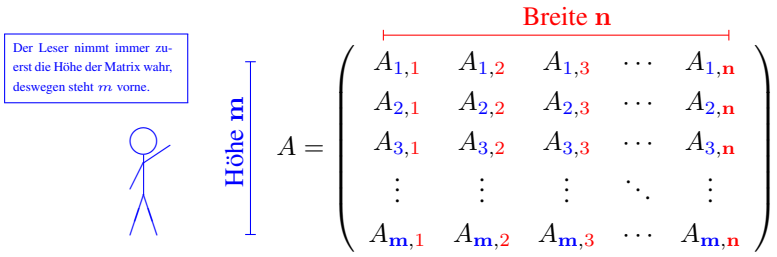
Bemerkung 6.1.2 (Matrizen (Einzahl: *Matrix*))**.**

In den folgenden Kapiteln wird die Menge S die Menge der reellen Zaheln $\mathbb{R}$ sein.

Matrizen sind ein Schlüsselkonzept der linearen Algebra und tauchen in fast allen Gebieten der Mathematik auf. Dabei stellen sie Zusammenhänge, in denen Linearkombinationen eine Rolle spielen, übersichtlich dar und werden insbesondere benutzt, um lineare Abbildungen darzustellen.

Eine *Matrix* $A \in \mathbb{R}^{m\times n}$ ist grob gesagt eine Tabelle von m mal n Zahlen, die in einem rechteckigen Schema von m Zeilen und n Spalten angeordnet sind. In $A \in \mathbb{R}^{\mathbf{m}\times\mathbf{n}}$ steht die erste Dimensions-Variable „m“ für die **Höhe** der Matrix. Dies kann man sich merken, indem man sich vorstellt, dass ein (virtueller) Leser, der von links nach rechts „angelaufen kommt“ immer zuerst die Höhe der Matrix wahrnimmt.

Eine $\mathbf{m}\times\mathbf{n}$-Matrix $A \in \mathbb{R}^{\mathbf{m}\times\mathbf{n}}$ ist also ein Zahlenschema mit $\mathbf{m}$ Zeilen und $\mathbf{n}$ Spalten. Dabei ist $A_{ij} \in \mathbb{R}$ jeweils den Eintrag in der i-ten Zeile und der j-ten Spalte:



Die Einträge $A_{ij} \in \mathbb{R}$ einer Matrix können beliebige Zahlen aus $\mathbb{R}$ sein, es ist aber unzulässig eine Position leer zu lassen.

Beispiel 6.1.3.

Sei $A = \begin{pmatrix} 1 & \mathbf{2} \\ 5 & \mathbf{3} \\ 7 & \mathbf{4} \end{pmatrix}$. Dann ist A eine 3×2-Matrix (d.h. $A \in \mathbb{R}^{3\times 2}$) und es gilt $\begin{array}{ll} A_{1,1} = 1 & A_{1,\mathbf{2}} = \mathbf{2} \\ A_{2,1} = 5 & A_{2,\mathbf{2}} = \mathbf{3} \\ A_{3,1} = 7 & A_{3,\mathbf{2}} = \mathbf{4} \end{array}$

Matrizen sind sehr nützliche Hilfsmittel in einer Vielzahl von Anwendungen. Sie eignen sich als Kurzschreibweise für größere Mengen von Daten. Die wahrscheinlich wichtigste solcher Anwendungen sind lineare Gleichungssysteme.

Beispiel 6.1.4.

Betrachten wir die folgenden beiden linearen Gleichungen:

$$\begin{aligned} 4x_1 \quad +6x_2 \quad -8x_3 \quad &= \quad 0 \\ -2x_2 \quad -8x_3 \quad &= \quad 0 \end{aligned}$$

Die wichtige Information dieses Systems steckt lediglich in den Koeffizienten der beiden Gleichungen. Wir können diese in einer Matrix A zusammenfassen, indem wir im Eintrag A_{ij} den Koeffizienten von x_j in der i-ten Gleichung schreiben. Taucht x_j in der i-ten Gleichung nicht auf, so setzten wir $A_{ij} = 0$. Hier lautet die Matrix A also

$$A = \begin{pmatrix} 4 & 6 & -8 \\ 0 & -2 & -8 \end{pmatrix}.$$

Mit den Rechenregeln, die wir in Kürze lernen werden, können wir das Gleichungssystem dann folgendermaßen schreiben:

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 & 6 & -8 \\ 0 & -2 & -8 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

6.2. Rechnen mit Matrizen

► **Addition** Matrizen mit gleichen Dimensionen lassen sich addieren. Die Addition funktioniert komponentenweise:

Definition 6.2.1.

Es seien $A, B \in \mathbb{R}^{m \times n}$. Die Matrix $C := A + B$ ist die Matrix mit den Einträgen $C_{ij} = A_{ij} + B_{ij}$.

Sage-Box (Rechnen mit Matrizen - Addition)**.**

```
sage: A = Matrix([[0,6],[2, 8],[4,10]])
sage: B = Matrix([[1,7],[3, 9],[5,11]])
sage: C = A + B
sage: C
[1 13]
[5 17]
[9 21]
```

Beispiel 6.2.2.

$$\begin{pmatrix} 0 & 6 \\ 2 & 8 \\ 4 & 10 \end{pmatrix} + \begin{pmatrix} 1 & 7 \\ 3 & 9 \\ 5 & 11 \end{pmatrix} = \begin{pmatrix} 0+1 & 6+7 \\ 2+3 & 8+9 \\ 4+5 & 10+11 \end{pmatrix} = \begin{pmatrix} 1 & 13 \\ 5 & 17 \\ 9 & 21 \end{pmatrix}$$

Beispiel 6.2.3.

$$\begin{pmatrix} 3 & 5 & 1 \\ 2 & 1 & 7 \end{pmatrix} + \begin{pmatrix} 2 & 6 \\ 1 & 2 \end{pmatrix} \text{ ist nicht definiert.}$$

Ganz analog definieren wir natürlich die Subtraktion $A - B$ ganz einfach als die komponentenweise Subtraktion aller Einträge. Die Addition von zwei Matrizen ist nur definiert, wenn sie beide die gleiche Anzahl von Zeilen und auch die gleiche Anzahl von Spalten haben.

► **Multiplikation mit Skalaren** Die Multiplikation einer Matrix A mit einem Skalar $\lambda \in \mathbb{R}$ funktioniert genauso wie bei Vektoren: Man multipliziert jeden Eintrag von A mit λ.

Definition 6.2.4.

Es sei $A \in \mathbb{R}^{m \times n}$ und $\lambda \in \mathbb{R}$. Dann ist $B := \lambda \cdot A \in \mathbb{R}^{m \times n}$ die Matrix mit den Einträgen $B_{ij} = \lambda \cdot a_{ij}$.

Sage-Box (Rechnen mit Matrizen - Multiplikation mit Skalaren)**.**

```
sage: A = Matrix([[1,2,3],[4,5,6]])
sage: 5 * A
[ 5 10 15]
[20 25 30]
```

Beispiel 6.2.5.

$$5 \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 5 \cdot 1 & 5 \cdot 2 & 5 \cdot 3 \\ 5 \cdot 5 & 5 \cdot 5 & 5 \cdot 6 \end{pmatrix} = \begin{pmatrix} 5 & 10 & 15 \\ 20 & 25 & 30 \end{pmatrix}$$

Bei der Multiplikation einer Matrix mit einem Skalar müssen wir uns keine Gedanken um passende Zeilen- und Spaltenanzahl machen. Diese Multiplikation ist immer definiert. Es gelten die folgenden Rechenregeln.

Lemma 6.2.6.

Seien $A, B, C \in \mathbb{R}^{m \times n}$ drei $m \times n$-Matrizen und seien $\lambda, \mu \in \mathbb{R}$ Skalare. Dann gelten:

$$A + B = B + A \qquad \text{(Kommutativgesetz der Addition)}$$

$$(A + B) + C = A + (B + C) \qquad \text{(Assoziativgesetz der Addition)}$$

$$\lambda(\mu \cdot A) = (\lambda \cdot \mu)A = \mu(\lambda \cdot A) \qquad \text{(Assoziativgesetz der Multiplikaton)}$$

$$(\lambda + \mu)A) = \lambda \cdot A + \mu \cdot A$$

$$\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B \qquad \text{(Distributivgesetze)}$$

Beweis. Folgt aus der Definition und den Rechenregeln der reellen Zahlen. □

Die Menge $\mathbb{R}^{n \times m}$ bildet zusammen mit der Addtition und der skalaren Multiplikation einen Vektorraum.

► **Transposition**

Definition 6.2.7 (Transposition)**.**

Es sei $A \in \mathbb{R}^{m\times n}$ eine Matrix.

Die zu A *transponierte* Matrix $A^T \in \mathbb{R}^{n\times m}$ ist die Matrix, mit den Einträgen $(A^T)_{k\ell} = A_{\ell k}$.

Die *Spalten* der Matrix A (von oben nach unten gelesen) werden zu
Zeilen der Matrix A^T (von links nach rechts gelesen)

Sage-Box (Rechnen mit Matrizen - Transposition)**.**

```
sage: A = Matrix([[1,2,3],[4,5,6]])
sage: transpose(A)
[1 4]
[2 5]
[3 6]
```

Bemerkung 6.2.8.

- Es ist für eine Matrix $A \in \mathbb{R}^{m\times n}$ und eine Matrix $B \in \mathbb{R}^{n\times m}$ die transponierte Matrix des Produkts $B\cdot A$ das Produkt der einzelnen Transponierten Matrizen in umgekehrter Reihenfolge, also $(B\cdot A)^T = A^T\cdot B^T$.
- Es ist für eine invertierbare Matrix A auch die transponierte Matrix invertierbar und es gilt $(A^T)^{-1} = (A^{-1})^T$.

Beispiel 6.2.9.

Aus $A \in \mathbb{R}^{3\times 2}$ wird wie folgt eine Matrix $A^T \in \mathbb{R}^{2\times 3}$

$$A = \begin{pmatrix} 1 & 7 \\ 2 & 8 \\ 3 & 9 \end{pmatrix} \quad \Rightarrow \quad A^T = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \end{pmatrix}$$

Liest man einen Vektor als eine $\mathbb{R}^{n\times 1}$-Matrix so kann man diesen auch Transponieren.

Aus einem "stehenden" Vektor $v \in \mathbb{R}^3$ wird so ein "liegender Vektor":

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad \Rightarrow \quad v^T = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

- **Multiplikation mit Vektoren** Die Multiplikation einer Matrix A mit einem Vektor v ist so definiert, dass die in A gespeicherten Koeffizienten wieder an die entsprechenden Einträge von v multipliziert werden. Das Berechnen von $A \cdot v$ erfolgt also zeilenweise, für jede *Zeile* von A wird eine Summe berechnet:

Definition 6.2.10.

Für eine Matrix $A \in \mathbb{R}^{\mathbf{m}\times\mathbf{n}}$ mit $\mathbf{n}$ Spalten und einen Vektor $v \in \mathbb{R}^{\mathbf{n}}$ mit $\mathbf{n}$ Einträgen gilt:

$$A \cdot v = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1\mathbf{n}} \\ A_{21} & A_{22} & \cdots & A_{2\mathbf{n}} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{m\mathbf{n}} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{\mathbf{n}} \end{pmatrix} = \begin{pmatrix} A_{11}\cdot v_1 + & A_{12}\cdot v_2 + & \cdots & +A_{1\mathbf{n}}\cdot v_{\mathbf{n}} \\ A_{21}\cdot v_1 + & A_{22}\cdot v_2 + & \cdots & +A_{2\mathbf{n}}\cdot v_{\mathbf{n}} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}\cdot v_1 + & A_{m2}\cdot v_2 + & \cdots & +A_{m\mathbf{n}}\cdot v_{\mathbf{n}} \end{pmatrix}$$

Das Ergebnis der Multiplikation $A \cdot v$ ist also ein Vektor aus $\mathbb{R}^{\mathbf{m}}$.

Sage-Box (Rechnen mit Matrizen - Matrix-Vektor-Multiplikation)**.**

```
sage: A = Matrix([[9,7,5],[8,6,4]])
sage: v = vector([1,2,3])
sage: A * v
(38,32)
```

In Beispiel 6.1.4 haben wir bereits eine Multiplikation von einer Matrix A mit einem Vektor x gesehen. Dort wurde die Multiplikation verwendet, um die linke Seite eines Gleichungssystems in Kurzschreibweise zu notieren.

Beispiel 6.2.11.

$$\begin{pmatrix} 9 & 7 & 5 \\ 8 & 6 & 4 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{1} \\ \mathbf{2} \\ \mathbf{3} \end{pmatrix} = \begin{pmatrix} 9\cdot\mathbf{1} & +7\cdot\mathbf{2} & +5\cdot\mathbf{3} \\ 8\cdot\mathbf{1} & +6\cdot\mathbf{2} & +4\cdot\mathbf{3} \end{pmatrix} = \begin{pmatrix} 38 \\ 32 \end{pmatrix}$$

Interpretation der Matrix-Vektor-Multiplikation

Die Multiplikation einer Matrix A mit einem Vektor v lässt sich auf zwei Weisen verstehen:

- Skalarprodukt mit den Zeilen von A:
  Es wird *zeilenweise* das Skalarprodukt (siehe Kapitel **??**) der i-ten Zeile von A mit v berechnet.

$$\begin{pmatrix} a & b & c \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a\cdot x & +b\cdot y & +c\cdot z \\ 1\cdot x & +2\cdot y & +3\cdot z \end{pmatrix} = \begin{pmatrix} \left\langle \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right\rangle \\ \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right\rangle \end{pmatrix}$$

- Linearkombination der Spalten von A:
  Es werden Vielfache der *Spalten* von A addiert – mit Vorfaktoren aus v. Der Vektor v ist also eine *Linearkombinations-Anweisung* für die Spalten von A.

$$\begin{pmatrix} a & b & c \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a\cdot x & +b\cdot y & +c\cdot z \\ 1\cdot x & +2\cdot y & +3\cdot z \end{pmatrix}$$

$$= x \cdot \begin{pmatrix} a \\ 1 \end{pmatrix} + y \cdot \begin{pmatrix} b \\ 2 \end{pmatrix} + z \cdot \begin{pmatrix} b \\ 2 \end{pmatrix}$$

6.2.1. Matrix-Matrix-Multiplikation

Üblicherweise wird die Multiplikation $A \cdot B$ einer Matrix $A \in \mathbb{R}^{k \times m}$ mit einer Matrix $B \in \mathbb{R}^{m \times n}$ „von rechts nach links“ durchgeführt. D.h. die Matrix B wird als Liste von Spalten aufgefasst, die jeweils mit A multipliziert werden:

Definition 6.2.12.

Es sei $A \in \mathbb{R}^{k \times \mathbf{m}}$ mit “Inputdimension” $\mathbf{m}$
und $B \in \mathbb{R}^{\mathbf{m} \times n}$ mit n Spalten $B^{(1)}, B^{(2)}, \ldots, B^{(1)} \in \mathbb{R}^{\mathbf{m}}$:

$$A = \begin{pmatrix} \overbrace{\begin{matrix} A_{11} & \ldots & A_{1\mathbf{m}} \\ \vdots & & \vdots \\ A_{k1} & \ldots & A_{k\mathbf{m}} \end{matrix}}^{\text{Breite } m} \end{pmatrix} \quad \overbrace{}^{\text{Höhe m}} \quad B = \begin{pmatrix} \begin{matrix} B_{11} & \ldots & B_{1n} \\ \vdots & & \vdots \\ B_{\mathbf{m}1} & \ldots & B_{\mathbf{m}n} \end{matrix} \end{pmatrix}$$

Die Matrix $C := A \cdot B$ ist die $k \times n$-Matrix mit den Einträgen

$$C_{i,j} := \sum_{s=1}^{m} A_{is} \cdot B_{sj}.$$

Das heißt die Matrix C hat n-viele Spalten der Form $C^{(j)} = A \cdot B^{(j)} \in \mathbb{R}^k$. Also ist

$$A \cdot B = \left(A \cdot B^{(1)}, A \cdot B^{(2)}, \ldots, A \cdot B^{(n)} \right).$$

Bemerkung 6.2.13.

Achtung:

- Das Produkt $A \cdot B$ zweier Matrizen A und B kann nur dann gebildet werden, wenn die **Spaltenanzahl von** A gleich der **Zeilenanzahl von** B ist.
- Die Matrix $A \cdot B$ “erbt” von A die “Output-Dimension” und von B die “Input-Dimension”.
  Die Zwischen-Dimension $\mathbf{m}$ geht bei der Matrixmultiplikation verloren:
  Ist $A \in \mathbb{R}^{k \times \mathbf{m}}$ mit “Output-Dimension” k und “Input-Dimension” $\mathbf{m}$
  und $B \in \mathbb{R}^{\mathbf{m} \times n}$ mit “Output-Dimension” $\mathbf{m}$ und “Input-Dimension” n
  So ist $A \cdot B \in \mathbb{R}^{k \times n}$ mit “Output-Dimension” k und “Input-Dimension” n

Beispiel 6.2.14.

Sei

$$A := \begin{pmatrix} 1 & 5 & 9 \\ 2 & 6 & 9 \end{pmatrix} \quad \text{und} \quad B := \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Die Matrix A hat 3 Spalten und B hat 3 Zeilen.

Da diese Zahlen gleich sind, können wir das Produkt $A \cdot B$ berechnen:

$$A \cdot B = \left(A \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \; A \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 10 & 6 \\ 11 & 8 \end{pmatrix}$$

Korollar 6.2.15.

Es seien $A \in \mathbb{R}^{k \times m}$, $B \in \mathbb{R}^{m \times n}$ und $x \in \mathbb{R}^n$. Dann ist

$$A \cdot (B \cdot x) \; = \; (A \cdot B) \cdot x.$$

Beweis.

Es sei $A \in \mathbb{R}^{k \times \mathbf{m}}$ mit "Inputdimension" $\mathbf{m}$
und $B \in \mathbb{R}^{\mathbf{m} \times n}$ mit n Spalten $B^{(1)}, B^{(2)}, \ldots, B^{(1)} \in \mathbb{R}^{\mathbf{m}}$ Weiter sei $x \in \mathbb{R}^n$.

Dann gilt $B \cdot x = x_1 \cdot B^{(1)} + \ldots + x_n \cdot B^{(n)} \in \mathbb{R}^{\mathbf{m}}$.

$$\begin{aligned} A \cdot (B \cdot x) &= A \cdot \left(x_1 \cdot B^{(1)} + \ldots + x_n \cdot B^{(n)} \right) \\ &\overset{\star}{=} x_1 \cdot A \cdot B^{(1)} + \ldots + x_n \cdot A \cdot B^{(n)} \qquad (\star \text{ Linearität von } A \cdot y) \\ &= \underbrace{\left(A \cdot B^{(1)} + \ldots + A \cdot B^{(n)} \right)}_{\text{Matrix mit Spalten } A \cdot B^{(i)}} \cdot \; x \; = \; (A \cdot B) \cdot x \end{aligned}$$

□

Die Rechenregeln für die Multiplikation (Lemma 6.2.16) von Matrizen sehen im Prinzip aus, wie Rechnen mit Zahlen aus $\mathbb{R}$. Allerdings gilt für Matrizen das Kommutativgesetz nicht! D.h. im Allgemeinen ist $A \cdot B \neq B \cdot A$. Selbst wenn beide Produkte definiert sind, gilt nicht immer die Gleichheit.

Lemma 6.2.16 (Rechenregeln für die Matrix-Multiplikation)**.**

Es seien $A, \widetilde{A}, B, \widetilde{B}, C$ Matrizen mit passender Größe, d.h.

$$A, \widetilde{A} \in \mathbb{R}^{m \times n}, \quad B, \widetilde{B} \in \mathbb{R}^{n \times k} \quad \text{und } C \in \mathbb{R}^{k \times \ell}$$

Dann gelten:

1)	$(A \cdot B) \cdot C$	$=$	$A \cdot (B \cdot C)$	(Assoziativgesetz)
2)	$A \cdot (B + \widetilde{B})$	$=$	$A \cdot B + A \cdot \widetilde{B}$	(Distributivgesetz)
	$(A + \widetilde{A}) \cdot B$	$=$	$A \cdot B + \widetilde{A} \cdot B$	
3)	$A \cdot (\lambda \cdot B)$	$=$	$\lambda \cdot A \cdot B$	gilt für alle $\lambda \in \mathbb{R}$

Im Allgemeinen gilt:

$A \cdot B$	$\neq$	$B \cdot A$	(Kommutativgesetz gilt im Allgemeinen nicht)

Beweis. Die Aussagen in 2) und 3) lassen sich direkt aus der Definition der Matrixmultiplikation ableiten.

Zu 1) Es sei $C = (c_1, \ldots, c_\ell)$ mit Spalten $c_i \in \mathbb{R}^k$.

$$\begin{aligned} A \cdot (B \cdot C) = A \cdot (\ B \cdot c_1 \ldots B \cdot c_\ell\ ) &= (\ A \cdot (B \cdot c_1) \quad \ldots \quad A \cdot (B \cdot c_\ell)\ ) \\ &\overset{\star}{=} (\ (A \cdot B) \cdot c_1 \quad \ldots \quad (A \cdot B) \cdot c_\ell\ ) \quad = (A \cdot B) \cdot C \end{aligned}$$

Denn bei $(\star)$ gilt nach Korollar 6.2.15 Assoziativität: $A \cdot (B \cdot x) = (A \cdot B) \cdot x$ gilt für alle $x \in \mathbb{R}^k$.

□

Beispiel 6.2.17 (Kommutativgesetz gilt nicht)**.**

Für die Matrizen $A := \begin{pmatrix} 3 & 5 \\ 0 & 0 \end{pmatrix}$ und $B := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ gilt $A \cdot B \neq B \cdot A$, denn:

$$A \cdot B = \left(A \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix} \qquad \text{und} \qquad B \cdot A = \left(B \cdot \begin{pmatrix} 3 \\ 0 \end{pmatrix} \quad B \cdot \begin{pmatrix} 5 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Wir haben jetzt gelernt wie man Matrizen addieren und auch miteinander multiplizieren kann, kann man sie dann auch durcheinander "dividieren"? Die Antwort auf diese Frage geben wir in Kapitel **??** nachdem wir uns zunächst mit Linearen Gleichungssystemen beschäftigt haben, welche durch Matrizen eine elegante Darstellungsform erhalten.

7 Matrizen und lineare Abbildungen

7.1. Einführung

Wir haben das vorherige Kapitel 6 begonnen mit dem Versprechen, lineare Abbildungen der Form $f : \mathbb{R}^n \to \mathbb{R}^m$ mit Hilfe von Matrizen beschreiben zu können. Diese Abbildungen bilden jeden Vektor aus dem Vektorraum $\mathbb{R}^n$ auf einen Vektor im Vektorraum $\mathbb{R}^m$ ab. Wir erinnern zunächst, was die uns geläufige Schreibweise von Vektoren aus reellen Vektorräumen der Form $\mathbb{R}^n$ letzlich bedeutet.

7.1.1. Komponentenschreibweise

Dazu erinnern wir an die Definition 5.2.4 des Vektorraums $\mathbb{R}^n$ - er wird aufgespannt von den n Einheitsvektoren. Die Komponenten $v_1, \dots v_n$ eines Vektors

$$v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$$

indizieren die Koeffizienten seiner eindeutigen Linearkombination der Basisvektoren alias den Einheitsvektoren $e^{(1)}, \dots e^{(n)}$. Denn es ist

$$v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_n \end{pmatrix} = v_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + v_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + v_n \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \sum_{k=1}^{n} v_k e^{(k)}.$$

Für einen Untervektorraum eines $\mathbb{R}^m$ oder für einen beliebigen Vektoraum lässt sich diese Komponentenschreibweise verallgemeinern. Sei also V ein beliebiger $\mathbb{R}$-Vektorraum. Sei $\mathcal{B} = \{b_1, \dots, b_n\}$ eine Basis von V. Dann gibt es nach Proposition 5.2.2 für jeden Vektor $u \in V$ eine eindeutige Linearkombination der Basisvektoren, also ein eindeutiges k-Tupel $u_1, \dots, u_n \in \mathbb{R}$ mit

$$u = u_1 \cdot b_1 + \ldots + u_n \cdot b_k = \sum_{k=1}^{n} u_k b_k.$$

Wir führen die Komponenten-Schreibweise ein

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}_{[\mathcal{B}]}$$

wobei die Komponten die Koeffizienten der eindeutigen Linearkombination der Basisvektoren $\mathcal{B}$ sind. Fehlt der Index, dann entspricht die Basis der Einheitsbasis des $\mathbb{R}^n$.

7.1.2. Matrixdarstellung linearer Abbildungen

Ist $f : \mathbb{R}^n \to \mathbb{R}^m$ eine lineare Abbildung, dann ist also

$$f(v) = f\left(\sum_{k=1}^{n} v_k e^{(k)}\right) = \sum_{k=1}^{n} v_k f(e^{(k)}).$$

Wenn wir nun die n Vektoren $f(e^{(1)}), \ldots, f(e^{(n)}) \in \mathbb{R}^m$ kennen, kennen wir auch das Bild $f(x)$ für alle $x \in \mathbb{R}^n$ unter der linearen Abbildung f. Mit anderen Worten: f ist vollständig durch die Bilder der Vektoren $e^{(1)}, \ldots e^{(n)}$ bestimmt. Wir fassen diese n Vektoren in einer Matrix zuammen. Genauer sei $M(f)$ die $m \times n$-Matrix mit Spalten

$$M(f)^{(1)} = f(e^{(1)}), M(f)^{(2)} = f(e^{(2)}), \ldots, M(f)^{(n)} = f(e^{(n)}).$$

Diese Matrix heißt die ***darstellende Matrix*** (oder Darstellungsmatrix) von f. Wir halten also fest:

Definition 7.1.1.

> Sei $f : \mathbb{R}^n \to \mathbb{R}^m$ eine lineare Abbildung. Wir nennen die $m \times n$-Matrix $M(f)$ deren Spalten den Bildern der Einheitsvektoren des $\mathbb{R}^n$ unter der Abbildung f entsprechen die ***darstellende Matrix*** (oder Darstellungsmatrix) von f.

Erinnert an die Multiplikation einer Matrix mit einem Vektor finden wir

$$f(v) = M(f) \cdot v.$$

Die lineare Abbildung f ist also nichts anderes als Multiplikation mit der Matrix $M(f)$. Umgekehrt stellt unsere Definition von "Matrix mal Vektor" sicher, dass für jede $m \times n$-Matrix A die Abbildung $f : \mathbb{R}^n \to \mathbb{R}^m, v \mapsto A \cdot x$ linear ist.

Beispiel 7.1.2.

- **Abbildungen $\mathbb{R} \to \mathbb{R}$:** Alle linearen Abbildung von $\mathbb{R}$ nach $\mathbb{R}$ sind von der Form $f_a(x) = a \cdot x$. Fassen wir die reellen Zahlen als Vektorraum auf, wird dieser von dem einzigen und in diesem Fall eindimensionalen Einheitsvektor (1) aufgespannt. Das Bild dieses Vektor ist $f((1)) = (a)$ und die Darstellungsmatrix ist also die 1×1-Matrix $M(f_a) = (a)$. Sowohl die Vektoren als auch die Matrizen sind in diesem Fall einfach reelle Zahlen.
- **Eine Abbildung von $\mathbb{R}^2$ nach $\mathbb{R}^2$:** Wir wählen konkret die Abbildung die durch die folgenden Bilder der Einheitsvektoren des $\mathbb{R}^2$ bestimmt ist:

  $$f\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ -\frac{1}{2} \end{pmatrix} \qquad \text{und} \qquad f\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} -\frac{1}{2} \\ 1 \end{pmatrix}$$

  Dann ist die Darstellungsmatrix von f gleich

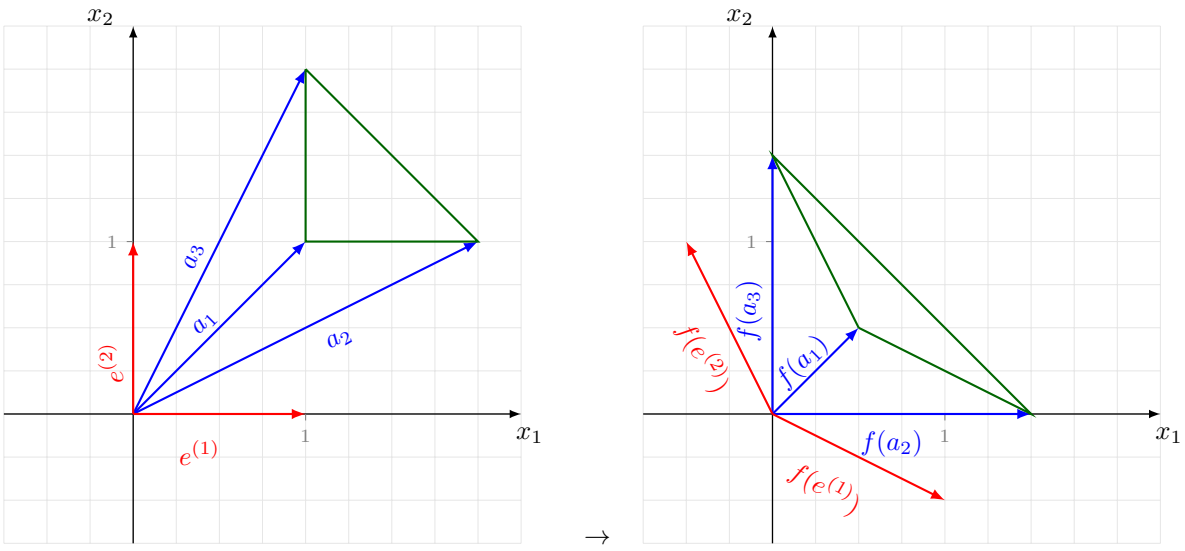
  $$M(f) = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix}$$

Um zu verdeutlichen, was geometrisch bei dieser linearen Abbildung geschieht, betrachte das Dreieck, dessen Ecken die Stützvektoren $a_1 = \begin{pmatrix}1\\1\end{pmatrix}$, $a_2 = \begin{pmatrix}2\\1\end{pmatrix}$ und $a_3 = \begin{pmatrix}1\\2\end{pmatrix}$ haben, wird abgebildet auf:

$$f(a_1) = M(f) \cdot a_1 = \begin{pmatrix}1 & -\frac{1}{2}\\ -\frac{1}{2} & 1\end{pmatrix} \cdot \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}\frac{1}{2}\\ \frac{1}{2}\end{pmatrix}$$

$$f(a_2) = M(f) \cdot a_2 = \begin{pmatrix}1 & -\frac{1}{2}\\ -\frac{1}{2} & 1\end{pmatrix} \cdot \begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}\frac{3}{2}\\ 0\end{pmatrix}$$

$$f(a_3) = M(f) \cdot a_3 = \begin{pmatrix}1 & -\frac{1}{2}\\ -\frac{1}{2} & 1\end{pmatrix} \cdot \begin{pmatrix}1\\2\end{pmatrix} = \begin{pmatrix}0\\ \frac{3}{2}\end{pmatrix}$$



Proposition 7.1.3.

Sind $f, g : \mathbb{R}^n \to \mathbb{R}^m$ lineare Abbildungen und ist $\lambda \in \mathbb{R}$, so ist

- $M(f+g) = M(f) + M(g)$
- $M(\lambda \cdot f) = \lambda \cdot M(f)$
- $M(g \circ f) = M(g) \cdot M(f)$.

Beweis. Übungsaufgabe. □

Bemerkung 7.1.4.

Notation:
Für quadratische Matrizen benutzen wir auch die Potenzschreibweise. Mit A^k für $k \in \mathbb{N}$ bezeichnen wir also das Produkt

$$A^k = \underbrace{A \cdot A \cdot \ldots \cdot A}_{k\text{mal}}$$

Einige Matrizen spielen eine besondere Rolle. Für jede Größe $m \times n$ bezeichnen wir mit 0 die Matrix, deren

Einträge alle gleich 0 sind. Diese Matrix hat die Eigenschaft, dass $A + 0 = 0 + A = A$ für alle A.

Außerdem bezeichnet id die $n \times n$-Matrix, deren Diagonaleinträge gleich 1 sind, während alle anderen Einträge gleich 0 sind. Für jede $n \times n$-Matrix A gilt $\mathrm{id} \cdot A = A \cdot id = A$. Ferner gilt $\mathrm{id} \cdot x = x$ für jeden Vektor $x \in \mathbb{R}^n$. Allgemeiner bezeichnen wir für einen Vektor $a \in \mathbb{R}^n$ mit $\mathrm{diag}(a)$ die $n \times n$-Matrix, deren Diagonale gerade der Vektor a ist, während alle anderen Einträge gleich 0 sind. Für jeden Vektor $x \in \mathbb{R}^n$ gilt dann

$$\mathrm{diag}(a) \cdot x = \begin{pmatrix} a_1 x_1 \\ a_2 x_2 \\ \vdots \\ a_n x_n \end{pmatrix}.$$

Schließlich sagen wir, dass eine $m \times n$-Matrix D ***Diagonalform*** hat, wenn aus $D_{ij} \neq 0$ folgt, dass $i = j (i = 1, \ldots, m; j = 1, \ldots, n)$. Mit anderen Worten: nur die Diagonaleinträge D_{ii} dürfen von Null verschieden sein.

Definition 7.1.5.

Seien A, B $n \times n$-Matrizen. Wir sagen, dass B zu A ***invers*** ist, wenn $A \cdot B = B \cdot A = \mathrm{id}$. Falls es eine Matrix B gibt, die zu A invers ist, heißt A ***invertierbar*** oder ***regulär***, andernfalls heißt A ***singulär***.

Proposition 7.1.6.

Eine $n \times n$-Matrix A ist genau dann invertierbar, wenn die lineare Abbildung $v \in \mathbb{R}^n \to A \cdot v$ ein Isomorphismus ist.

Beweis. ... □

7.1.3. Einige weitere Beispiel

Wir führen jetzt noch einige konkrete lineare Abbildungen beispielhaft auf.

Beispiel 7.1.7.

- Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x \end{pmatrix}$ entspricht der Spiegelung des $\mathbb{R}^2$ an der Geraden $x = y$.

  Die darstellende Matrix hat die Spalten $f(e_1) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $f(e_2) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, d.h.

$$M(f) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Die Abbildung $h : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x \\ y \end{pmatrix}$ entspricht einer Spiegelung des $\mathbb{R}^2$ an der y-Achse.

  Die darstellende Matrix hat die Spalten $h(e_1) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, $h(e_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, d.h.

$$M(h) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

- Die Abbildung $h \circ f : \mathbb{R}^2 \to \mathbb{R}^2$, entspricht der Hintereinanderausführung beider Spiegelungen:
  $h \circ f(\begin{pmatrix} x \\ y \end{pmatrix}) = h(\begin{pmatrix} y \\ x \end{pmatrix}) = \begin{pmatrix} -y \\ x \end{pmatrix}$
  Die darstellende Matrix hat also Spalten $h \circ f(e_1) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $h \circ f(e_2) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, d.h.

$$M(h \circ f) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

- Die Abbildung $h \circ f : \mathbb{R}^2 \to \mathbb{R}^2$, entspricht der Hintereinanderausführung beider Spiegelungen:
  $h \circ f(\begin{pmatrix} x \\ y \end{pmatrix}) = h(\begin{pmatrix} y \\ x \end{pmatrix}) = \begin{pmatrix} -y \\ x \end{pmatrix}$
  Die darstellende Matrix hat also Spalten $h \circ f(e_1) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $h \circ f(e_2) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, d.h.

$$M(h \circ f) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

7.2. Dimensionssatz

Wir definieren nun zwei Mengen, die etwas über die Dimension der Mengen aussagen, die bei einer linearen Abbildung beteiligt sind. Im Kern einer Matrix (eine dieser Mengen) liegen all jene Vektoren, die auf den Nullvektor abgebildet werden. Im Bild der Matrix liegen all jene Vektoren, die Bilder eines Vektors aus dem Urbild sind, also im Bild der assoziierten linearen Abbildung liegen. Der Kern ist eine Teilmenge des Urbildraums, das Bild ist eine Teilmenge des Bildraums. Beide Mengen bilden Untervektorräume. Tatsächlich gibt es einen Zusammenhang der Dimensionen dieser beiden Vektorräume und dem Urbildvektorraum. Der Dimensionssatz besagt, dass die Summe der Dimensionen von Kern und Bild immer gleich der Dimension des Urbildraums ist. Um dies formal zu fassen und zu beweisen definieren wir zunächst den Kern und das Bild einer Matrix.

Definition 7.2.1.

Für eine Matrix $A \in \mathbb{R}^{m \times n}$ definieren wir den Kern der Matrix und das Bild der Matrix als:

$$\mathsf{Kern}(A) := \{x \in \mathbb{R}^n \ : \ A \cdot x = 0\} \qquad \mathsf{Bild}(A) := \{A \cdot x \ : \ x \in \mathbb{R}^n\}$$

Bemerkung 7.2.2.

- Für $A = (a_1, \ldots, a_n)$ mit Spalten $a_i \in \mathbb{R}^m$ gilt: $\mathsf{Bild}(A) = \mathsf{span}\,(\{a_1, \ldots, a_n\})$
- Für die Abbildung $f : \mathbb{R}^n \to \mathbb{R}^m$, $x \mapsto A \cdot x$ gilt:
  - Der Kern ist eine Teilmenge der *Urbildmenge* $\mathbb{R}^n$ der Abbildung f
  - Das Bild ist eine Teilmenge des *Bildmenge* $\mathbb{R}^m$ der Abbildung f
- Sind A eine $m \times n$-Matrix, $b \in \mathbb{R}^m$ und $x \in \mathbb{R}^n$ so, dass $A \cdot x = b$, so gilt für jeden Vektor z im Kern von A, dass $A(x + z) = b$. Ist umgekehrt x' ein Vektor mit $A \cdot x' = b$, so ist $z = x - x'$ im Kern von A.

Lemma 7.2.3.

Für jede Matrix $A \in \mathbb{R}^{m\times n}$ sind $\mathsf{Kern}(A) \subset \mathbb{R}^n$ und $\mathsf{Bild}(A) \subset \mathbb{R}^m$ Vektorräume.

Beweis. Hat $A \in \mathbb{R}^{m\times n}$ die Spalten $a_1, \ldots, a_n \in \mathbb{R}^m$, d.h. $A = (a_1, \ldots, a_n)$ so gilt $\mathsf{Bild}(A) = \mathsf{span}\,(\{a_1, \ldots, a_n\})$:

$$\begin{aligned}\mathsf{Bild}(A) &= \{A \cdot x \,:\, x \in \mathbb{R}^n\} \\ &= \{x_1 \cdot a_1 + \ldots + x_n a_n \,:\, x_1, \ldots x_n \in \mathbb{R}\} \quad = \mathsf{span}\,(\{a_1, \ldots, a_n\})\end{aligned}$$

Der Spann von endlich vielen Vektoren ist stets ein Vektorraum, d.h. $\mathsf{Bild}(A)$ ist ein Vektorraum.

$\mathsf{Kern}(A) \subseteq \mathbb{R}^n$, "erbt" als Teilmenge von $\mathbb{R}^n$ fast alle Eigenschaften des $\mathbb{R}^n$. Deswegen genügt es nach Lemma 3.3.13 zu zeigen: $\mathsf{Kern}(A)$ ist abgeschlossen unter Addition und skalarer Multiplikation.

- z.z.: $\forall x, y \in \mathsf{Kern}(A) : x + y \in \mathsf{Kern}(A)$.
  Seien $x, y \in \mathsf{Kern}(A)$, dann gilt $A \cdot (x + y) = \underbrace{A \cdot x}_{=0} + \underbrace{A \cdot y}_{=0} = \mathbb{0}$ und das heißt: $x + y \in \mathsf{Kern}(A)$.
- z.z.: $\forall x \in \mathsf{Kern}(A), \lambda \in \mathbb{R} : \lambda \cdot x \in \mathsf{Kern}(A)$.
  Seien $x \in \mathsf{Kern}(A)$ und $\lambda \in \mathbb{R}$, dann gilt $A \cdot (\lambda x) = \lambda \cdot \underbrace{A \cdot x}_{=0} = \mathbb{0}$ und das heißt: $\lambda \cdot x \in \mathsf{Kern}(A)$.

□

Lemma 7.2.4.

Es sei $A \in \mathbb{R}^{m\times n}$ dann gilt für die Vektorräume Kern und Bild:

$$\dim\left(\mathsf{Kern}(A)\right) + \dim\left(\mathsf{Bild}(A)\right) = n$$

Beweis. Wir konstruieren aus einer Basis von $\mathsf{Kern}(A)$ und (den Urbildern von) einer Basis von $\mathsf{Bild}(A)$ eine Basis von $\mathbb{R}^n$:

Es sei $\{u_1, \ldots, u_k\} \subset \mathbb{R}^n$ eine Basis von $\mathsf{Kern}(A)$, d.h. $\dim(\mathsf{Kern}(A)) = k$.

Es sei $\{w_1, \ldots, w_\ell\} \subset \mathbb{R}^m$ eine Basis von $\mathsf{Bild}(A)$, d.h. $\dim(\mathsf{Bild}(A)) = \ell$.

Nach Definition von $\mathsf{Bild}(A)$ ist jeder der Vektoren w_i von der Form $w_i = A \cdot v_i$.

Es sei $\{v_1, \ldots, v_\ell\} \subset \mathbb{R}^n$ so dass für jedes $i = \{1, \ldots \ell\}$ gilt: $A \cdot v_i = w_i$.

Wir zeigen nun, dass $u_1, \ldots, u_k, v_1, \ldots v_\ell$ linear **un**abhängig sind: Es seien $\mu_1, \ldots, \mu_k, \lambda_1, \ldots, \lambda_\ell \in \mathbb{R}$

$$\begin{aligned}
(*) \quad & \mu_1 \cdot u_1 + \ldots + \mu_k \cdot u_k \quad + \lambda_1 \cdot v_1 + \ldots + \lambda_\ell \cdot v_\ell && = 0 \\
\Longrightarrow \quad & A \cdot \left(\mu_1 \cdot u_1 + \ldots + \mu_k \cdot u_k \quad + \lambda_1 \cdot v_1 + \ldots + \lambda_\ell \cdot v_\ell\right) && = A \cdot 0 \\
\Longrightarrow \quad & \mu_1 \underbrace{A \cdot u_1}_{=0} + \ldots + \mu_k \underbrace{A \cdot u_k}_{=0} \quad + \lambda_1 \cdot \underbrace{A \cdot v_1}_{=w_1} + \ldots + \lambda_\ell \cdot \underbrace{A \cdot v_\ell}_{=w_\ell} && = 0 \\
& \overset{\star}{\Rightarrow} \lambda_1 = \lambda_2 = \ldots = \lambda_\ell = 0 && \star\ w_1, \ldots, w_\ell \text{ sind linear unabhängig}
\end{aligned}$$

Setzt man $\lambda_1 = \lambda_2 = \ldots = \lambda_\ell = 0$ in $(*)$ ein, so erhält man

$$\begin{aligned} & \mu_1 \cdot u_1 + \ldots + \mu_k \cdot u_k + 0 \cdot v_1 + \ldots + 0 \cdot v_\ell = 0 \\ \Longrightarrow \quad & \mu_1 = \ldots = \mu_k = 0 \qquad \text{weil } u_1, \ldots, u_\ell \text{ linear unabhängig sind} \end{aligned}$$

Aus $(*)$ folgt also $\mu_1 = \ldots = \mu_k = 0$ und $\lambda_1 = \lambda_2 = \ldots = \lambda_\ell = 0$, d.h. die Vektoren sind linear **un**abhängig. Wir haben $k + \ell$-viele linear **un**abhängige Vektoren im $\mathbb{R}^n$ gefunden. Damit gilt nun:

$$k + \ell \leq \dim(\mathbb{R}^n) = n$$

Es bleibt zu zeigen: Für $V := \mathsf{span}\,(\{u_1, \ldots, u_k, v_1, \ldots v_\ell\})$ gilt $\mathbb{R}^n \subset V$.

Es sei $x \in \mathbb{R}^n$ beliebig und $y' := A \cdot x$. Wegen $y' \in \mathsf{Bild}(A)$ gilt $y' = \lambda_1 w_1 + \ldots + \lambda_\ell w_\ell$. Es gibt damit also $x' \in \mathsf{span}(v_1, \ldots v_\ell)$ mit $Ax' = y'$ nämlich $x' := \lambda_1 v_1 + \ldots + \lambda_\ell v_\ell$. Wegen $A \cdot x = A \cdot x'$ folgt $A(x - x') = 0$, d.h. $z := x - x' \in \mathsf{Kern}(A)$. Insgesamt folgt: $x = z + x'$ mit $z \in \mathsf{span}(u_1, \ldots, u_k)$ und $x' \in \mathsf{span}(v_1, \ldots, v_\ell)$.

Weil $x \in \mathbb{R}^n$ beliebig gewählt wurde, gilt also $\mathbb{R}^n \subset V$. □

7.3. Allgemeine lineare Abbildungen zwischen Vektorräumen

Wir haben gelernt, lineare Abbildungen $g : R^n \to R^m$ durch Matrizen darzustellen. Erlauben auch lineare Abbildungen $g : V \to V'$ zwischen anderen Vektorräumen V, V' eine solche Darstellung? Das geht tatsächlich, allerdings müssen wir zuvor Basen von V und V' festlegen. Sei also $\mathcal{A} = (a_1, \ldots, a_n)$ eine Basis von V und $\mathcal{B} = (b_1, \ldots, b_m)$ eine Basis von V'.

Die Matrixdarstellung von g ergibt sich aus den Bildern der Basisvektoren aus der Basis $\mathcal{A}$ als Linearkombination der Basisvektoren der Basis $\mathcal{A}$. Es ist also

$$g(a_j) = \sum_{i=1}^{m} c_{ij} b_i$$

und es gilt

$$M_{\mathcal{A},\mathcal{B}}(g) = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \cdots & c_{m,n} \end{pmatrix}.$$

Die Spalten dieser Matrix entsprechen Vektoren zur Basis $\mathcal{B}$ also

$$M_{\mathcal{A},\mathcal{B}}(g)^{(i)} = \begin{pmatrix} c_{1i} \\ \vdots \\ c_{mi} \end{pmatrix}_{[\mathcal{B}]}.$$

Wir definieren nun zwei Isomorphismen f_1 und f_2 um im Spezialfall $V = \mathbb{R}^n$ und $V = \mathbb{R}^m$ die Abbildung g als

Matrix-Vektor-Multiplikation bezüglich der Einheitsbasis darzustellen. Es seien

$$f_1 : \mathbb{R}^n \to V, \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{m} x_i a_i.$$

$$f_2 : \mathbb{R}^m \to V', \qquad \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \mapsto \sum_{i=1}^{m} y_i b_i.$$

Bemerkung 7.3.1.

Dass es sich dabei um Isomorphismen handelt folgt aus den beiden Beobachungen, dass die Bilder Linearkombinationen von Basisvektoren sind (mit Proposition 5.2.2 folgt die Injektivität) und dass das gesamte Bild gleich $\mathsf{span}(\mathcal{A})$ bzw. $\mathsf{span}(\mathcal{B})$ ist (Surjektivität).

Die beiden linearen Abbildungen f_1 und f_2 haben die Eigenschaft, dass die Einheitsvektoren auf die Basisvektoren in $\mathcal{A}$ bzw. $\mathcal{B}$ abgebildet werden. Umgekehrt ist $f_1^{-1}(a_i) = e^{(i)}$ und $f_2^{-1}(b_j) = e^{(j)}$ für alle $i \in \{1, \ldots, n\}$ und $j \in \{1, \ldots, m\}$.

Es ergibt sich die folgende Identität:

$$M_{\mathcal{A},\mathcal{B}}(g) = M(f_2^{-1} \cdot g \cdot f_1) = M(f_2)^{-1} \cdot M(g) \cdot M(f_1).$$

Anhand der Definition von f_1 und g sieht man ferner, dass $M(f_1)$ die Matrix ist, deren Spalten die Basisvektoren $\mathcal{A}$ sind. Entsprechend ist $M(f_2)$ die Matrix, deren Spalten die Basisvektoren $\mathcal{B}$ sind. Ein wesentliches Ziel der folgenden Abschnitte wird sein, Basen $\mathcal{A}, \mathcal{B}$ zu finden, so dass die Matrix $M_{\mathcal{A},\mathcal{B}}(g)$ eine möglichst einfache Gestalt hat.

Beispiel 7.3.2.

Sei $g : \mathbb{R}^2 \to \mathbb{R}^2$ eine lineare Abbildung mit Darstellungsmatrix $M(g) = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}$.

Wähle die Basen $\mathcal{A}$ mit $a_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ und $a_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ sowie $\mathcal{B}$ mit $b_1 = \begin{pmatrix} 5 \\ 5 \end{pmatrix}$ und $b_2 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$. Dann ist

$$g(a_1) = M(g) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix} = 1 \cdot b_1 + 0 \cdot b_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{[\mathcal{B}]}$$

$$g(a_2) = M(g) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} = 0 \cdot b_1 + 1 \cdot b_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{[\mathcal{B}]}$$

und wir erhalten $M_{\mathcal{A},\mathcal{B}}(g) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ und überprüfen die Identität

$$M_{\mathcal{A},\mathcal{B}}(g) = M(f_2^{-1} \circ g \circ f_1) = M(f_2)^{-1} \cdot M(g) \cdot M(f_1).$$

Wir haben die folgenden Darstellungsmatrizen:

$$M(f_1) = \left(f_1(e^{(1)}, f_1(e^{(2)}\right) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$M(f_2) = \left(f_2(e^{(1)}, f_2(e^{(2)}\right) = \begin{pmatrix} 5 & 3 \\ 5 & 1 \end{pmatrix}$$

$$M(f_2^{-1}) = M(f_2)^{-1} = \begin{pmatrix} -\frac{1}{10} & \frac{3}{10} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \qquad \text{[mit Hilfe des Schemas aus Bsp. 7.3.4]}$$

Tatsächlich rechnet man nach, dass

$$M(f_2)^{-1} \cdot M(g) \cdot M(f_1) = \begin{pmatrix} -\frac{1}{10} & \frac{3}{10} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M_{\mathcal{A},\mathcal{B}}(g).$$

7.3.1. Lineare Selbstabbildungen: Die Welt der quadratischen Matrizen

Eine Matrix $A \in \mathbb{R}^{n\times n}$ bei der die Anzahl der Zeilen mit der Anzahl der Spalten übereinstimmt heißt *quadratisch* ("Input-" gleich "Output-Dimension").

Quadratische Matrizen stehen für *lineare Selbstabbildungen*, d.h. eine Matrix $A \in \mathbb{R}^{n\times n}$ liefert eine Abbildung $f(x) := A(x)$ mit $f : \mathbb{R}^n \to \mathbb{R}^n$. Für solche "Automorphismen[3]" gibt es viele Anwendungen und deswegen eine reichhaltige Theorie.

Beispiel 7.3.3.

Für $A := \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$ gilt $A^{-1} = \begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix}$

$$A^{-1} \cdot A = \begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5\cdot 3 - 7\cdot 2 & 0 \\ 0 & -2\cdot 7 + 3\cdot 5 \end{pmatrix} = \mathrm{id}$$

Beispiel 7.3.4 (Formel für das Invertieren in $\mathbb{R}^{2\times 2}$)**.**

Es sei $A := \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ mit Einträgen $a, b, c, d \in \mathbb{R}$ so dass $ad - cb \neq 0$ gilt.

Es gilt dann:

$$A^{-1} = \frac{1}{ad-cb} \cdot \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

$$A^{-1} \cdot A = \frac{1}{ad-cb} \cdot \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \frac{1}{ad-cb} \cdot \begin{pmatrix} ad-cb & 0 \\ 0 & ad-cb \end{pmatrix} = \mathrm{id}$$

[3] Automorphismus = strukturerhaltende Selbstabbildungen ('auto' - selbst & 'morphismus' - Verformung)

7.4. Lineare Gleichungssysteme

Für eine gegebene lineare Abbildung $f : V \to V'$ und einen Vektor $y \in V'$ möchten wir einen Vektor $x \in V$ mit $f(x) = y$ finden, falls es ein solches x gibt. Weil f durch eine Matrix dargestellt werden kann (durch Wahl von Basen für V und V'), genügt es, das folgende, konkretere Problem zu lösen: Für eine $m \times n$- Matrix A und einen Vektor $b \in \mathbb{R}^m$ ist $x \in \mathbb{R}^n$ mit $A \cdot x = b$ zu bestimmen, falls es ein solches x gibt. Genauer gesagt möchten wir alle solchen Vektoren x bestimmen.

Definition 7.4.1.

Ein lineares Gleichungssystem (LGS) ist ein System von Gleichungen der Form

$$\begin{array}{ccccccc} A_{1,1} \cdot x_1 & +A_{1,2} \cdot x_2 & +\ldots+ & A_{1,n} \cdot x_n & = & b_1 \\ A_{2,1} \cdot x_1 & +A_{2,2} \cdot x_2 & +\ldots+ & A_{2,n} \cdot x_n & = & b_2 \\ \vdots & \vdots & & \vdots & & \\ A_{m1} \cdot x_1 & +A_{m,2} \cdot x_2 & +\ldots+ & A_{m,n} \cdot x_n & = & b_m \end{array}$$

mit $A_{1,1}, \ldots, A_{m,n} \in \mathbb{R}$ und $b_1, \ldots b_m \in \mathbb{R}$.

Jedes lineare Gleichungssystem lässt sich äquivalent schreiben als $A \cdot x = b$ mit $A \in \mathbb{R}^{m \times n}$ und $b \in \mathbb{R}^m$.

Das Lösen eines LGS kann per Gauß'schem Eliminationsverfahren erfolgen. Dabei wird eine Gleichung der Form $A \cdot x = b$ durch ein Tableau der Form $A|b$ ersetzt, auf dem Umformungen durchgeführt werden (sog. Gaussschritte), bis ein Tableau entsteht, das eine Matrix in *Zeilen-Stufen-Form* enthält:

Eine Matrix $A \in \mathbb{R}^{m \times n}$ hat Zeilen-Stufen-Form, wenn in jeder Zeile $z > 2$ mehr führende Nullen stehen als in der vorherigen Zeile $z - 1$ (es sei denn die Zeile $z - 1$ bestand schon komplett aus Nullen).

Definition 7.4.2.

Eine Matrix $A \in \mathbb{R}^{m \times n}$ hat Zeilen-Stufen-Form, wenn es einen Zeilen-Index $\ell \in \{1, \ldots, m+1\}$ gibt mit:

- Jede Zeile mit Index in $\{2, \ldots, \ell - 1\}$ enthält mindesten eine führende Null mehr als die Zeile davor.
- Jede Zeile mit Index in $\{\ell, \ldots, m\}$ enthält nur Nullen (falls $\ell = m + 1$ gibt es keine solchen Zeilen).

Beispiel 7.4.3.

Die folgenden Matrizen haben jeweils Zeilen-Stufen-Form mit $\ell = 4$:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 3 & 5 & 7 & 9 \\ 0 & 0 & 0 & 2 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 3 & 5 & 7 & 9 \\ 0 & 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Anzahl führender Nullen steigt bis Zeile $3 = \ell - 1$

Anzahl führender Nullen ist maximal ab Zeile $4 = \ell$

Beispiel 7.4.4.

Die folgende Matrix ist nicht in Zeilen-Stufen-Form, denn Zeile 2 enthält genauso viele führende Nullen wie Zeile 3, obwohl beide nicht maximal viele Nullen enthalten:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 5 & 7 & 9 \\ 0 & 0 & 2 & 4 & 6 \end{pmatrix}$$

Ein Gleichungssytem $A \cdot x = b$ mit einer Matrix in Zeilen Stufen-Form zu lösen ist leicht rekursiv möglich. In der Tat erhällt man so unmittelbar alle Lösungen des LGS.

Definition 7.4.5.

Für eine Gleichung $A \cdot x = b$ mit $A \in \mathbb{R}^{m \times n}$ und $b \in \mathbb{R}^m$ ist das zugehörige Tableau

$$\left(\begin{array}{ccc|c} A_{1,1} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & \vdots \\ A_{m,1} & \dots & A_{m,n} & b_m \end{array}\right)$$

Die Lösungen eines Tableaus sind die Lösungen der zugehörigen Gleichung $A \cdot x = b$.

Zwei Tableaus heißen *äquivalent*, wenn sie dieselben Lösungen haben.

Im Gaußverfahren sind folgende Schritte Zulässig auf einem Tabeau:

Lemma 7.4.6.

Die Lösungen eines Tableaus verändern sich nicht, wenn man einen der folgenden Schritte anwendet:

- **G1.** Addiere das Vielfache einer Zeile zu einer ***anderen*** Zeile.
- **G2.** Multipliziere eine Zeile des Tableaus mit einer Zahl.
- **G3.** Vertausche zwei Zeilen des Tableaus.
- **G4.** Streiche eine Nullzeile (eine Zeile deren Einträge alle Null sind).

. . . wobei jeweils die anderen Zeilen des Tableaus unberührt bleiben.

In einer früheren Version des Skripts hießen die unterschiedlichen Schritte noch *Typ 1)* bis *Typ 4)*.

Der Beweis für Schritte **G1** bis **G3** ergibt sich direkt aus den Eigenschaften von Gleichungen.

Beispiel 7.4.7.

Gegeben sei $A := \begin{pmatrix} 2 & 1 & 1 \\ 4 & 3 & 3 \\ -6 & -5 & -5 \end{pmatrix}$ und $b := \begin{pmatrix} 1 \\ 3 \\ -5 \end{pmatrix}$ gesucht ist die Lösung x von $A \cdot x = b$

$$\left(\begin{array}{ccc|c} \mathbf{2} & 1 & 1 & 1 \\ 4 & 3 & 3 & 3 \\ -6 & -5 & -5 & -5 \end{array}\right) \quad \begin{matrix} \\ \text{II} - (2) \cdot \text{I} \\ \text{III} + (3) \cdot \text{I} \end{matrix} \quad \left(\begin{array}{ccc|c} 2 & 1 & 1 & 1 \\ 0 & \mathbf{1} & 1 & 1 \\ 0 & \mathbf{-2} & -2 & -2 \end{array}\right) \quad \begin{matrix} \\ \\ \text{III} + (2) \cdot \text{II} \end{matrix} \quad \left(\begin{array}{ccc|c} 2 & 1 & 1 & 1 \\ 0 & \mathbf{1} & 1 & 1 \\ 0 & \mathbf{0} & 0 & 0 \end{array}\right)$$

Das letzte Tableau hat bereits Zeilen-Stufen-Form. Die letzte Zeile übersetzt sich zu der Gleichung $0 = 0$, die die Lösungsmenge nicht einschränkt. Diese Gleichung kann also gestrichen werden. Nach Streichen der letzten Nullzeile erhält man aus dem resultierenden Tableau die Gleichungen:

$$\begin{array}{lrrrrr} \text{I} & 2 \cdot x_1 & +1 \cdot x_2 & +1 \cdot x_3 & = & 1 \\ \text{II} & 0 \cdot x_1 & +1 \cdot x_2 & +1 \cdot x_3 & = & 1 \end{array}$$

Setzt man $x_3 := \lambda$ mit $\lambda \in \mathbb{R}$ so erhält man nach umstellen:

$$\left.\begin{array}{lrrrrrl} \text{I} & 2 \cdot x_1 & = & 1 & -x_2 & -x_3 & \overset{\text{II}}{=} 1 - (1 - \lambda) - \lambda = 0 \\ \text{II} & x_2 & = & 1 & -x_3 & = & 1 - \lambda \end{array}\right\} \quad \Longrightarrow \quad x = \begin{pmatrix} 0 \\ 1 - \lambda \\ \lambda \end{pmatrix} \text{ mit } \lambda \in \mathbb{R}$$

Die Lösungsmenge lautet also: $\mathbb{L} := \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \; : \; \lambda \in \mathbb{R} \right\}$

7.4.1. Allgemeine Worte zur Lösungsmenge

Spezielle Lösung des LGS plus homogene Lösung.

7.4.2. Interpretation eines Tableaus mit Nullzeilen

Das Interpretieren eines Tableaus mit Nullzeile ist üblicherweise anfänglich etwas schwierig, aber im Grunde genommen einfach: Eine Nullzeile entspricht einer Gleichung $0 = 0$, und weil diese Gleichung immer wahr ist, schränkt sie die Startmenge $\mathbb{R}^n$ nicht ein.

- "Fragt" man alle $x \in \mathbb{R}$, ob sie $x^2 = 4$ erfüllen, so "antworten" nur 2 und -2 mit ja:
  $\{x \in \mathbb{R} \; : \; x^2 = 4\} = \{-2, 2\}$
- "Fragt" man alle $x \in \mathbb{R}$, ob sie $0 = 0$ erfüllen, so "antworten" *alle* mit ja, denn diese Gleichung ist stets erfüllt! Es gilt also:
  $\{x \in \mathbb{R} \; : \; 0 = 0\} = \mathbb{R}$
- "Fragt" man alle $x \in \mathbb{R}$, ob sie $0 = 1$ erfüllen, so "antworten" *alle* mit nein, denn diese Gleichung ist immer falsch! Es gilt also:
  $\{x \in \mathbb{R} \; : \; 0 = 1\} = \emptyset$

Bemerkung 7.4.8 (Nullzeilen)**.**

Hat man ein Tableau, dass (am Ende) eine Nullzeile enthält, so entspricht dies der folgenden Situation:

Das Tableau hat einen "Vorspann" aus einer Matrix $A \in \mathbb{R}^{m \times n}$ und $b \in \mathbb{R}^m$, gefolgt von einer Nullzeile. Dieses Tableau hat dann die selben Lösungen wie $A \cdot x = b$:

Tableau:
$$\left(\begin{array}{ccc|c} A_{1,1} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & \vdots \\ A_{m,1} & \dots & A_{m,n} & b_m \\ 0 & \dots & 0 & 0 \end{array}\right)$$

Gleichungssystem
$$\left[\begin{array}{cccc} A_{1,1}x_1 & + \ldots + & A_{1,n}x_n & = b_1 \\ & & & \vdots \\ A_{m,1}x_1 & + \ldots + & A_{m,n}x_n & = b_m \\ & & 0 & = 0 \end{array}\right.$$

Die Lösungen dieses Systems sind:

$$\{x \in \mathbb{R}^n \ : \ A \cdot x = b\} \ \bigcap \ \underbrace{\{x \in \mathbb{R}^n \ : \ 0 = 0\}}_{=\mathbb{R}^n} \ = \ \{x \in \mathbb{R}^n \ : \ A \cdot x = b\}$$

Bemerkung 7.4.9 (Fast-Nullzeilen)**.**

Hat man ein Tableau, dass (am Ende) eine Nullzeile mit Rechter Seite ungleich Null enthält, so hat das zugehörige Gleichungssytem **keine Lösung**

Allgemein sieht dies wie folgt aus: Nach umsortieren der Zeilen, hat das Tableau hat einen "Vorspann" aus einer Matrix $A \in \mathbb{R}^{m \times n}$ und $b \in \mathbb{R}^m$, gefolgt von einer weiteren Zeile:

Tableau:
$$\left(\begin{array}{ccc|c} A_{1,1} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & \vdots \\ A_{m,1} & \dots & A_{m,n} & b_m \\ \hline 0 & \dots & 0 & \mathbf{1} \end{array}\right)$$

Gleichungssystem
$$\left[\begin{array}{ccccc} A_{1,1}x_1 & +\ldots+ & A_{1,n}x_n & = & b_1 \\ & & & & \vdots \\ A_{m,1}x_1 & +\ldots+ & A_{m,n}x_n & = & b_{m-1} \\ & & 0 & = & \mathbf{1} \end{array}\right.$$

Die Lösungen dieses Systems sind:

$$\{x \in \mathbb{R}^n \ : \ A \cdot x = \vec{b}\} \ \bigcap \ \underbrace{\{x \in \mathbb{R}^n \ : \ 0 = \mathbf{1}\}}_{=\emptyset} \ = \ \emptyset$$

7.4.3. Interpretation eines Tableaus mit Sprüngen

Hat in einem Tableau eine Zeile $z+1$ mehr als eine führende Nullen mehr als die vorhergehende Zeile so bezeichnet man dies als einen "Sprung". Die folgende Matrix hat zwei Sprünge:

- einen Sprung der Länge 3 von Zeile 2 zu Zeile 3
- einen Sprung der Länge 2 von Zeile 4 zu Zeile 5

$$\left(\begin{array}{ccccc|cc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Länge 3 Länge 2

Hat ein Tableau in Zeilen-Stufen-Form einen Sprung der Länge k, so bedeutet dies, dass sich $k-1$ der gegebenen Variablen *nicht konkret* festlegen lassen (s. Beispiel 7.4.7). Diese Variablen bleiben als Variablen in der Lösung erhalten, man drückt dies durch ersetzen der Variable mit einer weiteren, neuen Variable (meist Griechische Lettern) aus.

Beispiel 7.4.10.

$$\left(\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & 1 & 9 \\ 0 & 1 & 2 & 0 & 4 & 7 \\ 0 & 0 & 0 & 1 & 1 & 5 \end{array}\right) \longrightarrow \begin{array}{l} x_1 = 9 \quad -x_3 \quad -x_5 \\ x_2 = 7 \quad -2x_3 \quad -4x_5 \\ x_4 = 5 \quad -x_5 \end{array}$$

Hier lässt sich

- x_1 nur ausdrücken in Abhängigkeit von x_3 und x_5 (oder umgekehrt).
- x_2 nur ausdrücken in Abhängigkeit von x_3 und x_5 (oder umgekehrt).
- x_4 nur ausdrücken in Abhängigkeit von x_5 (oder umgekehrt).

Hat man dies getan (s. Gleichungen oben), und legt man x_5 und x_3 fest, so lassen sich *alle* weiteren Variablen aus x_5 und x_3 berechnen. D.h. für *alle* Werte von x_5 und x_3 gibt es eine Lösungsvektor x.

Die Lösung hat also 2 Freiheitsgrade, bzw. ist 2 dimensional. Konkret erhält man mit $x_3 := \lambda_1$ und $x_5 := \lambda_2$ die Lösungsmege:

$$\mathbb{L} = \left\{ \begin{pmatrix} 9 & -\lambda_1 & -\lambda_2 \\ 7 & -2\lambda_1 & -4\lambda_2 \\ & \lambda_1 & \\ 5 & & -\lambda_2 \\ & & \lambda_2 \end{pmatrix} : \lambda_1, \lambda_2 \in \mathbb{R} \right\}$$

7.4.4. Gauß'sches Eliminationsverfahren im Kleid der Matrixmultiplikation

Die nach Lemma 7.4.6 erlaubten Umformungsschritte lassen sich auch als "Matrixmultiplikation von links" beschreiben. Dabei entspricht für ein gegebenes LGS $A \cdot x = b$ die Umformung der einzelnen Typen 1) bis 3) jeweils der Multiplikation der Matrix A mit einer spezifischen Matrix von links.

Um diese beschreiben zu können sei

- $S[i, j]$ die $m \times m$-Matrix, die aus der Einheitsmatrix id durch Vertauschen der $i$ten und der j-ten Zeile hervorgeht.
- $T[i, j, \lambda]$ die $m \times m$-Matrix, deren Diagonaleinträge alle gleich 1 sind, deren Eintrag in Zeile i und Spalte j gleich λ ist, und deren übrige Einträge gleich 0 sind (ist $i = j$, dann ist der entsprechende Diagonaleintrag in Zeile und Spalte i gleich $z \in \mathbb{R}$).
- $U[i]$ die $m \times (m-1)$-Matrix, die aus der Einheitsmatrix id durch Weglassen der $i$ten Zeile hervorgeht.

Bemerkung 7.4.11.

Man rechnet leicht nach, dass $S[i, j] \cdot S[i, j] = \text{id}$ ist, also $S[i, j]$ für alle $i, j \in \{1, \ldots, m\}$ invertierbar ist.
Außerdem entspricht $S[i, j] \cdot A$ der Matrix, die aus A durch Vertauschen der Zeilen i und j hervorgeht.

Man rechnet ebenfalls leicht nach, dass $T[i, j, z] \cdot T[i, j, -z] = \text{id}$ ist, also $T[i, j, z]$ für alle $i, j \in \{1, \ldots, m\}$ invertierbar ist.
Außerdem entspricht $T[i, j] \cdot A$ der Matrix, die aus A durch Addition des z-fachen der Zeile j zur Zeile i hervorgeht.

Es entspricht $U[i] \cdot A$ der Matrix, die aus A durch Weglassen der Zeile i hervorgeht.

Beispiel 7.4.12.

Es sei $A = \begin{pmatrix} 1 & 4 & 3 \\ 2 & 11 & 1 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix}$. Dann ist

$$S[2,4] \cdot A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & 3 \\ 2 & 11 & 1 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 \\ 1 & 16 & 3 \\ 0 & 4 & 8 \\ 2 & 11 & 1 \end{pmatrix}$$

$$T[1,3,\frac{1}{2}] \cdot A = \begin{pmatrix} 1 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & 3 \\ 2 & 11 & 1 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 7 \\ 2 & 11 & 1 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix}$$

$$T[2,2,3] \cdot A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & 3 \\ 2 & 11 & 1 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 \\ 6 & 33 & 3 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix}$$

$$U[3] \cdot A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & 3 \\ 2 & 11 & 1 \\ 0 & 4 & 8 \\ 1 & 16 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 \\ 2 & 11 & 1 \\ 1 & 16 & 3 \end{pmatrix}$$

Wir finden für die einzelnen Typen der Umformung der Matrix A im Gauß'schen Eliminationsverfahren die folgenden korrespondierenen Matrizenmultiplikationen von links der Matrix A:

G1.	Addition des z-fachen der Zeile i zur Zeile j	$T[i,j,z] \cdot A$
G2.	Multiplizieren der Zeile i mit einer Zahl z	$T[i,i,z] \cdot A$
G3.	Vertauschen der Zeilen i und j	$S[i,j] \cdot A$
G4.	Streichen der Nullzeile i (eine Zeile deren Einträge alle Null sind).	$U[i] \cdot A$

Bemerkung 7.4.13.

Um das zugehörige Tableau nach einem Umformungsschritt zu erhalten, multipliziert man nicht bloß die Matrix A mit einer der Umformungsmatrizen, sondern auch den Vektor b.

Satz 7.4.14.

Zu jeder $m \times n$-Matrix A gibt es eine invertierbare $m \times m$-Matrix C, so dass $C \cdot A$ Zeilenstufenform hat.

Beweis. Wir haben gesehen, daß eine Matrix durch das Gauß'schen Eliminationsverfahren in Zeilenstufenform gebracht werden kann. Die Operationen **G1** bis **G3**, die im Gauß'schen Eliminationsverfahren durchgeführt werden, entsprechen einfach der Multiplikation von links mit invertierbaren $m \times m$-Matrizen der Form $S[i,j]$ oder $T[i,j,z]$. Die Matrix C ist das Produkt derselben. □

Für den Beweis der folgenden Aussage sei daran erinnert, dass für eine Matrix $A \in \mathbb{R}^{m\times n}$ und eine Matrix $B \in \mathbb{R}^{n\times m}$ gilt $(B \cdot A)^T = A^T \cdot B^T$.

Korollar 7.4.15.

Zu jeder $m \times n$-Matrix A gibt es eine invertierbare $m \times m$-Matrix C und eine invertierbare $n \times n$-Matrix D und eine Zahl $r \leq \min\{m, n\}$, so dass $C \cdot A \cdot D = E_r$, wobei E_r die Matrix ist, deren erste r Diagonaleinträge gleich 1 sind und deren übrige Einträge gleich 0 sind.

Beweis. Zunächst wenden wir das Gauß'sche Eliminationsverfahren an, um eine invertierbare Matrix C zu erhalten, so daß $C \cdot A$ Zeilenstufenform hat. Dann wenden wir das Gauß'sche Eliminationsverfahren auf die transponierte Matrix $(C \cdot A)^T$ an. Dies gibt eine invertierbare $n \times n$-Matrix F, so dass $F \cdot (C \cdot A)^T$ eine $n \times m$-Matrix ist, die nur auf der Diagonalen von Null verschiedene Einträge hat. Durch Multiplikation mit einer geeigneten invertierbaren $n \times n$-Diagonalmatrix G kann man erreichen, daß die Matrix $G \cdot F \cdot (C \cdot A)^T$ Diagonalform hat mit Einträgen 1 oder 0. Die transponierte Matrix $C \cdot A \cdot (G \cdot F)^T$ ist also eine $m \times n$-Matrix in Diagonalform mit Einträgen 1 oder 0, und die Matrix $D = (G \cdot F)^T$ ist invertierbar. □

Korollar 7.4.15 liefert eine erste Lösung des Problems, eine lineare Abbildung durch eine möglichst einfache Matrix darzustellen. Sehen wir nämlich die $m \times n$-Matrix A als eine lineare Abbildung $f : R^n \to \mathbb{R}^m, x \mapsto A \cdot x$, so gibt Korollar 7.4.15 Basen $\mathcal{A}, \mathcal{B}$ von $\mathbb{R}^n$ und $\mathbb{R}^m$, so dass $M_{\mathcal{A},\mathcal{B}}(f) = E_r$. Genauer ist $\mathcal{A}$ die Basis, die aus den Spalten der Matrix D besteht, während $\mathcal{B}$ aus den Spalten von C^{-1} besteht. Zwar ist $M_{\mathcal{A},\mathcal{B}}(f) = E_r$ eine sehr einfache Matrix und diese Darstellung ist auch durchaus hilfreich (s. die folgenden Anwendungen). Jedoch sind leider die Basen $\mathcal{A}, \mathcal{B}$ im allgemeinen nicht besonders "schön". Wir setzen uns daher weiterhin das (zugegebenermaßen etwas vage) Ziel, lineare Abbildungen durch möglichst einfache Matrizen darzustellen, allerdings bezüglich möglichst "schöner" Basen.

7.4.5. Zeilen- und Spaltenrang

Ist A eine $m \times n$-Matrix, so sind die Zeilen $A_{(1)}, \ldots, A_{(m)}$ Vektoren in $\mathbb{R}^n$. Die Spalten $A^{(1)}, \ldots, A^{(n)}$ sind Vektoren in R^m.

Definition 7.4.16.

Für eine Matrix $A \in \mathbb{R}^{m\times n}$ sei der ***Zeilenrang*** von A definiert als

$$\dim\left(\mathsf{span}\left(A_{(1)}, \ldots, A_{(m)}\right)\right)$$

und der ***Spaltenrang*** von A definiert als

$$\dim\left(\mathsf{span}\left(A^{(1)}, \ldots, A^{(n)}\right)\right).$$

Bemerkung 7.4.17.

Wir haben als das Bild von A den Aufspann der Spaltenvektoren $A^{(1)}, \ldots, A^{(n)}$ definiert. Also ist der Spaltenrang gleich $\dim(\mathsf{Bild}(A))$.

Korollar 7.4.18.

Für jede Matrix A stimmen Zeilen- und Spaltenrang überein.

Beweis. Mit den Bezeichnungen von Korollar 7.4.15 sieht man, dass r sowohl der Zeilen- als auch der Spaltenrang von A ist. □

Bemerkung 7.4.19.

Aufgrund von Korollar 7.4.18 kann man einfach vom Rang der Matrix A sprechen.

Korollar 7.4.20.

Sei A eine $m \times n$-Matrix und $b \in \mathbb{R}^m$. Es gibt genau dann ein $x \in \mathbb{R}^n$ mit $A \cdot x = b$, wenn die Matrix A den selben Rang hat wie die Matrix (A, b), die aus A durch Hinzufügen von b als $n+1$ter Spalte entsteht.

Korollar 7.4.21.

Sei A eine $m \times n$-Matrix vom Rang r. Sei l die Dimension des Kerns von A.

- Dann gilt $n = r + l$.
- Ferner ist A genau dann invertierbar, wenn $m = n = r$.

Beweis. Die erste Aussage folgt direkt aus Lemma 7.2.4, dem Dimensionssatz.
Zur zweiten Aussage müssen wir zwei Richtungen Zeigen:

"⇒" Wenn A invertierbar ist, muss notwendigerweise $m = n$ gelten. Außerdem ist in diesem Fall die lineare Abbildung, für welche A die Darstellungsmatrix ist, bijektiv, d.h. der Kern besteht nur aus dem Nullvektor. Aus der ersten Behauptung folgt also $r = n$.

"⇐" Wenn umgekehrt $r = n$ ist, dann ist $C \cdot A \cdot D = \mathrm{id}$. Die inverse Matrix von A ist also einfach $D \cdot C$. Denn

$$\begin{aligned} & C \cdot A \cdot D = \mathrm{id} \\ \Leftrightarrow \quad & C^{-1} \cdot C \cdot A \cdot D = C^{-1} \cdot \mathrm{id} \\ \Leftrightarrow \quad & C^{-1} \cdot C \cdot A \cdot D \cdot D^{-1} = C^{-1} \cdot \mathrm{id} \cdot D^{-1} \\ \Leftrightarrow \quad & A = C^{-1} \cdot D^{-1} \end{aligned}$$

Dann ist $A^{-1} = \left(C^{-1} \cdot D^{-1}\right)^{-1} = (D^{-1})^{-1} \cdot (C^{-1})^{-1} = D \cdot C$.

□

Wie der letzte Beweis zeigt, erlauben uns die Umformungsregeln des Gaußverfahrens, zu einer gegebenen $n \times n$-Matrix A festzustellen, ob sie invertierbar ist, und ggf. ihre inverse Matrix zu berechnen. Dazu geht man wie folgt vor. Zunächst bringt man die Matrix A mit dem Gaußverfahren auf Zeilenstufenform. An der Zeilenstufenform von A kann man den Rang ablesen und A ist genau dann invertierbar, wenn der Rang gleich n ist. In diesem Fall führt man weitere Zeilenumformungen durch, bis aus A eine Diagonalmatrix geworden ist. Dann multipliziert man jede Zeile mit einer reellen Zahl, um die Einheitsmatrix id zu erhalten. Parallel dazu führt man dieselben Umformungen ausgehend von der Einheitsmatrix id durch. Die Matrix B, die dabei aus der Einheitsmatrix entsteht, ist A^{-1}.

Beispiel 7.4.22.

Wir invertieren die Matrix

$$A = \begin{pmatrix} -1 & -1 & 0 & 2 \\ -1 & 0 & 0 & 3 \\ -1 & 0 & 1 & 2 \\ 2 & 1 & 0 & -4 \end{pmatrix}$$

Zunächst subtrahieren wir die ertse Zeile von der zweiten und dritten und addieren ihr 2-faches zur vierten. Dieselben Umformungen führen wir auch ausgehend von der Matrix id durch und erhalten

$$\begin{pmatrix} -1 & -1 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}.$$

Als nächstes subtrahieren wir die zweite Zeile von der dritten und addieren sie zur vierten

$$\begin{pmatrix} -1 & -1 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

An dieser Stelle erkennen wir, dass die Matrix A Rang 4 hat, also invertierbar ist. Wir fahren fort, indem wir die letzte Zeile zur dritten Zeile addieren, von der zweiten Zeile abziehen und zweimal von der ersten Zeile abziehen. Dieselben Umformungen führen wir an der rechten Matrix durch und erhalten

$$\begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} -1 & -2 & 0 & -2 \\ -2 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Als nächsten Schritt addieren wir in beiden Matrizen die zweite Zeile zur ersten. Dies ergibt

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} -3 & -2 & 0 & -3 \\ -2 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Schließlich multiplizieren wir die erste Zeile beider Matrizen mit -1

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 3 & 2 & 0 & 3 \\ -2 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Wir haben also ausgerechnet, dass

$$A^{-1} = \begin{pmatrix} 3 & 2 & 0 & 3 \\ -2 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

8 Die Determinante

8.1. Überblick

In diesem Abschnitt ordnen wir einer quadratischen Matrix eine reelle Zahl zu, die gewisse geometrische Eigenschaften der Matrix widerspiegelt.

Genauer gilt: Für eine $A \in \mathbb{R}^{n\times n}$ misst die Determinante das (orientierte) Volumen des von den Spalten von A aufgespannten Parallelotops im $\mathbb{R}^n$ (s. Def 8.1.1, Bsp. 8.1.2). Dieses Volumen hat den Wert 0 genau dann, wenn die Spalten von A linear abhängig sind. Diese geometrische Interpretation als Volumen der Determinante ist jedoch nur eine *Hilfe*, um sich die Regeln bei der Deteminantenberechnung dauerhaft merken zu können.

Wichtig sind die drei folgenden Einsichten:

- Es gilt $\det(A) = 0$ genau dann wenn die Spalten von A linear abhängig sind.
- Die Determinante ist multilinear (dies Hilft beim Berechnen per Gauß-Verfahren).
- Die Determinante lässt sich...
  - per Zeilen- oder Spaltenentwicklung berechnen
    (Verfahren hat theoretische Bedeutung, in der Praxis nur für kleine Matrizen geeignet)
  - per Gauß-Verfahren berechnen
    (Verfahren hat große praktische Bedeutung).

Geometrische Interpretation:
Hat die *quadratische* Matrix $A \in \mathbb{R}^{n\times n}$ die Spalten $A^{(1)}, \dots A^{(n)} \in \mathbb{R}^n$, so ist die Determinante von A das *orientierte* Volumen, des von $A^{(1)}, \dots, A^{(n)}$ aufgespannten Parallelotops[4] im $\mathbb{R}^n$.

Die Orientierung bedeutet hier ein Vorzeichen, dass die Reihenfolge der Vektoren wiederspiegelt.

Definition 8.1.1.

Für n Vektoren $a_1, \dots, a_n \in \mathbb{R}^n$ sei

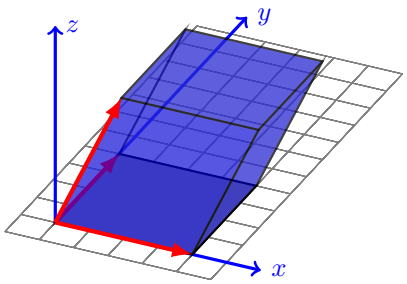
$$\mathsf{P}(\{a_1, \dots, a_n\}) := \{\lambda_1 \cdot a_1 + \dots + \lambda_n \cdot a_n \ : \ 0 \le \lambda_1, \dots, \lambda_n \le 1\}\,.$$

Für die Matrix $A \in \mathbb{R}^{n\times n}$ mit Spalten $A^{(1)}, \dots, A^{(n)}$ schreibt man auch kurz $\mathsf{P}(A)$ für $\mathsf{P}(\{A^{(1)}, \dots, A^{(n)}\})$

Beispiel 8.1.2.

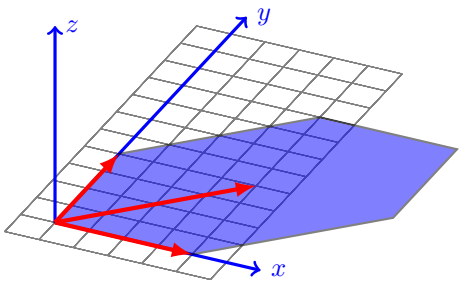
Sind die $A^{(1)}, \dots A^{(n)}$ linear **un**abhängig	so ist $\mathsf{P}(A)$ das Parallelotop mit Kanten parallel zu den $A^{(i)}$.
Sind die $A^{(1)}, \dots A^{(n)}$ linear **ab**hängig	so ist $\mathsf{P}(A)$ ***flach***.

[4] das Parallelotop ist die mehrdimensionale Verallgemeinerung des Parallelogramms im $\mathbb{R}^2$.



Das Parallelotop $\mathsf{P}\left(\begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}\right)$

Volumen ist 8 = Höhe 2 mal Grundfläche 4



Das Parallelotop $\mathsf{P}\left(\begin{pmatrix}2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}2\\2\\0\end{pmatrix}\right)$ ist **flach**.

Volumen ist 0

Was wir bisher wissen: Die Determinante $\det(A)$ einer Matrix $A \in \mathbb{R}^{n\times n}$ ist das orientierte Volumen von $\mathsf{P}(A)$ (die Genaue Definition folgt in Definition 8.2.4). Das *tatsächliche* Volumen ist in den seltensten Fällen interessant! Was wirklich interessiert ist der Fall $\det(A) = 0$:

Lemma 8.1.3.

In einer quadratischen Matrix A sind die Spalten linear **ab**hängig genau dann wenn $\det(A) = 0$ gilt.

Eine Richtung dieser Aussage ist leicht zu sehen: Sind die Spalten von A linear **ab**hängig, so ist der Körper $\mathsf{P}(A)$ relativ zum Raum $\mathbb{R}^n$ flach. Das Volumen hat in diesem Falle den Wert 0.

$$\text{Spalten von } A \text{ sind linear abhängig} \Rightarrow \mathsf{P}(A) \text{ ist flach} \Rightarrow \operatorname{vol}(\mathsf{P}(A)) = 0 \Rightarrow \det(A) = 0$$

Das die Umkehrungen "$\Leftarrow$" hier auch gelten werden wir später zeigen.

Die Determinante ist also insbesondere ein (schneller!) Weg zu entscheiden, ob Vektoren linear abhängig sind.

8.2. Definition

Wir definieren die Determinante zunächst in ihrer Allgemeinheit, um dann festzustellen, dass die Definition zu sperrig ist, um sie tatsächlich für eine Berechnung zu verwenden. Nach der Definition werden wir einen Weg kennenlernen, die Determinante systematisch zu berechnen, der allerdings sehr viel Rechenaufwand erfordert. Für die Spezialfälle $n = 2, 3$ werden wir einfache Formeln (oder besser Merkhilfen der Formel aus der Definition für diese Fälle) kennenlernen und dann beobachten, dass für allgemeine Fälle die Determinante mit Hilfe des Gauß-Verfahrens berechnet werden kann.

Um die Determinante formal korrekt zu definieren, müssen wir uns zunächst mit Permutationen befassen.

Exkurs 8.2.1 (Permutationen)**.**

- Eine Permutation der Länge n ist eine Bijektion $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$.
- Wir schreiben eine Permutation auch als $[\sigma(1), \sigma(2), \dots, \sigma(n)]$.
- Wir bezeichnen die Menge aller Permutationen der Länge n mit S_n.
- Es ist $|S_n| = n!$ (Beweis beispielsweise über vollständige Induktion.)

- Ferner definieren wir das ***Vorzeichen*** oder ***Signum*** von $\sigma \in S_n$ als

$$\operatorname{sign}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Das Signum ist gleich 1, wenn die Anzahl der "Fehlstände" (ein Fehlstand liegt dann vor, wenn $\sigma(i) > \sigma(j)$, wenn $i < j$) der gerade ist und -1, wenn sie ungerade ist.

Beispiel 8.2.2.

Sei $n = 3$, dann findet man:

- $S_3 = \{[123], [132], [213], [231], [312], [321]\}$.
- Tatsächlich ist $|S_3| = 3! = 6$.
- Betrachtet man die Permutation $[312]$ so lässt sich also leicht ablesen, dass $\sigma(1) = 3, \sigma(2) = 1$ und $\sigma(3) = 2$ ist, also die 1 auf die 3, die 2 auf die 1 und die 3 auf die 2 abgebildet wird.
- Um das Vorzeichen zu bestimmen, schreibt man die Urbilder in aufsteigender Reihenfolge nebeneinander und die entsprechenden Bilder unter die Urbilder. Dann verbindet man identische Urbilder und Bildern und zählt die Kreuzungen:

i	1	2	3
$\sigma(i)$	3	1	2

Es treten für $[312]$ also zwei Kreuzungen auf - dies entspricht der Anzahl der Fehlstände. Da die Anzahl der Fehlstände gerade ist, ist das Vorzeichen also 1. Wir haben also $\operatorname{sign}([312]) = 1$.

Es gilt die folgende Rechenregel für das Signum zweier Permutationen.

Lemma 8.2.3.

Es gilt:

- Für alle $\sigma \in S_n$ ist $\operatorname{sign}(\sigma) \in \{-1, 1\}$.
- Für alle $\sigma, \tau \in S_n$ ist $\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau)$.

Beweis. Die erste Aussage folgt aus der folgenden Identität.

$$\operatorname{sign}(\sigma)^2 = \left(\prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \right)^2 = \prod_{i \ne j} \frac{\sigma(i) - \sigma(j)}{i - j} = 1.$$

Die letzte Gleichheit gilt, weil σ eine Permutation ist (jeder Nenner taucht genauso oft auf wie jeder Zähler). Daraus folgt, dass $\operatorname{sign}(\sigma) \in \{-1, 1\}$.

Den Beweis für die zweite Aussage überlassen wir dem Leser (ist nicht ganz einfach einzusehen). □

Wir definieren nun die Determinante über die Leibniz-Formel. Die Formel ist nach dem deutschen Mathematiker Gottfried Wilhelm Leibniz benannt.

Definition 8.2.4 ("Leibniz-Formel")**.**

Die ***Determinante*** einer Matrix $A \in \mathbb{R}^{n\times n}$ ist

$$\det(A) = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} A_{i\sigma(i)}.$$

Die Summe läuft über alle Permutationen in S_n, involviert also insgesamt $n!$ viele Summanden. Jeder Summand besteht aus dem Vorzeichen einer Permutation und dem Produkt von n vielen Matrixeinträgen, aus jeder Zeile und jeder Spalte genau einen (entsrechend der zu dem Summanden gehörenden Permutation). Wir rechnen direkt ein Beispiel:

Beispiel 8.2.5.

Sei $A \in \mathbb{R}^{3\times 3}$, also $n = 3$ mit

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Dann ist $S_3 = \{[123], [132], [213], [231], [312], [321]\}$ mit $|S_3| = 3! = 1 \cdot 2 \cdot 3 = 6$. Wir haben

$$\operatorname{sign}([123]) = 1 \qquad \operatorname{sign}([213]) = -1 \qquad \operatorname{sign}([312]) = 1$$

$$\operatorname{sign}([132]) = -1 \qquad \operatorname{sign}([231]) = 1 \qquad \operatorname{sign}([321]) = -1$$

Dann ist

$$\begin{aligned}
\det(A) &= \sum_{\sigma\in S_3} (\operatorname{sign}(\sigma) && \cdot && \prod_{i=1}^{3} A_{i\sigma(i)}) \\
&= \quad 1 && \cdot && A_{11}\cdot A_{22}\cdot A_{33} \\
&\quad + (-1) && \cdot && A_{11}\cdot A_{23}\cdot A_{32} \\
&\quad + (-1) && \cdot && A_{12}\cdot A_{21}\cdot A_{33} \\
&\quad + 1 && \cdot && A_{12}\cdot A_{23}\cdot A_{31} \\
&\quad + 1 && \cdot && A_{13}\cdot A_{21}\cdot A_{32} \\
&\quad + (-1) && \cdot && A_{13}\cdot A_{22}\cdot A_{31} \\
&= \quad 1 && \cdot && 1\cdot 5\cdot 9 \\
&\quad + (-1) && \cdot && 1\cdot 6\cdot 8 \\
&\quad + (-1) && \cdot && 2\cdot 4\cdot 9 \\
&\quad + 1 && \cdot && 2\cdot 6\cdot 7 \\
&\quad + 1 && \cdot && 3\cdot 4\cdot 8 \\
&\quad + (-1) && \cdot && 3\cdot 5\cdot 7 \\
&= 0
\end{aligned}$$

Wir erinnern, dass die Zeilen einer $n \times n$-Matrix A mit $A_{(1)}, \ldots, A_{(n)}$ bezeichnet werden.

Die folgende Proposition listet insgesamt neun Eigenschaften auf, die für die Determinante gelten.

Proposition 8.2.6.

Seien A, B, C drei $n \times n$-Matrizen. Die Determinante hat die folgenden Eigenschaften

DET1. $\det(\mathrm{id}) = 1$.

DET2. Falls A zwei identische Zeilen hat, gilt $\det(A) = 0$.

DET3. Die Determinante ist linear in jeder Zeile, d.h. die beiden folgenden Bedingungen sind erfüllt.

- Angenommen es gibt ein $i \in \{1, \ldots, n\}$, so dass $A_{(i)} + B_{(i)} = C_{(i)}$, während $A_{(h)} = B_{(h)} = C_{(h)}$ für alle $h \neq i$. Dann gilt $\det(A) + \det(B) = \det(C)$.
- Angenommen es gibt ein $i \in \{1, \ldots, n\}$ und ein $z \in \mathbb{R}$ so dass $B_{(i)} = z \cdot A_{(i)}$, während $B_{(h)} = A_{(h)}$ für alle $h \neq i$. Dann gilt $\det(B) = z \cdot \det(A)$.

Insbesondere gilt $\det(A) = 0$ wenn A eine Zeile hat, die nur aus 0en besteht.

DET4. Wenn B aus A durch Vertauschen von zwei Zeilen entsteht, gilt $\det(B) = -\det(A)$.

DET5. Seien $i, j \in \{1, \ldots, n\}$ verschieden und $z \in \mathbb{R}$. Wenn B aus A durch Addition des z-fachen der $i$ten Zeile zur j-ten Zeile entsteht, gilt $\det(B) = \det(A)$.

DET6. Wenn A in Zeilen-Stufen-Form ist, gilt $\det(A) = \prod_{i=1}^{n} A_{ii}$.

DET7. Es gilt $\det(A \cdot B) = \det(A) \cdot \det(B)$.

DET8. Die Matrix A ist invertierbar genau dann, wenn $\det(A) \neq 0$. In diesem Fall gilt $\det(A) = \det(A^{-1})^{-1} = \frac{1}{\det(A^{-1})}$.

DET9. Es gilt $\det(A^T) = \det(A)$.

Beweis.

- **DET1:** Folgt unmittelbar aus der Definition.
- **DET2:** Wir nehmen an, dass die Zeilen i_1 und i_2 von A identisch sind ($i_1 \neq i_2$). Sei $\tau \in S_n$ die Permutation, die die Zahlen i_1 und i_2 vertauscht, während $\tau(h) = h$ für alle $h \in \{1, \ldots, n\} \setminus \{i_1, i_2\}$. Dann gilt

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)} = \frac{1}{2} \sum_{\sigma \in S_n} \left[\mathrm{sign}(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)} + \mathrm{sign}(\sigma \circ \tau) \prod_{i=1}^{n} A_{i\sigma\circ\tau(i)} \right]. \quad (8.1)$$

Nun zeigt Lemma 8.2.3, dass $\mathrm{sign}(\sigma\circ\tau) = \mathrm{sign}(\sigma)\cdot\mathrm{sign}(\tau)$. Weil τ einfach zwei Zahlen i_1, i_2 vertauscht, zeigt die Definition von $\mathrm{sign}(\tau)$, dass $\mathrm{sign}(\tau) = -1$. Daher können wir (8.1) schreiben als

$$\det(A) = \frac{1}{2} \sum_{\sigma \in S_n} \left[\prod_{i=1}^{n} A_{i\sigma(i)} + \prod_{i=1}^{n} A_{i\sigma\circ\tau(i)} \right]. \quad (8.2)$$

Weil die i_1-te Zeile und die i_2-te Zeile von A übereinstimmen, erhalten wir

$$\begin{aligned}\prod_{i=1}^{n} A_{i\sigma(i)} =& A_{i_1\sigma(i_1)}A_{i_2\sigma(i_2)} \cdot \prod_{i\notin\{i_1,i_1\}} A_{i\sigma(i)} \\ =& A_{i_1\sigma(i_2)}A_{i_2\sigma(i_1)} \cdot \prod_{i\notin\{i_1,i_1\}} A_{i\sigma(i)} \\ =& A_{i_1\sigma\circ\tau(i_1)}A_{i_2\sigma\circ\tau(i_2)} \cdot \prod_{i\notin\{i_1,i_1\}} A_{i\sigma(i)} \\ =& \prod_{i=1}^{n} A_{i\sigma\circ\tau(i)}.\end{aligned}$$

Folglich zeigt (8.2), dass $\det(A) = 0$.

- **DET3:** Betracht A, B, C, so dass $A_{(i)} + B_{(i)} = C_{(i)}$, während alle anderen Zeilen der drei Matrizen übereinstimmen. Dann gilt

$$\begin{aligned}\det(C) &= \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) \prod_{j=1}^{n} C_{j\sigma(j)} = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma)(A_{i\sigma(i)} + B_{i\sigma(i)}) \prod_{j\neq i}^{n} C_{j\sigma(j)} \\ &= \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) A_{i\sigma(i)} \prod_{j\neq i}^{n} C_{j\sigma(j)} + \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) B_{i\sigma(i)} \prod_{j\neq i}^{n} C_{j\sigma(j)} \\ &= \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) A_{i\sigma(i)} \prod_{j\neq i}^{n} A_{j\sigma(j)} + \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) B_{i\sigma(i)} \prod_{j\neq i}^{n} B_{j\sigma(j)} \\ &= \det(A) + \det(B).\end{aligned}$$

  Der Nachweis der zweiten Bedingung geht analog.
- **DET4-DET8:** Diese Eigenschaften können aus **DET1-DET3** hergeleitet werden.
- **DET9:** Folgt aus Lemma 8.2.3 und der Definition der Determinante.

□

Bemerkung 8.2.7.

- Im Allgemeinen gilt nicht $\det(A + B) = \det(A) + \det(B)$.
- Die Eigenschaft **DET6** ist wenig überraschend. Jede andere Permutation als die Identität, welche zu dem Produkt der Diagonaleinträgen korrespondiert, involviert in dem Produkt mindestens ein Element unterhalb der Diagonalen. Diese Einträge sind allerdings bei einer Matrix in Zeilen-Stufen-Form alle gleich 0.
- Die Eigenschaft **DET1** folgt direkt aus Eigenschaft **DET6**, weil id in Zeilen-Stufen-Form ist.
- Aufgrund von **DET9** gelten **DET2-DET6** auch entsprechend für die Spalten der Matrix.

8.3. Berechnung der Determinante

Die Formel zur Berechnung der Determinante einer Matrix lässt sich in allgemeiner Dimension am Besten durch Verfahren ausdrücken. Wir werden zwei solcher Verfahren kennenlernen:

- Das Entwickeln der Determinante – dieses Verfahren hat theoretische Bedeutung, in der Praxis nur für kleine Matrizen geeignet.
- Berechnen per Gauß-Verfahren – dieses Verfahren hat große praktische Bedeutung.

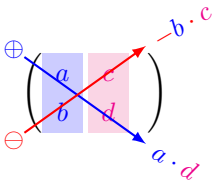
Aber zunächst lernen wir die Formeln für die Fälle $n = 2$ und $n = 3$ kennen.

8.3.1. Die Determinante in den Spezialfällen $n = 2$ und $n = 3$ bestimmen

Um $\det(A)$ mit $A \in \mathbb{R}^{2\times 2}$ bzw. $A \in \mathbb{R}^{3\times 3}$ zu berechnen gibt es Merkhilfen.

Lemma 8.3.1.

Es sei $A \in \mathbb{R}^{2\times 2}$ mit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ dann lässt sich $\det(A)$ über das Bilden von 2 Summanden berechnen:



Man erhält $\det(A) = a \cdot d - b \cdot c$

Beispiel 8.3.2.

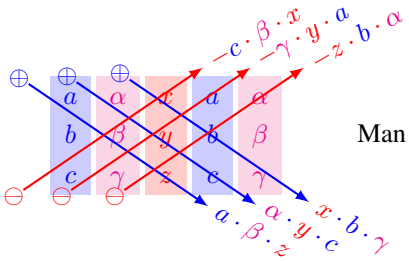
Sei $A = \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}$. Dann ist nach der Formel aus Lemma 8.3.1

$$\det(A) = 3 \cdot 6 - 5 \cdot 4 = -2.$$

Lemma 8.3.3 (Sarrusregel)**.**

Es sei $A \in \mathbb{R}^{3\times 3}$ mit $A = \begin{pmatrix} a & \alpha & x \\ b & \beta & y \\ c & \gamma & z \end{pmatrix}$ dann lässt sich $\det(A)$ über das Bilden von 6 Summanden berechnen.

Für das Ermitteln der Summanden schreibt man die drei Spalten von A in ein Schema und wiederholt die ersten beiden Spalten. Dann bildet man drei "Abwärts-Produkte" mit positivem Vorzeichen, und drei "Aufwärts-Produkte" mit negativem Vorzeichen. Die Determinante ist dann die Summe dieser 6 Produkte:



Man erhält: $\det(A) = \left\{ \begin{array}{lll} a \cdot \beta \cdot z & +\alpha \cdot y \cdot c & +x \cdot b \cdot \gamma \\ -c \cdot \beta \cdot x & -\gamma \cdot y \cdot a & -z \cdot b \cdot \alpha \end{array} \right.$

8.3.2. Die Determinante durch Entwicklung nach Zeile und Spalte bestimmen

Zunächst definieren wir für eine Matrix eine ganze Familie von Matrizen, die sogenannten Streichungsmatrizen. Die einzelnen Matrizen in dieser Familien entstehen durch das Streichen jeweils einer Zeile und einer Spalte der ursprünglichen Matrix. Es handelt sich bei den Streichungsmatrizen also um $(n-1)\times(n-1)$-Matrizen.

Definition 8.3.4 (Streichungsmatrix)**.**

Für eine Matrix $A \in \mathbb{R}^{\mathbf{n}\times\mathbf{n}}$ und zwei Indices $k, \ell \in \{1,\dots,n\}$

ist die *Streichungsmatrix* $A^{\cancel{k,\ell}} \in \mathbb{R}^{(\mathbf{n-1})\times(\mathbf{n-1})}$ die jenige Matrix, die aus A hervorgeht durch

Streichen der k-ten Zeile und Streichen der ℓ-ten Spalte :

$$A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,\ell-1} & A_{1,\ell} & A_{1,\ell+1} & \cdots & A_{1,n} \\ \vdots & & & \vdots & & & \vdots \\ A_{k-1,1} & \cdots & A_{k-1,\ell-1} & A_{k-1,\ell} & A_{k-1,\ell+1} & \cdots & A_{k-1,n} \\ A_{k,1} & \cdots & A_{k,\ell-1} & A_{k,\ell} & A_{k,\ell+1} & \cdots & A_{k,n} \\ A_{k+1,1} & \cdots & A_{k+1,\ell-1} & A_{k+1,\ell} & A_{k+1,\ell+1} & \cdots & A_{k+1,n} \\ \vdots & & & \vdots & & & \vdots \\ A_{n,1} & \cdots & A_{n,\ell-1} & A_{n,\ell} & A_{n,\ell+1} & \cdots & A_{n,n} \end{pmatrix}$$

$$A^{\cancel{k,\ell}} = \begin{pmatrix} A_{1,1} & \cdots & A_{1,\ell-1} & A_{1,\ell+1} & \cdots & A_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{k-1,1} & \cdots & A_{k-1,\ell-1} & A_{k-1,\ell+1} & \cdots & A_{k-1,n} \\ A_{k+1,1} & \cdots & A_{k+1,\ell-1} & A_{k+1,\ell+1} & \cdots & A_{k+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{n,1} & \cdots & A_{n,\ell-1} & A_{n,\ell+1} & \cdots & A_{n,n} \end{pmatrix}$$

Beispiel 8.3.5.

$$A := \begin{pmatrix} 1 & a & \alpha \\ 2 & b & \beta \\ 3 & c & \gamma \end{pmatrix} \quad \Rightarrow \quad A^{\cancel{2,2}} = \begin{pmatrix} 1 & a & \alpha \\ \cancel{2} & \cancel{b} & \cancel{\beta} \\ 3 & c & \gamma \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 3 & \gamma \end{pmatrix}$$

$$A^{\cancel{2,3}} = \begin{pmatrix} 1 & a & \alpha \\ \cancel{2} & \cancel{b} & \cancel{\beta} \\ 3 & c & \gamma \end{pmatrix} = \begin{pmatrix} 1 & a \\ 3 & c \end{pmatrix}$$

Lemma 8.3.6.

Für eine Matrix $A \in \mathbb{R}^{n\times n}$ mit $n \in \mathbb{N}$ gilt:

- Falls $n = 1$ gilt, so hat $A = (A_{1,1})$ genau einen Eintrag $A_{1,1} \in \mathbb{R}$ und des gilt $\det(A) = A_{1,1}$
- Falls $n > 1$ gilt, so können wir eine Spalte $\ell \in \{1, \dots, n\}$ wählen und nach dieser Spalte die Determinante *entwickeln*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+\ell} A_{i,\ell} \cdot \det\left(A^{\not i,\not \ell}\right)$$

Bemerkung 8.3.7.

Das Vorzeichen $(-1)^{i+\ell}$ für das Element $A_{i,\ell}$ ist nur bestimmt durch die Zahlen i und ℓ, d.h. bestimmt durch die Position in der i-ten Zeile und ℓ-ten Spalte. Die Zahl $(-1)^{i+\ell}$ ist also unabhängig von der Dimension n (und auch unabhängig vom Wert $A_{i,\ell}$).

Hilfreich zum Ermitteln des korrekten Vorzeichens ist eine "Vorzeichen-Matrix": Man trägt in einer Matrix in Zeile i und Spalte ℓ nur das Vorzeichen von $(-1)^{i+\ell}$ ein, dies sieht dann wie folgt aus:

$$\begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix} \text{ für } \mathbb{R}^{3\times 3} \qquad \begin{pmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{pmatrix} \text{ für } \mathbb{R}^{4\times 4}$$

Aufwand $O(n!)$
Diese rekursive Definition der Determinante ist *nicht* für große Inputdaten geeignet:

Um $\det(A)$ für $A \in \mathbb{R}^{k\times k}$ zu berechnen, muss man die Determinanten von k-vielen *verschiedenen* $(k-1)\times(k-1)$-Matrizen berechnen. Ist $R(n)$ der Aufwand beim Berechnen der Determinante einer $n \times n$-Matrix, dann gilt also (grob) die Rekursionsformel:

$$R(n) = n \cdot R(n-1).$$

Mit dem Wissen $R(1) = 1$ führt dies zu $R(n) = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = n!$.

Beispiel 8.3.8.

Für $A := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathbb{R}^{2\times 2}$ gilt stets: $\det(A) = a \cdot d - c \cdot b$.

Entwickelt man die Determinante nach der ersten Spalte so erhält man:

$$\begin{aligned} \det(A) = \quad & (1) \cdot a \cdot \det\begin{pmatrix} \not a & \not c \\ \not b & d \end{pmatrix} \quad + (-1) \cdot b \cdot \det\begin{pmatrix} \not a & c \\ \not b & \not d \end{pmatrix} \\ = \quad & a \cdot \det\begin{pmatrix} d \end{pmatrix} \qquad\qquad - b \cdot \det\begin{pmatrix} c \end{pmatrix} \end{aligned}$$

Beispiel 8.3.9.

Es sei $A := \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$. Entwickelt man die Determinante nach der zweiten Spalte so erhält man:

$$\begin{aligned} \det(A) = & (-1)\cdot 4 \cdot \det\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} + (1)\cdot 5 \cdot \det\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} + (-1)\cdot 6 \cdot \det\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} \\ = & -4\cdot \det\begin{pmatrix} 2 & 8 \\ 3 & 9 \end{pmatrix} + 5\cdot \det\begin{pmatrix} 1 & 7 \\ 3 & 9 \end{pmatrix} - 6\cdot \det\begin{pmatrix} 1 & 7 \\ 2 & 8 \end{pmatrix} \\ = & -4\cdot(2\cdot 9 - 3\cdot 8) \quad 5\cdot(1\cdot 9 - 3\cdot 7) \quad 6\cdot(1\cdot 8 - 2\cdot 7) \end{aligned}$$

Bemerkung 8.3.10.

Nach **DET9** lässt sich dieses Verfahren auch auf die Zeilen übertragen. Die Determinante kann also auch analog nach Zeilen entwickelt werden.

Bemerkung 8.3.11 (Rechentrick)**.**

Das rekursive Enwickeln einer Determinante nach einer Zeile oder Spalte ist für "große" Matrizen im Allgemeinen schlicht *nicht* möglich. Für Matrizen mit vielen Null-Einträgen ist dies aber weiterhin möglich:

Beispiel 8.3.12.

Beim Entwickeln der Determinante nach einer Spalte (bzw. Zeile) sollte man eine Spalte (bzw. Zeile) mit vielen Nulleinträgen wählen. Hierdurch veringert sich der Rechenaufwand erheblich!

Es sei

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Entwickeln nach Zeile 3, dann nach Original-Zeile 4 und dann nach Original-Zeile 5 liefert:

$$\det(A) = +1 \cdot \det\begin{pmatrix} 2 & 3 & 4 & 5 \\ 7 & 8 & 9 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = +1 \cdot 2 \det\begin{pmatrix} 3 & 4 & 5 \\ 8 & 9 & 1 \\ 1 & 0 & 0 \end{pmatrix} = +1 \cdot 2 \cdot 1 \cdot \det\begin{pmatrix} 4 & 5 \\ 9 & 1 \end{pmatrix}$$

8.3.3. Die Determinante mit Hilfe des Gauß'schen Eliminationsverfahrens bestimmen

Wir haben gesehen, dass sowohl die Formel in der Definition der Determinante als auch das Entwickeln nach Zeile oder Spalte mit hohem Rechenaufwand verbunden ist, zumindest für größere Matrizen, und deshalb nicht

zur praktischen Berechnung der Determinante geeignet. Der Grund dafür ist die große Anzahl von $n!$ Summanden. Andererseits ermöglichen die Aussagen **DET1-DET6** eine geschicktere Berechnung der Determinante: Wir können die Matrix $n \times n$ mit dem Gaußverfahren (d.h. durch geeignetes Vertauschen von Zeilen und Addieren eines Vielfachen einer Zeile zu einer anderen) auf Zeilenstufenform bringen. Dabei verändert sich dabei der Betrag der Determinante nicht. Das Vorzeichen ändert sich jedesmal, wenn wir zwei Zeilen vertauschen. Und die Determinante einer Matrix in Zeilenstufenform können wir mit **DET6** unmittelbar ausrechnen. Wenn also B die Matrix in Zeilenstufenform ist, die wir mit dem Gaußschen Eliminationsverfahren bekommen, und k die Anzahl der Zeilenvertauschungen ist, die wir auf dem Weg von A zu B durchgeführt haben, gilt $\det(A) = (-1)^k \det(B)$.

Beispiel 8.3.13.

Wir möchten die Determinante von

$$A = \begin{pmatrix} 1 & 0 & -3 \\ -1 & 0 & 4 \\ -1 & 2 & 2 \end{pmatrix}$$

bestimmen. Nach Gauß addieren wir die ersten Zeilen zur zweiten und dritten Zeile; wegen **DET5** ändert sich die Determinante dabei nicht:

$$\begin{pmatrix} 1 & 0 & -3 \\ 0 & 0 & 1 \\ 0 & 2 & -1 \end{pmatrix}.$$

Um die Matrix in Zeilen-Stufen-Form zu bringen, bruachen wir nur noch die zweite und dritte Zeile zu tauschen. Dies ergibt

$$B = \begin{pmatrix} 1 & 0 & -3 \\ 0 & 2 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nun zeigt **DET6**, dass $\det(B) = 1 \cdot 2 \cdot 1 = 2$. Die Gesamtzahl der Zeilenvertauschungen, die wir durchgeführt haben, ist $k = 1$. Also zeigt **DET4**, dass $\det(A) = (-1)^k \det(B) = -\det(B) = -2$.

9 Orthogonalität

Gemeinhin versteht man unter dem Schlagwort $orthogonal$, dass ein rechter Winkel (ein Winkel von $90°$) vorliegt, zwei Strecken sich senkrecht schneiden. Und tatsächlich wird es in diesem Kapitel darum gehen, Winkel zwischen zwei Vektoren zu identifizieren. Das Ziel ist es diejenigen Selbstabbildungen (Automorphismen) des $\mathbb{R}^n$ anhand ihrer Darstellungsmatrizen zu identifizieren, die Längen und Winkel erhalten (so genannte Kongruenzabbildungen). Dazu benötigen wir jeweils ein "Werkzeug", das Winkel zweier Vektoren und die Länge eines Vektors misst. Deshalb werden wir zunächst das Skalarprodukt (Winkel) und die euklidiche Norm (Länge) kennen lernen.

9.1. Das Skalarprodukt und die euklidische Norm

Wir beginnen unumwunden mit den zwei grundlegenden Definitionen des Kapitels.

Definition 9.1.1.

Es seien $v, w \in \mathbb{R}^n$ dann ist das ***Skalarprodukt*** der beiden v und w definiert als

$$\langle v, w\rangle := v_1 \cdot w_1 + \ldots + v_n \cdot w_n = \sum_{i=1}^{n} v_i w_i.$$

Bemerkung 9.1.2.

- Man beachte, dass das **Skalarprodukt eine *Zahl* berechnet**.
- Das Skalarprodukt ist gleich dem Matrix-Matrix-Produkt des transponierten Vektors v^T und w, es ist:

$$\langle v, w\rangle = v^T \cdot w = (v_1, \ldots, v_n) \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$

Beispiel 9.1.3.

Es gilt: $\left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\rangle = 1 \cdot 4 + 2 \cdot 5 + 3 \cdot 6 = 32$

Definition 9.1.4.

Für $v \in \mathbb{R}^n$ ist die ***euklidische Norm*** definiert als

$$\|v\| := \sqrt{\langle v, v\rangle} = \sqrt{v_1^2 + \ldots + v_n^2}.$$

Bemerkung 9.1.5.

- Die euklidische Norm eines Vektors entspricht geometrisch seiner Länge.
- **F:** Warum wird die Länge eines Vektors mit Doppelstrichen angegeben?
  A: Um den Unterschied zum Betrag einer Zahl klar darzustellen (z.B. $|-3|$)

Beispiel 9.1.6.

Es gilt: $\| \begin{pmatrix} -3 \\ 4 \end{pmatrix} \| = \sqrt{(-3)^2 + 4^2} = \sqrt{25} = 5$

9.1.1. Rechenregeln für das Skalarprodukt und die euklidische Norm

Um die Rechenregeln für das Skalarprodukt und die euklidische Norm zu beweisen, brauchen wir eine unter dem Namen "Cauchy-Schwarz-Ungleichung" bekannte Ungleichung, die das Skalarprodukt zweier Vektoren und ihre euklidischen Normen in Beziehung setzt.

Korollar 9.1.7 ("Cauchy-Schwarz-Ungleichung")**.**

Für Vektoren $v, w \in \mathbb{R}^n$ gilt stets

$$| \langle v, w \rangle | \leq \|v\| \cdot \|w\|.$$

Beweis. Dieses Korollar folgt direkt aus Lemma .... □

- Für das Skalarprodukt gelten die folgenden Rechenregeln:

Korollar 9.1.8 (Rechenregeln für das Skalarprodukt)**.**

Es seien $v, w, y \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ dann gelten:

i.	$\langle v, y \rangle$	$=$	$\langle y, v \rangle$	(Symmetrie)
ii.	$\langle v + w \ , \ y \rangle$	$=$	$\langle v \ , \ y \rangle + \langle w \ , \ y \rangle$	(Additivität im ersten Eintrag)
iii.	$\langle v + w \ , \ y \rangle$	$=$	$\langle v \ , \ y \rangle + \langle w \ , \ y \rangle$	(Homogenität im ersten Eintrag)

Beweis. Die Aussagen folgen direkt aus der Definition des Skalarprodukts. □

Bemerkung 9.1.9.

Wegen der Symmetrie gilt sofort, dass das Skalarprodukt auch linear, also additiv und homogen im zweiten Eintrag ist:

$$\langle y \ , \ w + v \rangle = \langle y \ , \ v \rangle + \langle y \ , \ w \rangle$$

$$\langle y \ , \ \lambda \cdot v \rangle = \lambda \cdot \langle y \ , \ v \rangle$$

Dass das Skalarprodukt linear in beiden Einträgen ist, ähnelt der Multilinearität der Determinante und wird tatsächlich auch als Bilinearität bezeichnet.

► Für die euklidische Norm gelten die folgenden Rechenregeln:

Korollar 9.1.10 (Rechenregeln für die Norm)**.**

Für alle $v, w \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gelten:

i.	$\|v\|$	$=$	0	$\Leftrightarrow$	$v = 0$	(Definitheit)
ii.	$\|v + w\|$	$\leq$	$\|v\| + \|w\|$			(Dreiecksungleichung)
iii.	$\|\lambda \cdot v\|$	$=$	$\|\lambda\| \cdot \|v\|$			(Absolute Homgenität)

Beweis. Aussagen **i.** und **ii.** folgen direkt aus der Definition der Norm . Für **iii.** berechnen wir:

$$\begin{aligned}\|v + w\|^2 &= \langle v + w, v + w\rangle = \langle v, v\rangle + 2\langle v, w\rangle + \langle w, w\rangle \\ &\leq \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 = (\|v\| + \|w\|)^2 \qquad \text{(nach Cauchy-Schwarz-Ungl.)}\end{aligned}$$

Wurzelziehen auf beiden Seiten von $\|v + w\|^2 \leq (\|v\| + \|w\|)^2$ liefert die Aussage. □

9.1.2. Geometrische Interpretation des Skalarprodukts

Wir möchten nun einige geometrische Eigenschaften des Skalarprodukts untersuchen. Dazu beginnen wir mit der Definition von Orthogonalität.

Definition 9.1.11.

Zwei Vektoren $v, w \in \mathbb{R}^n$ heißen *orthogonal*, wenn gilt

$$\langle v\ ,\ w\rangle = 0.$$

Bemerkung 9.1.12.

Der Nullvektor spielt eine Sonderrolle. Jeder Vektor ist orthogonal zum Nullvektor, denn $\langle 0, v\rangle = 0$ für alle $v \in \mathbb{R}^n$. Die geometrische Interpretation ist für diesen Fall schwierig und wird im Folgenden bei anschaulichen Erklärungen stillschweigend ausgeklammert, bzw. muss gesondert betrachtet werden.

Geometrisch bedeutet dies, dass zwei orthogonale Vektoren senkrecht aufeinander stehen. Um das einzusehen benötigen wir zunächst eine Formel, welche das Skalarprodukt zweier Vektoren bezüglich ihrer Normen ausdrückt.

Lemma 9.1.13.

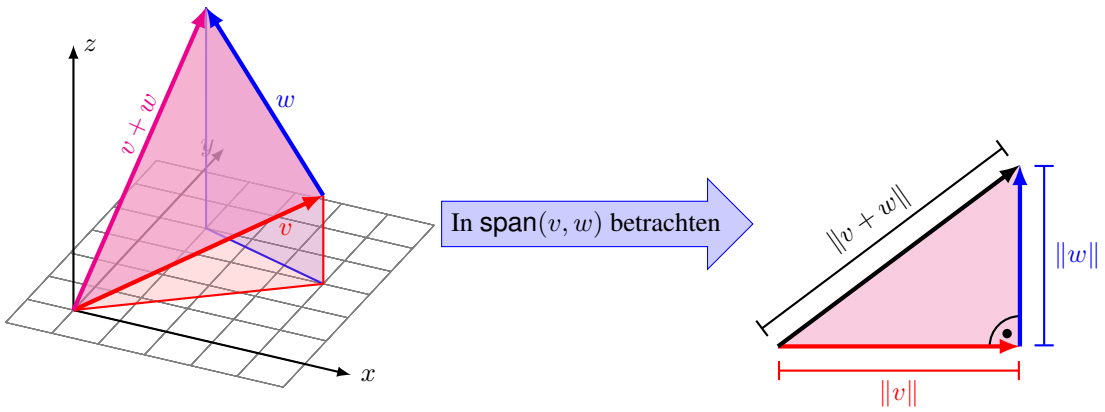
Für $v, w \in \mathbb{R}^n$ ist

$$\langle v, w\rangle = \frac{\|v + w\|^2 - \|v\|^2 - \|w\|^2}{2}.$$

Beweis. Es seien $v, w \in \mathbb{R}^n$. Dann gilt:

$$\|v + w\|^2 = \langle \vec{v} + w\ ,\ v + w\rangle \overset{\star}{=} \underbrace{\langle v\ ,\ v\rangle}_{=\|v\|^2} + \langle v\ ,\ w\rangle + \langle w\ ,\ v\rangle + \underbrace{\langle w\ ,\ w\rangle}_{=\|w\|^2}$$

$$\overset{\star\star}{=} \|v\|^2 + \|w\|^2 + 2\langle v\ ,\ w\rangle$$



Phytagoras: $\|v\|^2 + \|w\|^2 = \|v + w\|^2$

Abbildung 9.1.: Phytagoras für Dreiecke im $\mathbb{R}^3$

Hier haben wir verwendet: $\star$ Das Skalarprodukt ist bilinear, $\star\star$ Symmetrie $\langle v, w\rangle = \langle w, v\rangle$

Es gilt also $\langle v, w\rangle = \frac{1}{2}\left(\|v + w\|^2 - \|v\|^2 - \|w\|^2\right)$. □

Wir können nun beweisen:

Lemma 9.1.14.

Zwei orthogonale Vektoren $v, w \in \mathbb{R}^n$ stehen senkrecht aufeinander.

Beweis. Die Vektoren v, w und $v + w$ bilden die Seiten eines Dreiecks (siehe Abb. 9.1 für eine Skizze im $\mathbb{R}^3$). Dieses Dreieck betrachtet man relativ zur 2-dimensionalen Ebene $\mathsf{span}\,(v, w)$ an.

Nach dem Satz des Phytagoras ist das Dreieck rechtwinklig genau dann wenn gilt:

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2$$

Nach Lemma 9.1.13 gilt jedoch:

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2 + 2\langle v\ ,\ w\rangle$$

Das Dreieck ist also genau dann rechtwinklig, wenn gilt: $\langle v\ ,\ w\rangle = 0$. □

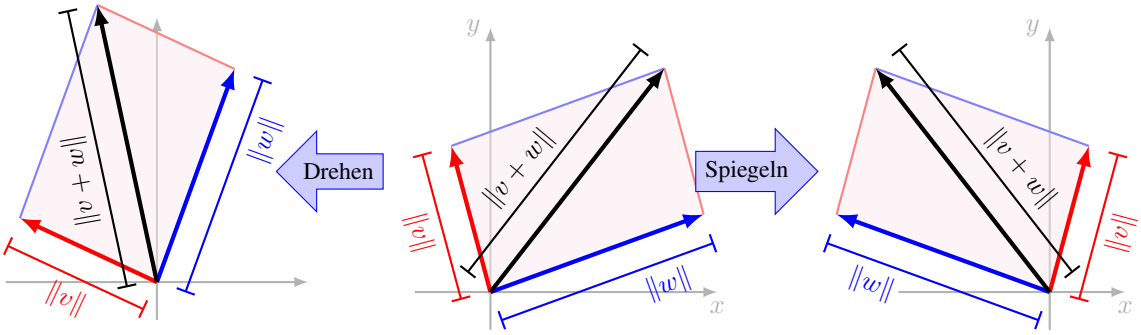
Aus Lemma 9.1.13 folgt eine weitere geometrische Eigenschaft des Skalarprodukts.

Korollar 9.1.15.

Das Skalarprodukt ist Invariant unter Drehungen und Spiegelungen des $\mathbb{R}^n$.

Bemerkung 9.1.16.

Drehungen und Spiegelungen verändern die Länge der abgebildeten Vektoren nicht und erhalten den Winkel, der zwischen zwei Vektoren eingeschlossen wird.



Wendet man also eine Drehung oder eine Spiegelung gleichzeitig auf v und w so ändern sich deren Längen nicht, und der *eingeschlossene Winkel* ändert sich ebenfalls nicht. Dies führt dazu, dass sich die Länge der Summe $v+w$ ebenfalls nicht ändert: Ist v' das Bild von v und w' das Bild von w, so gilt: $\|v+w\| = \|v'+w'\|$.

Das nächste Lemma zeigt, dass das Skalarprodukt zweier Vektoren auch tatsächlich Information über den Winkel in sich trägt, welche die beiden Vektoren einschließen.

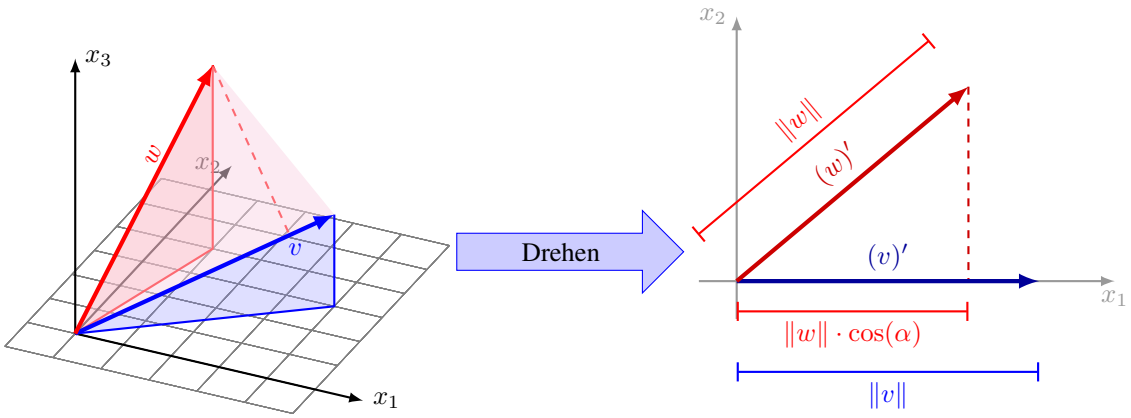
Lemma 9.1.17.

Es seien $v, w \in \mathbb{R}^n$ und $\alpha \in [0, \pi]$ der Winkel, der zwischen v und w eingeschlossen wird, dann gilt:

$$\langle v, w\rangle = \|v\| \cdot \|w\| \cdot \cos(\alpha)$$

Beweis. Um die Geichung $\langle v, w\rangle = \|v\| \cdot \|w\| \cdot \cos(\alpha)$ zu zeigen bedienen wir uns einer geeigneten Drehung:

Man drehe den gesamten $\mathbb{R}^n$, so dass v auf die x_1-Achse gedreht wird, und w in die x_1-x_2 Ebene gedreht wird.



Ist $(v)'$ das Bild von v unter der Drehung und $(w)'$ das Bild von w, so gibt es $\lambda, a, b \in \mathbb{R}$ mit:

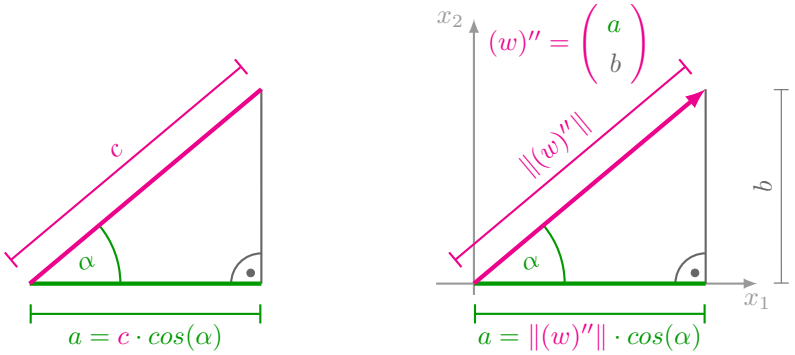
$$(v)' = \begin{pmatrix} \lambda \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (w)' = \begin{pmatrix} a \\ b \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{und} \qquad \langle v, w\rangle = \langle (v)', (w)'\rangle \quad = \lambda \cdot a$$

Um die Rechnungen kurz zu halten, streichen wir die letzten $n-2$ Nullen aus $(v)', (w)'$ und erhalten:

$$(v)'' = \begin{pmatrix} \lambda \\ 0 \end{pmatrix} \quad (w)'' = \begin{pmatrix} a \\ b \end{pmatrix} \qquad \text{mit weiterhin} \qquad \langle v, w\rangle = \langle (v)'', (w)''\rangle \quad = \lambda \cdot a$$

Wir zeigen nun $\lambda = \|v\|$ und $a = \|w\| \cdot \cos(\alpha)$. Daraus folgt dann die Behauptung $\langle v, w\rangle = \|v\| \cdot \|w\| \cdot \cos(\alpha)$.

- Berechnung von $\lambda = \|v\|$.
  Es gilt $\|v\| = \|(v)'\|$ weil das Drehen von v auf $(v)'$ die Längen der Vektoren nicht ändert.
  Es muss also $\|v\| = \lambda$ gelten, weil $\|v\| = \|(v)'\|$ (drehen) und $\|(v)'\| = \|(v)''\| = \lambda$ (nachrechnen!) gelten.
- Berechnung von $a = \|w\| \cdot \cos(\alpha)$.
  Auch für w ist Drehen Längenerhaltend, d.h. $\|w\| = \|(w)'\|$, und es gilt $\|(w)'\| = \|(w)''\| = \sqrt{a^2 + b^2}$.
  Weiter gilt $a = \|(w)''\| \cdot \cos(\alpha)$, denn das Dreieck Mit den Ecken $\begin{pmatrix}0\\0\end{pmatrix}$, $\begin{pmatrix}a\\0\end{pmatrix}$ und $(\vec{w})'' = \begin{pmatrix}a\\b\end{pmatrix}$ ist rechtwinklig:



Im Rechtwinkligen Dreieck mit Hypothenuse c und Ankathete[2] a gilt:

$$\cos(\alpha) = \frac{a}{c} = \frac{\text{Länge der Ankathete}}{\text{Länge der Hypothenuse}} \qquad \text{bzw.} \qquad a = c \cdot \cos(\alpha)$$

Angewendet auf das Dreieck mit Hypothenuse $(w)''$ liefert dies: $a = \|(w)''\| \cdot \cos(\alpha)$, und wegen $\|(w)''\| = \|w\|$ folgt die Behauptung.

□

9.2. Orthonormalbasen

Immer noch sind wir auf der Suche nach schönen Basen bezüglich derer lineare Abbildung mit zugehörigen Darstellungsmatrizen einfach und übersichtlich beschrieben werden können. In diesem Abschnitt kommen wir diesem Ziel ein gutes Stück näher.

Wir beginnen doch zunächst mit einer Verallgemeinerung und Ergänzung von Definition 9.1.11.

Definition 9.2.1.

- Wir nennen zwei Vektoren $v_1, v_2 \in \mathbb{R}^n$ ***orthogonal***, falls $\langle v_1, v_2\rangle = 0$.(Definition 9.1.11)
- Allgemeiner heißen Vektoren $v_1, \ldots, v_k$ ***orthogonal***, wenn alle paarweise verschiedenen Vektoren v_i, v_j orthogonal sind.
- Für einen Vektor $v \in \mathbb{R}^n$ mit $v \neq 0$ ist $w = \frac{v}{\|v\|}$ der zu v gehörige ***normierte*** Vektor. Ein Vektor, für den gilt $w = v$, wird auch als normierter Vektor bezeichnet.
- Ferner heißen $v_1, \ldots, v_k$ ***orthonormal***, wenn $v_1, \ldots, v_k$ orthogonal und normierte Vektoren sind.
- Sei V ein Vektorraum mit $\dim(V) = k$. Wir nennen $v_1, \ldots, v_k$ eine ***Orthonormalbasis*** von V, falls

$v_1, \ldots, v_k$ orthonormal sind.

Bemerkung 9.2.2.

- Für einen Vektor $v \in \mathbb{R}^n$ gilt, dass der zugehörige normierte Vektor $w = \frac{v}{\|v\|}$ die Norm $\|w\| = 1$ hat und in die selbe Richtung wie v zeigt. Außerdem ist $\langle w, v\rangle = \frac{1}{\|v\|} \cdot \langle v, v\rangle = \frac{\|v\|^2}{\|v\|} = \|v\|$.
- In der Definition von Orthonormalbasen von Vektorräumen, fehlt die Bedingung, dass die Vektoren linear unabhängig sein müssen. Da sie orthonormal sind, sind sie auf jeden Fall ungleich 0 (dem Nullvektor). Wir werden in Lemma 9.2.4 sehen, dass orthogonale Vektoren, welche alle ungleich 0 sind, linear unabhängig sind.

Beispiel 9.2.3.

- Die Vektoren $\{v, w\}$ mit $v = \frac{1}{5}\begin{pmatrix} 3 \\ 4 \end{pmatrix}$, $w = \frac{1}{5}\begin{pmatrix} -4 \\ 3 \end{pmatrix}$ sind orthonormal, denn:

  orthognal $\quad \langle v, w\rangle = \left\langle \begin{pmatrix} \frac{3}{5} \\ \frac{4}{5} \end{pmatrix}, \begin{pmatrix} \frac{-4}{5} \\ \frac{3}{5} \end{pmatrix} \right\rangle = \frac{3}{5} \cdot \frac{(-4)}{5} + \frac{4}{5} \cdot \frac{3}{5} = 0$

  normiert $\quad \|v\|^2 = \langle v, v\rangle = \left\langle \begin{pmatrix} \frac{3}{5} \\ \frac{4}{5} \end{pmatrix}, \begin{pmatrix} \frac{3}{5} \\ \frac{4}{5} \end{pmatrix} \right\rangle = \frac{3^2}{5^2} + \frac{4^2}{5^2} = 1$

  $\|w\|^2 = \langle w, w\rangle = \left\langle \begin{pmatrix} \frac{-4}{5} \\ \frac{3}{5} \end{pmatrix}, \begin{pmatrix} \frac{-4}{5} \\ \frac{3}{5} \end{pmatrix} \right\rangle = \frac{(-4)^2}{5^2} + \frac{3^2}{5^2} = 1$

- Die Vektoren $\left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ sind ortho**gonal** aber nicht ortho**normal**, denn $\left\| \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\| = \sqrt{2} \neq 1$

  Die Vektoren $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{5}\begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\}$ sind *weder* ortho**gonal** *noch* ortho**normal**.
  (Die Vektoren sind zwar normiert (d.h. haben Länge 1), sind aber nicht orthogonal.)

Lemma 9.2.4.

Wenn die Vektoren $v_1, \ldots, v_k$ alle ungleich 0 und orthogonal sind, dann sind sie linear unabhängig.

Beweis. Seien also die $v_1, \ldots, v_k$ alle ungleich 0 und orthogonal, d.h.

i. Für paarweise verschiedene Vektoren v_i und v_j aus dieser Menge ist $\langle v_i, v_j\rangle = 0$.
ii. Für jeden Vektor v_i aus dieser Menge gilt $\|v_i\| > 0$ (Definitheit).

Wir möchten zeigen, dass die Gleichung

$$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \ldots + \lambda_k \cdot v_k = 0 \tag{9.1}$$

nur die triviale Lösung $\lambda_1 = \lambda_2 = \ldots = \lambda_k = 0$ hat.

Dazu wähle einen Index $\ell \in \{1, \ldots, k\}$ beliebig und betrachte

$$\langle \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \ldots + \lambda_k \cdot v_k, v_\ell \rangle = \langle 0, v_\ell \rangle \tag{9.2}$$

also auf beiden Seiten von Gleichung (9.1) das Skalarprodukt mit dem Vektor v_ℓ. Dann vereinfacht sich die Gleichung (9.2) zu

$$\langle \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \ldots + \lambda_k \cdot v_k, v_\ell \rangle = \langle 0, v_\ell \rangle$$

$$\lambda_1 \cdot \langle v_1, v_\ell \rangle + \lambda_2 \cdot \langle v_2, v_\ell \rangle + \ldots + \lambda_k \cdot \langle v_k, v_\ell \rangle = 0$$

[Nach der Additivität & Homogenität der ersten Komponente des Skalarprodukts]

$$\lambda_\ell \cdot \langle v_\ell, v_\ell \rangle = 0 \qquad \text{[nach i. sind alle } \langle v_i, v_j \rangle = 0 \text{ für } i \neq j\text{]}$$

$$\lambda_\ell \cdot \|v_\ell\| = 0.$$

Nach ii. ist aber $\|v_\ell\| > 0$ also muss $\lambda_\ell = 0$ sein.

Da ℓ beliebig aus $\{1, \ldots, k\}$ gewählt war gilt: Es ist $\lambda_i = 0$ für alle $i \in \{1, \ldots, k\}$. Also sind die $v_1, \ldots, v_k$ linear unabhängig. □

Satz 9.2.5.

Jeder reelle Vektorraum V hat eine Orthonormalbasis.

Beweis. Wir führen eine Induktion über die Dimension des Vektorraums V. Wir wissen, dass jeder Vektorraum eine Basis $b_1, \ldots, b_n$ hat mit $n = \dim(V)$.

Induktionsverankerung: Ist $n = 1$, so ist $\tilde{b}_1 = \frac{b_1}{\|b_1\|}$ eine Orthonormalbasis.

Induktionsannahme: Wir nehmen als Induktionsvorraussetzung an, dass jeder n dimensionale reelle Vektorraum eine Orthonormalbasis besitzt.

Induktionsschluss: Sei also der reelle Vektorraum V von Dimension $n + 1$. Wir können aus jeder beliebigen Basis $b_1, \ldots, b_{n+1}$ von V eine Orthonormalbasis mit dem sogenannten ***Gram-Schmidt-Verfahren*** konstruieren. Dazu definieren wir

$$\tilde{b}_{n+1} = \frac{b_{n+1}}{\|b_{n+1}\|} \tag{9.3}$$

(dabei ist $\tilde{b}_{n+1}$ nichts anderes als der normierte Vektor zu b_{n+1}) und

$$V' = \{v \in V : \langle v, \tilde{b}_{n+1} \rangle = 0\}. \tag{9.4}$$

Diese Menge ist eine Untervektorraum von V. Sei $m = \dim(V')$ seine Dimension. Weil $\langle \tilde{b}_{n+1}, \tilde{b}_{n+1} \rangle = \frac{\langle b_{n+1}, b_{n+1} \rangle}{\|b_{n+1}\|^2} = 1$, ist $\tilde{b}_{n+1} \notin V'$. Also ist V' eine echte Teilmenge von V und demnach ist $m < n + 1$. Nach Induktionsannahme hat V also eine Orthonormalbasis $\tilde{b}_1, \ldots, \tilde{b}_m$.

Wir behaupten nun, dass $\tilde{b}_1, \ldots, \tilde{b}_n, \tilde{b}_{n+1}$ eine Orthonormalbasis von V' ist.

- **Orthonormalität:** Wir beobachten, dass die Vektoren $\tilde{b}_1, \ldots, \tilde{b}_m$ orthonormal und nach (9.4) alle orthogonal zu $\tilde{b}_{n+1}$ sind. Außerdem ist per Konstruktion (9.3) der Vektor $\tilde{b}_{n+1}$ normiert. Also sind die

Vektoren $\tilde{b}_1, \ldots, \tilde{b}_m, \tilde{b}_{n+1}$ orthonormal.

- **Lineare Unabhängigkeit:** Da die Vektoren $\tilde{b}_1, \ldots, \tilde{b}_m, \tilde{b}_{n+1}$ orthonormal, also insbesondere ungleich 0 und orthogonal sind, sind sie nach Lemma 9.2.4 linear unabhängig.
- **Spann ist ganz V:** Sei $v \in V$ ein beliebiger Vektor aus V. Betrachte den Vektor

$$u = v - \langle v, \tilde{b}_{n+1} \rangle \cdot \tilde{b}_{n+1}.$$

Es gilt

$$\langle u, \tilde{b}_{n+1} \rangle = \langle v, \tilde{b}_{n+1} \rangle - \langle v, \tilde{b}_{n+1} \rangle \cdot \langle \tilde{b}_{n+1}, \tilde{b}_{n+1} \rangle = \langle v, \tilde{b}_{n+1} \rangle - \langle v, \tilde{b}_{n+1} \rangle \cdot \|\tilde{b}_{n+1}\|^2 = 0,$$

also ist $u \in V'$ nach (9.4). Also existieren $\lambda_1, \ldots, \lambda_m$ mit $u = \sum_{i=1}^{m} \lambda_i \cdot \tilde{b}_i$. Setzten wir ferner $\lambda_{n+1} = \langle v, \tilde{b}_{n+1} \rangle$, so erhalten wir

$$v = \lambda_{n+1} \cdot \tilde{b}_{n+1} + \sum_{i=1}^{m} \lambda_i \cdot \tilde{b}_i.$$

Also liegt v im Spann von $\tilde{b}_1, \ldots, \tilde{b}_m, \tilde{b}_{n+1}$. Da v beliebig in V gewählt war ist

$$V = \mathsf{span}\{\tilde{b}_1, \ldots, \tilde{b}_m, \tilde{b}_{n+1}\}$$

und insbesondere $m = n$.

□

Wir haben in dem obigen Beweis beobachtet, dass für eine Orthonormalbasis $b_1, \ldots, b_n$ eines Vektorraums V sich jeder Vektor $v \in V$ schreiben lässt als

$$v = \sum_{i=1}^{n} \langle v, b_i \rangle \cdot b_i.$$

Die Zahlen $\langle v, b_i \rangle$ werden ***Fourierkoeffizienten*** von v bezüglich der Basis $b_1, \ldots, b_n$ genannt.

9.2.1. Das orthogonale Komplement

Der Begriff der Orthogonalität führt auf eine natürliche Zerlegung von Vektorräumen. Dazu definieren wir allgemein Mengen, die alle orthogonale Vektoren zu einem Untervektorraum enthalten (vergleiche die Menge V' im Beweis von Satz 9.2.5).

Definition 9.2.6.

Sei V ein Vektorraum und $W \subset V$ ein Untervektorraum. Das ***orthogonale Komplement*** von W in V ist

$$W^{\perp} = \{v \in V : \langle v, w \rangle \forall w \in W\}.$$

Lemma 9.2.7.

Die Menge $W^\perp$ ist ein Untervektorraum von V.

Beweis. Die Nachweise der Abgeschlossenheit bezüglich der Addition und der skalaren Multiplikation geht auf die Bilinearität des Skalarproduktes zurück und ist leicht zu prüfen. □

Proposition 9.2.8.

Sei V ein Vektorraum und $W \subset V$ ein Untervektorraum. Die Abbildung

$$f : W \times W^\perp \to V,$$

$$(w_1, w_2) \mapsto w_1 + w_2$$

ist bijektiv und es gilt

$$\dim(W) + \dim(W^\perp) = dim(V).$$

Beweis. Sei $b_1, \ldots, b_n$ eine Orthonormalbasis von W und $c_1, \ldots, c_m$ eine Orthonormalbasis von $W^\perp$. Wir behaupten, dass $b_1, \ldots, b_n, c_1, \ldots, c_m$ eine Orthonormalbasis von V ist.

- **Orthonormalität:** Aus der Definition von $W^\perp$ folgt unmittelbar, dass die Vektoren

  $$b_1, \ldots, b_n, c_1, \ldots, c_m$$

  orthonormal sind.
- **Lineare Unabhängigkeit:** Da die Vektoren $b_1, \ldots, b_n, c_1, \ldots, c_m$ orthonormal, also insbesondere ungleich 0 und orthogonal sind, sind sie nach Lemma 9.2.4 linear unabhängig.
- **Spann ist ganz V:** Sei $v \in V$ ein beliebiger Vektor aus V. Betrachte den Vektor

  $$v' = v - \sum_{i=1}^{n} \langle v, b_i \rangle \cdot b_i. \tag{9.5}$$

  Für jeden Vektor b_j mit $j = 1, \ldots, n$ gilt

  $$\langle v', b_j \rangle = \langle v, b_j \rangle - \sum_{i=1}^{n} \langle z, b_i \rangle \cdot \langle b_i, b_j \rangle = \langle z, b_j \rangle - \langle z, b_j \rangle = 0.$$

  Die zweite Gleichung folgt aus der Orthonormalität von $b_1, \ldots, b_n$. Weil $b_1, \ldots, b_n$ eine Basis von W ist, können wir schließen, dass $\langle v', w \rangle = 0$ für alle $w \in W$. Also gilt $v' \in W^\perp$ und somit

  $$v' = \sum_{i=1}^{m} \langle v', c_i \rangle \cdot c_i. \tag{9.6}$$

  Aus (9.5) und (9.6) folgt, dass sich jeder Vektor $v \in V$ darstellen lässt als

  $$v = \sum_{i=1}^{n} \langle v, b_i \rangle \cdot b_i + \sum_{i=1}^{m} \langle v, c_i \rangle \cdot c_i$$

  das heißt, $v \in \mathsf{span}\{b_1, \ldots, b_n, c_1, \ldots, c_m\}$. Da v beliebig aus V gewählt war, ist also

  $$V \subset \mathsf{span}\{b_1, \ldots, b_n, c_1, \ldots, c_m\}.$$

Umgekehrt gilt

$$\mathsf{span}\{b_1, \ldots, b_n, c_1, \ldots, c_m\} \subset V,$$

weil $\{b_1, \ldots, b_n, c_1, \ldots, c_m\} \subset V$ und somit

$$V = \mathsf{span}\{b_1, \ldots, b_n, c_1, \ldots, c_m\},$$

was zu zeigen war.

□

9.3. Orthogonale Abbildungen

Orthogonale Abbildungen werden anhand ihrer Darstellungsmatrizen definiert, welche selbst die Eigenschaft der Orthogonalität tragen. Bevor wir jedoch solche orthogonalen Matrizen definieren, blicken wir auf die Multiplikation zweier Matrizen $A \in \mathbb{R}^{k\times m}$ und $B \in \mathbb{R}^{m\times n}$ zurück. Die Spalten der Produktmatrix $C = A \cdot B$ sind die Ergebnisse der Matrix-Vektor Multiplikation der Matrix A mit den Spalten der Matrix B. Genauer gesagt ist die $i$te Spalte der Produktmatrix C gegeben durch

$$C^{(i)} = \begin{pmatrix} \langle A_{(1)}, B^{(i)} \rangle \\ \langle A_{(2)}, B^{(i)} \rangle \\ \vdots \\ \langle A_{(k)}, B^{(i)} \rangle \end{pmatrix}$$

also ist

$$C = \begin{pmatrix} C^{(1)} & C^{(2)} & \ldots & C^{(n)} \end{pmatrix} = \begin{pmatrix} \langle A_{(1)}, B^{(1)} \rangle & \langle A_{(1)}, B^{(2)} \rangle & \ldots & \langle A_{(1)}, B^{(n)} \rangle \\ \langle A_{(2)}, B^{(1)} \rangle & \langle A_{(2)}, B^{(2)} \rangle & \ldots & \langle A_{(2)}, B^{(n)} \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle A_{(k)}, B^{(1)} \rangle & \langle A_{(k)}, B^{(2)} \rangle & \ldots & \langle A_{(k)}, B^{(n)} \rangle \end{pmatrix}.$$

Wir erhalten also mit dem Skalarprodukt eine alternative Beschreibung der Matrix-Matrix-Multiplikation.

Beispiel 9.3.1.

Betrachte die Matrizen $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ und $B = \begin{pmatrix} 5 & 6 & 7 \\ 8 & 9 & 10 \end{pmatrix}$, dann sind

$$A_{(1)} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, A_{(2)} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}, B^{(1)} = \begin{pmatrix} 5 \\ 8 \end{pmatrix}, B^{(2)} = \begin{pmatrix} 6 \\ 9 \end{pmatrix}, B^{(3)} = \begin{pmatrix} 7 \\ 10 \end{pmatrix}$$

und wir haben

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

$$= \begin{pmatrix} \langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \end{pmatrix} \rangle & \langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 6 \\ 9 \end{pmatrix} \rangle & \langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 7 \\ 10 \end{pmatrix} \rangle \\ \langle \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \end{pmatrix} \rangle & \langle \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 9 \end{pmatrix} \rangle & \langle \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 7 \\ 10 \end{pmatrix} \rangle \end{pmatrix}$$

$$= \begin{pmatrix} \langle A_{(1)}, B^{(1)} \rangle & \langle A_{(1)}, B^{(2)} \rangle & \langle A_{(1)}, B^{(3)} \rangle \\ & & \\ \langle A_{(2)}, B^{(1)} \rangle & \langle A_{(2)}, B^{(2)} \rangle & \langle A_{(2)}, B^{(3)} \rangle \end{pmatrix}$$

Seien nun also $v_1, \ldots, v_n \in \mathbb{R}^n$ orthonormal. Die $n \times n$ Matrix A mit Spalten $A^{(i)} = v_i$ stellt die lineare Abbildung, die den Einheitsvektor $e^{(i)}$ auf v_i abbildet, dar. Betrachtet man die transponierte Matrix von A, dann entsprechen die Zeilen von A^T genau den Vektoren $v_1, \ldots, v_n$, es ist $A^T_{(i)} = v_i$ für alle $i \in \{1, \ldots, n\}$.

Dann hat das Produkt $B = A^T \cdot A$ nach obiger Regel die Einträge $B_{ij} = \langle b_i, b_j \rangle$. Da die Vektoren $b_1, \ldots, b_n$ orthonormal sind, ist $B = \mathrm{id}$. Das bedeutet, dass in diesem Fall $A^{-1} = A^T$ ist.

Hat umgekehrt die $n \times n$-Matrix A die Eigenschaft, dass $A^{-1} = A^T$, dann sind die Spalten von A orthonormal. Wir geben Matrizen mit dieser Eigenschaft einen besonderen Namen.

Definition 9.3.2.

Eine $n \times n$-Matrix A heißt ***orthogonal***, wenn $A^T \cdot A = \mathrm{id}$.

Bemerkung 9.3.3.

Das Skalarprodukt spielt in diesem Zusammenhang eine besondere Rolle.

- Ist A eine $n \times n$-Matrix und sind $v, w \in \mathbb{R}^n$ so gilt

$$\langle A \cdot v, w \rangle = \langle v, A^T \cdot w \rangle,$$

  wie man leicht nachrechnet.
- In der Tat ist A^T die einzige Matrix mit dieser Eigenschaft: Wenn B eine Matrix ist, so dass

$$\langle A \cdot v, w \rangle = \langle v, B \cdot w \rangle,$$

  für alle $v, w \in \mathbb{R}^n$, so gilt $B = A^T$.

Beispiel 9.3.4.

Die folgenden Matrizen sind orthogonale Matrizen

$$A = \begin{pmatrix} \frac{3}{5} & \frac{-4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix} \qquad B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad C = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{3}} & -\frac{2}{\sqrt{6}} \end{pmatrix}$$

Das folgende Lemma besagt, dass orthogonale Abbildungen (deren Darstellungsmatrix eine orthogonale Matrix ist) das Skalarprodukt und somit auch die euklidische Norm erhalten. Orthogonale Abbildungen sind demnach ***Kongruenzabbildungen***.

Lemma 9.3.5.

Wenn A eine orthogonale Matrix ist, dann gilt

$$\langle A \cdot v, A \cdot w \rangle = \langle v, w \rangle$$

für alle $v, w \in \mathbb{R}^n$. Ferner ist A^T orthogonal.

Beweis. Mit der obigen Bemerkung erhalten wir, dass

$$\langle A \cdot v, A \cdot w \rangle = \langle v, A^T \cdot A \cdot w \rangle = \langle v, \mathrm{id} \cdot w \rangle = \langle v, w \rangle$$

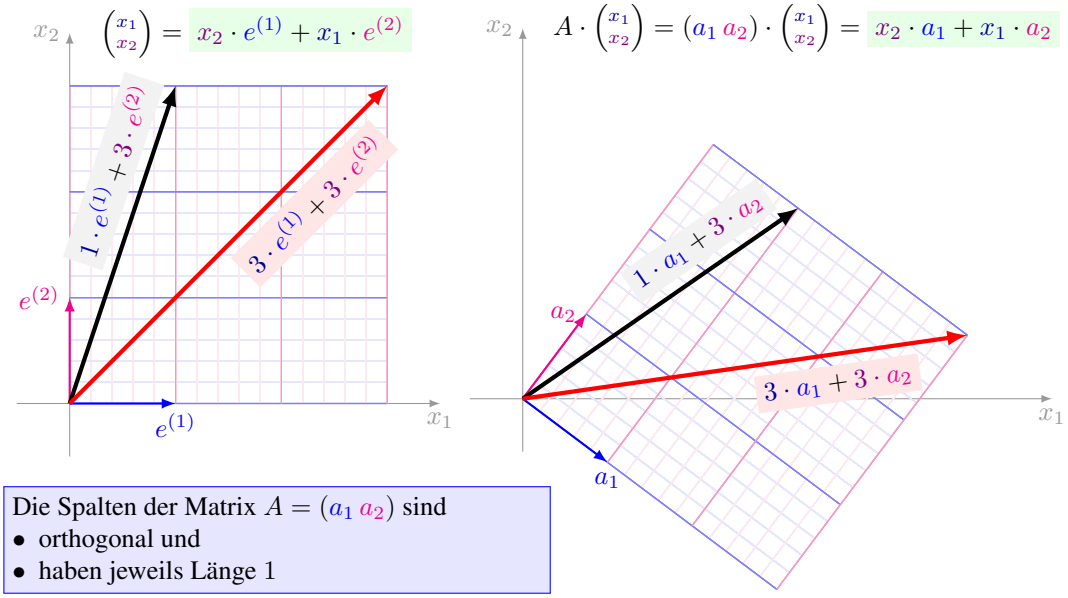
für alle $v, w \in \mathbb{R}^n$. Außerdem ist A invertierbar. Deshalb trifft dies auch auf A^T zu und $(A^T)^{-1} = (A^{-1})^T = (A^T)^T = A$. □

Lemma 9.3.6.

Wenn A, B orthogonale $n \times n$-Matrizen sind, dann ist $A \cdot B$ orthogonal.

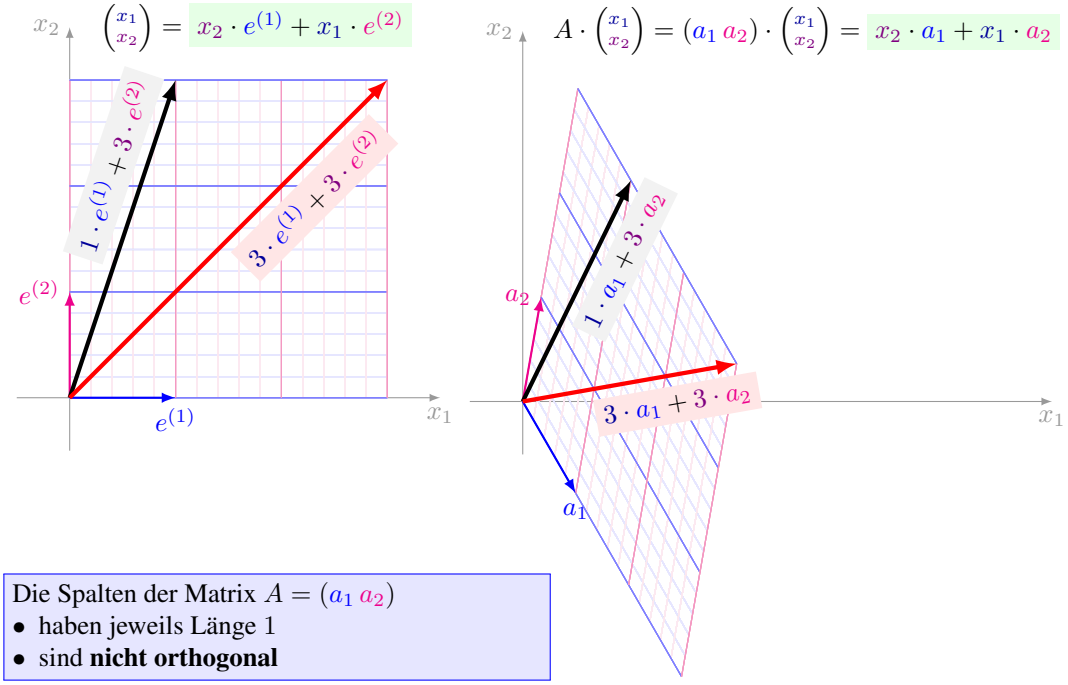
Beweis. Es gilt $(A \cdot B)^T \cdot A \cdot B = B^T \cdot A^T \cdot A \cdot B = B^T \cdot \mathrm{id} \cdot B = B^T \cdot B = \mathrm{id}$. □

Im Folgenden noch zwei Abbildungen, die insbesondere Lemma 9.3.5 veranschaulichen: Orthogonale Abbildungen sind Kongruenzabbildungen.



Die Spalten der Matrix $A = (a_1\ a_2)$ sind
- orthogonal und
- haben jeweils Länge 1

Abbildung 9.2.: Orthogonale Abbildungen ***sind*** winkel- und längenerhaltend.



Die Spalten der Matrix $A = (a_1\ a_2)$
- haben jeweils Länge 1
- sind **nicht orthogonal**

Abbildung 9.3.: Gewöhnliche lineare Abbildungen ***sind nicht*** winkel- und längenerhaltend.

10 Eigen- und Singulärwerte

Sei $f : V \to V'$ eine lineare Abbildung zwischen zwei n-dimensionalen Vektorräumen. Wir erinnern uns an das Ziel, "schöne" Basen $\mathcal{A}$ bzw. $\mathcal{B}$ von V bzw. V' zu finden, so dass die Matrix $M_{\mathcal{A},\mathcal{B}}(f)$ möglichst einfach ist. Genauer werden wir zeigen, dass dies für Orthonormalbasen $\mathcal{A}$ bzw. $\mathcal{B}$ möglich ist. Die Kernbegriffe in diesem Unterfangen sind Eigenwerte und Eigenvektoren.

Bevor wir diese Begriffe jedoch definieren, beginnen wir mit einem Beispiel, dass uns in dem ersten Teil des Kapitels begleiten wird.

Beispiel 10.0.7.

Sei $A = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}$. Betrachtet man das Bild der Vektoren $v_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ und $v_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ unter der Multiplikation mit A stellt man fest, dass

$$A \cdot v_1 = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 3 \cdot 1 + 2 \cdot (-1) \\ 1 \cdot 1 + 2 \cdot (-1) \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot v_1$$

$$A \cdot v_1 = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \cdot 2 + 2 \cdot 1 \\ 1 \cdot 2 + 2 \cdot 1 \end{pmatrix} \begin{pmatrix} 8 \\ 4 \end{pmatrix} = 4 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 4 \cdot v_2$$

die beiden Vektoren also auf sich selbst, bzw. Vielfache von sich selbst abgebildet werden. Das gleiche gilt sogar allgemein für Vielfache von v_1 und v_2, also Vektoren der Form $\lambda_1 \cdot v_1$ bzw. $\lambda_2 \cdot v_2$ für $\lambda_1, \lambda_2 \in \mathbb{R}$. Es ist nämlich

$$A \cdot (\lambda_1 \cdot v_1) = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \cdot 1 \\ \lambda_1 \cdot (-1) \end{pmatrix} = \begin{pmatrix} 3 \cdot \lambda_1 \cdot 1 + 2 \cdot \lambda_1 \cdot (-1) \\ 1 \cdot \lambda_1 \cdot 1 + 2 \cdot \lambda_1 \cdot (-1) \end{pmatrix} = \begin{pmatrix} \lambda_1 \cdot (3 \cdot 1 + 2 \cdot (-1)) \\ \lambda_1 \cdot (1 \cdot 1 + 2 \cdot (-1)) \end{pmatrix}$$
$$= \lambda_1 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot \lambda_1 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot \lambda_1 \cdot v_1$$

$$A \cdot (\lambda_2 \cdot v_2) = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_2 \cdot 2 \\ \lambda_1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 3 \cdot \lambda_2 \cdot 2 + 2 \cdot \lambda_2 \cdot 1 \\ 1 \cdot \lambda_2 \cdot 2 + 2 \cdot \lambda_2 \cdot 1 \end{pmatrix} = \begin{pmatrix} \lambda_2 \cdot (3 \cdot 2 + 2 \cdot 1) \\ \lambda_2 \cdot (1 \cdot 2 + 2 \cdot 1) \end{pmatrix}$$
$$= \lambda_2 \cdot \begin{pmatrix} 8 \\ 4 \end{pmatrix} = 4 \cdot \lambda_2 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 4 \cdot \lambda_2 \cdot v_2.$$

Wir stellen also fest: Es gibt zumindest für die Matrix A aus Beispiel 10.0.7 Vektoren, welche durch die Abbildung nicht ihre Richtung ändern. Dabei lassen sich in diesem Beispiel Vektoren unterscheiden, die um den Faktor 4 gestreckt werden und solche, die völlig unverändert bleiben ("Streckung/Stauchung" um den Faktor 1). Tatsäch-

lich bezeichnet man solche Vektoren als Eigenvektoren und den Streckungs/Stauchungsfaktor als Eigenwert zu der zu A gehörenden linearen Abbildung. Doch nun zur Definition von Eigenwerten und Eigenvektoren linearer Abbildungen.

Definition 10.0.8.

Sei A eine $n \times n$-Matrix.

- Eine reelle Zahl k heißt ***Eigenwert*** von A, wenn es einen Vektor $v \neq 0$ gibt, so dass $A \cdot v = k \cdot v$.
- Entsprechend heißt ein Vektor v ***Eigenvektor*** von A zum Eigenwert k, falls $A \cdot v = k \cdot v$.
- Ferner heißt die Menge aller Eigenvektoren von A zum Eigenwert k ***Eigenraum*** von A zum Eigenwert k. Man schreibt

$$\mathsf{ER}_k(A) = \{v \in \mathbb{R}^n : A \cdot v = k \cdot v\}.$$

Bemerkung 10.0.9.

Eigenwerte charakterisieren wesentliche Eigenschaften linearer Abbildungen, etwa ob ein entsprechendes lineares Gleichungssystem eindeutig lösbar ist oder nicht. In vielen Anwendungen beschreiben Eigenwerte physikalische Eigenschaften eines mathematischen Modells.

Die Verwendung der Vorsilbe "Eigen-" für charakteristische Größen in diesem Sinne lässt sich auf eine Veröffentlichung von David Hilbert aus dem Jahre 1904 zurückführen.

Lemma 10.0.10.

Es sei k ein Eigenwert einer Matrix $A \in \mathbb{R}^{n \times n}$. Der Eigenraum $\mathsf{ER}_k(A)$ zum Eigenwert k ist ein Unterraum des $\mathbb{R}^n$.

Beweis. Es sei k ein Eigenwert einer Matrix A und $\mathsf{ER}_k(A) \subset \mathbb{R}^n$ der zugehörige Eigenraum.

Zu Zeigen ist, dass $\mathsf{ER}_k(A)$ abgeschlossen ist unter Addition und skalarer Multiplikation:

Dazu seien $v, w \in \mathsf{ER}_k(A)$ zwei beliebige Eigenvektoren, sowie $\mu \in \mathbb{R}$ eine beliebige Zahl. Dann sind sowohl $v + w$ als auch $\mu \cdot v$ Eigenvektoren zum Eigenvert k, denn es gilt:

$$\begin{aligned} A \cdot (v + w) &= A \cdot v + A \cdot w & \qquad A \cdot (\mu \cdot v) &= \mu \cdot A \cdot v \\ &= k \cdot v + k \cdot w = k \cdot (v + w) & &= \mu \cdot k \cdot v = k \cdot (\mu \cdot v) \end{aligned}$$

Es gelten also $v + w \in \mathsf{ER}_k(A)$ sowie $\mu \cdot v \in \mathsf{ER}_k(A)$, d.h. $\mathsf{ER}_k(A)$ ist abgeschlossen unter Addition und skalarer Multiplikation und damit ein Unterraum von $\mathbb{R}^n$. □

10.1. Berechnen von Eigenwerten und Eigenvektoren

Es stellen sich nun verschiedene Fragen: Hat jede $n \times n$-Matrix Eigenwerte und Eigenvektoren? Wenn ja, wieviele unterschiedliche Eigenwerte gibt es? Welche Dimension haben die Eigenräume der Eigenwerte? Kann man die Eigenwerte und Eigenvektoren (effizient) bestimmen bzw. gibt es algorithmische Herangehensweisen um diese Fragen zu beantworten?

Eine erste Antwort wird lauten: Ist man in der Lage Eigenwert zu bestimmen, dann kann man die zugehörigen

Eigenvektoren (also den Eigenraum) effizient (natürlich mit dem Gauß-Verfahren) berechnen (also insbesondere die Dimension der Eigenräume bestimmen).

Wie geht man dabei vor, bzw. wo liegen die Schwierigkeiten?

Betrachtet man die definierende Gleichung

$$A \cdot v = k \cdot v, \tag{10.1}$$

dann lässt sich diese als ein Gleichungssystem mit n Gleichungen und $n+1$ Unbekannten (die Komponenten des gesuchten Eigenvektors v und der gesuchte Eigenwert k) interpretieren. Unglücklicher Weise handelt es sich dabei nicht um ein lineares Gleichungssystem, denn auf der rechten Seite der Gleichung stehen Produkte von zwei Unbekannten. Ist jedoch der Eigenwert bekannt, hält man ein lineares Gleichungssystem in der Hand, welches mit Hilfe des Gauß-Verfahrens gelöst werden kann.

Wir verdeutlichen dies zunächst an der Matrix A aus Beispiel 10.0.7:

Beispiel 10.1.1.

Betrachtet man die Matrix $A = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}$, so liest sich Gleichung (10.1) als

$$A \cdot v = \begin{pmatrix} 3 \cdot v_1 + 2 \cdot v_2 \\ 1 \cdot v_1 + 2 \cdot v_2 \end{pmatrix} = \begin{pmatrix} k \cdot v_1 \\ k \cdot v_2 \end{pmatrix}. \tag{10.2}$$

Wir haben in Beispiel 10.0.7 gesehen, dass 4 ein Eigenwert der Matrix A ist. Dort haben wir auch schon gesehen, dass der Eigenraum zu diesem Eigenwert mindestens Vielfache des Vektors $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ beinhaltet. Tatsächlich können wir das mit dem Gauß-Verfahren verifizieren und zeigen, dass der Eigenraum tatsächlich gleich dem Spann dieses Vektors ist. Dazu setze in Gleichung (10.2) $k = 4$ und löse das resultierende LGS:

$$\begin{pmatrix} 3 \cdot v_1 + 2 \cdot v_2 \\ 1 \cdot v_1 + 2 \cdot v_2 \end{pmatrix} = \begin{pmatrix} 4 \cdot v_1 \\ 4 \cdot v_2 \end{pmatrix} \Leftrightarrow \begin{pmatrix} (3-4) \cdot v_1 + 2 \cdot v_2 \\ 1 \cdot v_1 + (2-4) \cdot v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{10.3}$$

Per Gauss-Verfahren lösen:

$$\begin{array}{lccc|c} \text{I} & 3-4 & 2 & & 0 \\ \text{II} & 1 & & 2-4 & 0 \end{array} \quad \rightarrow \quad \begin{array}{lccc|c} \text{I} & -1 & 2 & & 0 \\ \text{II} & 1 & -2 & & 0 \end{array} \quad \xrightarrow{\text{II+I}} \quad \begin{array}{lccc|c} \text{I} & & -1 & 2 & 0 \\ \text{II'} = \text{II} + \text{I} & & 0 & 0 & 0 \end{array}$$

Die einzige Anforderung an einen Eigenvektor v zum Eigenwert $k = 4$ ist also

$$-v_1 + 2 \cdot v_2 = 0 \qquad \text{bzw.} \quad v_1 = 2 \cdot v_2$$

Wir setzen $v_2 := \lambda$ mit $\lambda \in \mathbb{R}$ und erhalten $v = \begin{pmatrix} 2 \cdot \lambda \\ \lambda \end{pmatrix} = \lambda \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix}$. Der zum Eigenwert $k = 4$ gehörige Eigenraum ist also die Menge

$$\mathsf{ER}_4 = \left\{ \lambda \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} \; : \; \lambda \in \mathbb{R} \right\}$$

wie wir es in Beispiel 10.0.7 schon gesehen haben.

Das Ziel ist es also tatsächlich zunächst Eigenwerte zu finden, das berechnen der Eigenräume fällt dann leicht.

10.1.1. Berechnen von Eigenwerten

Schauen wir uns nochmal die Gleichung (10.3) aus Beispiel 10.1.1 etwas näher an. Aus der allgemeinen Gleichung (10.1) folgt, dass für einen Eigenwert k die Gleichung

$$(A - k \cdot \mathrm{id}) \cdot v = 0$$

eine Lösung/Lösungen hat (nämlich die zugehörigen Eigenvektoren).

Insbesondere ist die Matrix $A - k \cdot \mathrm{id}$ also genau dann nicht invertierbar, wenn es einen Eigenvektor zu k gibt.

Bemerkung 10.1.2.

Wieso stimmt diese Aussage?
Wenn k ein Eigenwert ist, ist der Kern von $A - k \cdot \mathrm{id}$ nicht trivial (beinhaltet mehr als nur den Nullvektor, nämlich mindestens einen vom Nullvektor verschiedenen Eigenvektor zu dem Eigenwert k) und demnach der Rang von A echt kleiner n. Nach Korrolar 7.4.21 ist A dann also nicht invertierbar.

An dieser Stelle kommt die Determinante ins Spiel. Denn mit der Eigenschaft **DET8** der Determinante haben wir ein Kriterium in der Hand, dass die Frage beantwortet, ob eine Matrix invertierbar ist. Ist die Determinante einer Matrix ungleich 0, dann ist die Matrix invertierbar, ist die Determinante gleich 0, dann ist sie nicht invertierbar. Wir können also nun für jede Zahl $k \in \mathbb{R}$ prüfe, ob sie ein Eigenwert von A ist, indem wir die Determinante von $(A - k \cdot \mathrm{id})$ berechnen. Denn:

- Wenn $\det(A - k \cdot \mathrm{id}) = 0$ ist, dann ist $A - k \cdot \mathrm{id}$ nicht invertierbar und k ist ein Eigenwert von A.
- Wenn $\det(A - k \cdot \mathrm{id}) \neq 0$ ist, dann ist $A - k \cdot \mathrm{id}$ invertierbar und k ist kein Eigenwert von A.

Es liegt daher nahe, die Funktion

$$\mathsf{char}_A : \mathbb{R} \to \mathbb{R}, \qquad k \mapsto \det(A - k \cdot \mathrm{id})$$

zu betrachten. Nach Definition der Determinante kann man diese Funktion schreiben in der Form

$$\mathsf{char}_A(k) = c_n \cdot k^n + c_{n-1} \cdot k^{n-1} + \ldots + c_1 \cdot k + c_0,$$

wobei $c_0, \ldots, c_n$ reele Zahlen sind (die selbstverständlich von A abhängen). Eine solche Funktion nennt man ***Polynom***. Wir definieren also:

Definition 10.1.3.

Sei A eine $n \times n$-Matrix. Dann heißt char_A das ***charakteristische Polynom*** von A.

Wir formulieren nun eine unseren Überlegungen entsprechende Aussage.

Lemma 10.1.4.

Eine reele Zahl k ist genau dann ein Eigenwert von einer $n \times n$-Matrix A, wenn $\mathsf{char}_A(k) = 0$.

Beispiel 10.1.5.

Für unsere Beispielmatrix $A = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}$ berechnet sich das charakteristische Polynom char_A wie folgt:

$$\begin{aligned} \mathsf{char}_A(k) = \det(A - k \cdot I) &= \det\left(\begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} - z \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = \det\left(\begin{pmatrix} 3-k & 2 \\ 1 & 2-k \end{pmatrix} \right) \\ &= (3-k) \cdot (2-k) - 1 \cdot 2 \\ &= k^2 - 5z + 4 \end{aligned}$$

Die Nullstellen $k_1 = 1$ und $k_2 = 4$ des charakteristischen Polynoms berechnet man entweder per p-q-Formel oder entnimmt sie aus $k^2 - 5k + 4 = (k-4) \cdot (k-1)$.

Die Eigenwerte von A sind also $k_1 = 1$ und $k_2 = 4$.

10.2. Diagonalisierbarkeit - Symmetrische Matrizen (Eigenwertzerlegung)

In diesem Abschnitt werden wir das Ziel erreichen, (zumindest manche) lineare Abbildungen mittels eines Basiswechsels durch einfache, das heißt in Diagonalform (nur auf der Diagonalen sind die Einträge von Null verschieden), Darstellungsmatrizen zu beschreiben. Tatsächlich sind die Diagonaleinträge Eigenwerte und die Basis bezüglich welche die schöne Darstellung in Diagonalform existiert ist orthogonal und besteht aus Eigenvektoren. Die linearen Abbildungen, für welche diese Darstellung immer möglich ist, haben Darstellungsmatrizen (bezüglich der Standartbasis), die symmetrisch sind. Das meint, dass jeweils die i-te Zeile der i-ten Spalte entspricht. Wir starten mit der Definition von symmetrischen Matrizen.

Definition 10.2.1.

Eine $n \times n$-Matrix A heißt ***symmetrisch***, wenn $A^T = A$.

Wir sind also in der Lage den Satz für symmetrische Matrizen zu formulieren.

Satz 10.2.2.

Zu jeder symmetrischen $n \times n$-Matrix A existieren

- eine orthogonale $n \times n$-Matrix U
- reelle Zahlen $k_1, \ldots, k_n$ (nicht notwendigerweise verschieden)

so dass

$$U^T \cdot A \cdot U = \mathrm{diag}(k_1, \ldots, k_n).$$

Dabei sind

- die Zahlen $k_1, \ldots, k_n$ genau die Eigenwerte von A
- die Spalten von U eine Orthonormalbasis, die aus Eigenvektoren von A besteht.

Für den Beweis dieses Satzes benötigt man folgendes Lemma, dessen Beweis über den Rahmen dieser Vorlesung hinaus geht.

Lemma 10.2.3.

Wenn A eine symmetrische Matrix ist, dann existieren ein n reelle Zahlen $k_1, \ldots, k_n$ (nicht notwendigerweise verschieden) und ein $q \in \{-1, 1\}$, so dass

$$\mathsf{char}_A(k) = q \cdot \prod_{i=1}^{n} (k - k_i).$$

Bemerkung 10.2.4.

Bei den reellen (nicht notwendigerweise verschiedenen) Zahlen $k_1, \ldots, k_n$ handelt es sich also genau um die Nullstellen des charakteristischen Polynoms char_A, also nach Lemma 10.1.4 um die Eigenwerte von A.

Beweis. [Beweis von Satz 10.2.2] Wir führen eine vollständige Induktion über die Größe n der Matrix.

Induktionsverankerung: Im Fall $n = 1$ hat die Matrix A selbst bereits die gewünschte Form und wir wählen einfach $U = (1)$ und $k_1 = A_{11}$

Induktionsannahme: Wir nehmen als Induktionsvorraussetzung an, dass für ein festes n und für jede symmetrische $n \times n$-Matrix A es

- eine orthogonale $n \times n$-Matrix U
- reelle Zahlen $k_1, \ldots, k_n$ (nicht notwendigerweise verschieden)

gibt, so dass

$$U^T \cdot A \cdot U = \mathrm{diag}(k_1, \ldots, k_n).$$

Wobei

- die Zahlen $k_1, \ldots, k_n$ genau die Eigenwerte von A sind.
- die Spalten von U eine Orthonormalbasis ist, die aus Eigenvektoren von A besteht.

Induktionsschluss: Sei Also A eine symmetrische $(n+1) \times (n+1)$-Matrix. Lemma 10.2.3 zeigt, dass es eine reele Zahl k_1 gibt mit $\mathsf{char}_A(k_1) = 0$. Demnach hat A einen Eigenvektor $b_1 \neq 0$. Sei $F_1 = \mathsf{span}\{x_1\}$. Betrachte nun die Menge

$$W_1^{\perp} = \{v \in V : \langle v, v_1 \rangle\}.$$

Der Vektorraum $W_1^{\perp}$ besitzt eine Orthonormalbasis $b_2, \ldots, b_n$. Sei U_1 die orthogonale Matrix mit Spalten

$b_1, \ldots, b_n$. Weil b_1 ein Eigenvektor und A symmetrisch ist, gibt es eine $n \times n$-Matrix A', so dass

$$U_1^T \cdot A \cdot U_1 = \begin{pmatrix} k_1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}.$$

Nach Induktionsvorraussetzung gibt es eine orthonormale $n \times n$-Matrix U_2 und reelle Zahlen $k_2, \ldots, k_n$, so dass

$$U_2^T \cdot A' \cdot U_2 = \text{diag}(k_2, \ldots, k_n).$$

Sei nun U die $n \times n$-Matrix

$$U = U_1 \cdot \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & U_2 & \\ 0 & & & \end{pmatrix}.$$

Nach Lemma 9.3.6 ist U orthogonal. Ferner gilt

$$U^T \cdot A \cdot U = \begin{pmatrix} k_1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & U_2^T \cdot A' \cdot U_2 & \\ 0 & & & \end{pmatrix} = \text{diag}(k_1, \ldots, k_n),$$

wie behauptet. □

Beispiel 10.2.5.

Wir diagonalisieren die Matrix $A = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$.

Ihr charakteristisches Polynom lautet

$$\begin{aligned} \mathsf{char}_A(k) = \det(A - k \cdot \mathrm{id}) &= \det\left(\begin{pmatrix} -1-k & 1 \\ 1 & 1-k \end{pmatrix}\right) \\ &= (-1-k)\cdot(1-k) - 1 \cdot 1 = k^2 - 2 = (k - \sqrt{2}) \cdot (k + \sqrt{2}). \end{aligned}$$

Die Nullstellen des charakteristischen Polynoms (und damit die Eigenwerte von A) sind also $k_1 = -\sqrt{2}$ und

$k_2 = \sqrt{2}$. Um auch die Eigenvektoren zu bestimmen, lösen wir die beiden linearen gleichungssysteme

$$(A - k_1\mathrm{id}) \cdot x = \begin{pmatrix} -1+\sqrt{2} & 1 \\ 1 & 1+\sqrt{2} \end{pmatrix}$$

$$(A - k_2\mathrm{id}) \cdot x = \begin{pmatrix} -1-\sqrt{2} & 1 \\ 1 & 1-\sqrt{2} \end{pmatrix}$$

Die Lösungsmenge für das erste lineare Gleichungssystem zum Eigenwert $k_1 = -\sqrt{2}$ ist

$$\mathsf{span}\left\{\begin{pmatrix} 1/(1-\sqrt{2}) \\ 1 \end{pmatrix}\right\}$$

und die Lösungsmenge für das zweite lineare Gleichungssystem zum Eigenwert $k_1 = \sqrt{2}$ ist

$$\mathsf{span}\left\{\begin{pmatrix} 1/(1+\sqrt{2}) \\ 1 \end{pmatrix}\right\}.$$

Wir haben also die beiden Eigenräume zu den Eigenwerten $k_1 = -\sqrt{2}$ und $k_2 = \sqrt{2}$ berechnet. Es ist

$$\mathsf{ER}_{-\sqrt{2}}(A) = \mathsf{span}\left\{\begin{pmatrix} 1/(1-\sqrt{2}) \\ 1 \end{pmatrix}\right\} \quad \text{und} \quad \mathsf{ER}_{\sqrt{2}}(A) = \mathsf{span}\left\{\begin{pmatrix} 1/(1+\sqrt{2}) \\ 1 \end{pmatrix}\right\}.$$

Betrachte die Vektoren

$$v_1 = \begin{pmatrix} 1/(1-\sqrt{2}) \\ 1 \end{pmatrix} \quad \text{und} \quad v_2 = \begin{pmatrix} 1/(1+\sqrt{2}) \\ 1 \end{pmatrix}.$$

Die Norm dieser Vektoren ist

$$\|v_1\| = \sqrt{1 + 1/(1-\sqrt{2})^2}, \qquad \|v_2\| = \sqrt{1 + 1/(1+\sqrt{2})^2}.$$

Die beiden Vektoren

$$u_1 = \frac{1}{\|v_1\|} \cdot v_1 = \sqrt{1 + 1/(1-\sqrt{2})^2} \cdot \begin{pmatrix} 1/(1-\sqrt{2}) \\ 1 \end{pmatrix} \quad \text{und}$$

$$u_2 = \frac{1}{\|v_2\|} \cdot v_2 = \sqrt{1 + 1/(1+\sqrt{2})^2} \cdot \begin{pmatrix} 1/(1+\sqrt{2}) \\ 1 \end{pmatrix}$$

bilden also eine Orthonormalbasis des $\mathbb{R}^2$, die aus Eigenvektoren besteht. Wenn U die Matrix mit den Spalten u_1 und u_2 ist, dann ist U orthogonal und

$$U^T \cdot A \cdot U = \begin{pmatrix} k_1 & 0 \\ 0 & k_2 \end{pmatrix} = \begin{pmatrix} -\sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}.$$

10.3. Diagonalisierbarkeit - Allgemeine Matrizen (Singulärwertzerlegung)

Leider erfaßt Satz 10.2.2 nur symmetrische Matrizen und in der Tat gibt es Matrizen, die (zwar quadratisch aber) nicht symmetrisch sind, für die keine Zerlegung der Form $U^T \cdot A \cdot U$ existiert. Allerdings kann man die Matrix in Diagnalform bringen, indem man links und rechts mit zwei möglicherweise verschiedenen orthogonalen Matrizen multipliziert. Mehr noch, dies ist sogar für allgemeine Matrizen immer möglich, das heißt insbesondere auch für nicht quadratische Matrizen.

Satz 10.3.1.

Sei A eine $m \times n$-Matrix. Dann existieren eine orthogonale $m \times m$-Matrix V, eine orthogonale $n \times n$-Matrix U und eine $m \times n$-Matrix in Diagonalform, so dass $V^T \cdot A \cdot U = D$.

Beweis. Wir beschäftigen uns zunächst mit dem Spezialfall, dass A eine invertierbare $n \times n$-Matrix ist. Weil die Matrix $A^T \cdot A$ symmetrisch ist, kann man sie nach Satz 10.2.2 schreiben als

$$U^T \cdot A^T \cdot A \cdot U = \text{diag}(k_1, \ldots, k_n).$$

Dabei sind $k_1, \ldots, k_n$ von Null verschieden, weil A invertierbar ist. Wir behaupten, dass die Vektoren

$$A \cdot U^{(1)}, \ldots, A \cdot U^{(n)}$$

orthogonal sind. Denn für je zwei Indices $1 \leq i < j \leq n$ gilt

$$\begin{aligned}\langle A \cdot U^{(i)}, A \cdot U^{(j)} \rangle &= \langle A^T \cdot A \cdot U^{(i)}, U^{(j)} \rangle = \langle U \cdot \text{diag}(k_1, \ldots, k_n) \cdot U^T \cdot U^{(i)}, U^{(j)} \rangle \\ &= \langle \text{diag}(k_1, \ldots, k_n) \cdot U^T \cdot U^{(i)}, U^T \cdot U^{(j)} \rangle \\ &= \langle \text{diag}(k_1, \ldots, k_n) \cdot e^{(i)}, e^{(j)} \rangle \\ &= k_i \langle e^{(i)}, e^{(j)} \rangle = 0.\end{aligned}$$

Analog gilt für alle $i = 1, \ldots, n$

$$\|A \cdot U^{(i)}\|^2 = \langle A \cdot U^{(i)}, A \cdot U^{(i)} \rangle = k_i \langle e^{(i)}, e^{(v)} \rangle \neq 0.$$

Die Vektoren

$$v_i = \frac{1}{\|A \cdot U^{(i)}\|} \cdot A \cdot U^{(i)} \qquad (i = 1, \ldots, n)$$

sind also orthonormal. Folglich ist die Matrix V mit den Spalten $v_1, \ldots, v_n$ orthogonal. Wir definieren

$$d_i = \langle A \cdot U^{(i)}, v_i \rangle$$

und $D = \text{diag}(d_1, \ldots, d_n)$. Sei nun $B = V \cdot D \cdot U^T$. Für $i = 1, \ldots, n$ erhalten wir

$$\begin{aligned}B \cdot U \cdot e^{(i)} = B \cdot U^{(i)} &= (V \cdot D \cdot U^T) \cdot U^{(i)} = V \cdot D \cdot e^{(i)} = d_i \cdot v_i \\ &= \frac{\langle A \cdot U^{(i)}, A \cdot U^{(i)} \rangle}{\|A \cdot U^{(i)}\|^2} \cdot A \cdot U^{(i)} = A \cdot U^{(i)} = A \cdot U^{(i)} \cdot e^{(i)}.\end{aligned}$$

Folglich gilt $B \cdot U = A \cdot U$, weshalb $V \cdot D \cdot U^T = B = A$.

Wir befassen uns nun mit dem Fall, dass A keine invertierbare $n \times n$-Matrix ist. In diesem Fall betrachten wir den Kern von A als Teilmenge des $\mathbb{R}^n$ und das Bild von A im $\mathbb{R}^m$, als den von den Spalten von A aufgespannten Untervektorraum.

Nach dem Dimensionssatz und Proposition 9.2.8 haben die beiden Vektorräume $\mathsf{Kern}(A)^\perp$ und $\mathsf{Bild}(A)$ dieselbe Dimension ℓ und die lineare Abbildung $f : \mathsf{Kern}(A)^\perp \to \mathsf{Bild}(A), v \mapsto A \cdot V$ ist invertierbar.

Nach dem soeben gezeigten, existieren also Orthonormalbasen $\mathcal{A}'$ und $\mathcal{B}'$ von $\mathsf{Kern}(A)^\perp$ und $\mathsf{Bild}(A)$ sowie eine Diagonalmatrix D', so dass $M_{\mathcal{A}',\mathcal{B}'}(f) = D'$. Seien $\mathcal{A}''$ und $\mathcal{B}''$ nun Orthonormalbasen von $\mathsf{Kern}(A)$ und $\mathsf{Bild}(A)^\perp$. Fügen wir $\mathcal{A}'$ und $\mathcal{A}''$ zu $\mathcal{A}$ sowie $\mathcal{B}'$ und $\mathcal{B}''$ zu $\mathcal{B}$ zusammen, so erhalten wir eine Orthonormalbasis $\mathcal{A}$ von $\mathbb{R}^n$ und eine Orthonormalbasis $\mathcal{B}$ von $\mathbb{R}^m$. Sei schließlich D die $m \times n$-Matrix in Diagonalform deren einzige von Null verschiede Einträge die Einträge $D_{ii} = D'_{ii}$ für $i = 1, \ldots, \ell$ sind. Dann ist $M_{\mathcal{A},\mathcal{B}}(A) = D$. Die Spalten von $\mathcal{A}$ und $\mathcal{B}$ bilden also orthogonale Matrizen U und V, so dass $A = V^T \cdot D \cdot U$. □

Definition 10.3.2.

Die Darstellung $A = V \cdot D \cdot U$ aus Satz 10.3.1 nennt sich die ***Singulärwertzerlegung von*** A. Die Diagonaleinträge der Matrix D heißen entsprechend die ***Singulärwerte von*** A.

Teil III.

Ausgewählte Themen der Analysis

11 Folgen und Reihen

Das Thema des nun folgenden zweiten Abschnittes der Vorlesung ist die Analysis zunächst auf $\mathbb{R}$, dann auch auf $\mathbb{R}^n$.

11.1. Folgen

Wir beginnen direkt mit der Definition von Folgen.

Definition 11.1.1.

Eine Folge $(a_n)_{n\in\mathbb{N}}$ reeller Zahlen ist eine Abbildung $\mathbb{N} \to \mathbb{R}$, der Form $n \mapsto a_n$. Man schreibt die Folge in der Form $(a_n)_{n\in\mathbb{N}} = (a_1, a_2, a_3, \ldots)$. Die a_n werden als Folgenglieder bezeichnet.

Bemerkung 11.1.2.

Eine Folge kann auf verschiedene Weisen angegeben werden.

- Aufzählend (z.B. $(a_n)_{n\in\mathbb{N}} = (\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \ldots)$)
- Definierend (z.B. $a_n := \frac{1}{2^n}$ für alle $n \in \mathbb{N}$)
- Rekursiv durch einen Startwert und eine Rekursionsgleichung (z.B. $a_1 = \frac{1}{2}$ und $a_{n+1} = \frac{1}{2} \cdot a_n$)

Beispiel 11.1.3.

Die Folge $(a_n)_{n\in\mathbb{N}} = (0, 1, 2, 3, 4, \ldots)$ der natürlichen Zahlen lässt sich tatsächlich auf alle drei unterschiedlichen Weisen angeben:

- Definierend ist $a_n := n$ für alle $n \in \mathbb{N}$
- Rekursiv durch (einen) Startwert(e) und eine Rekursionsgleichung, zum Beispiel:
  - $a_1 = 1$ und $a_{n+1} = a_n + 1$ für alle $n \in \mathbb{N}$
  - $a_1 = 1, a_2 = 2$ und $a_{n+2} = a_n + 2$ für alle $n \in \mathbb{N}$

Definition 11.1.4.

Eine Zahl $x \in \mathbb{R}$ heißt ***Grenzwert*** oder ***Limes*** der Folge $(a_n)_{n\in\mathbb{N}}$ wenn folgende Bedingung erfüllt ist.

$$\forall \varepsilon \in \mathbb{R}, \varepsilon > 0 \ : \ \exists N \in \mathbb{N} \ : \ |a_n - x| \leq \varepsilon \quad \forall n \in \mathbb{N}, n \geq N$$

In diesem Fall schreibt man $x = \lim_{n\to\infty} a_n$ an und sagt, dass *"$(a_n)_{n\in\mathbb{N}}$ gegen x konvergiert"*.

Bemerkung 11.1.5.

In Worten bedeutet dies, dass eine Zahl $x \in \mathbb{R}$ dann Grenzwert der Folge $(a_n)_{n\in\mathbb{N}}$ heißt, wenn:

Zu jedem reellen Abstand $\varepsilon > 0$ existiert ein Index $N \in \mathbb{N}$, ab dem für alle $n \geq N$ gilt:

a_n ist dichter an x als der Abstand ε.

Beispiel 11.1.6.

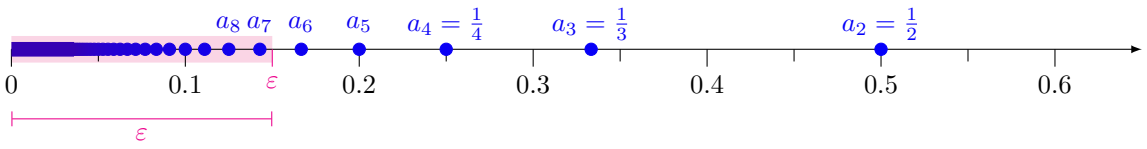
Die Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_n = \frac{1}{n}$ hat den Grenzwert $x = 0$:

Zu gegebenem $\varepsilon > 0$ definiert man $N_\varepsilon := \lceil \frac{1}{\varepsilon} \rceil$ (dies ist Aufrunden von $\frac{1}{\varepsilon}$). Für alle $n \geq N_\varepsilon$ gilt dann zunächst $|a_n - x| = |a_n - 0| = |a_n| = \frac{1}{n}$ und dies lässt sich wie folgt gegen ε abschätzen:

$$|a_n - x| = \frac{1}{n} \leq \frac{1}{N} = \frac{1}{\lceil \frac{1}{\varepsilon} \rceil} \leq \frac{1}{\frac{1}{\varepsilon}} = \varepsilon$$

Ein Beispiel: Für $\varepsilon = 0.15$ ist $N_\varepsilon := \lceil \frac{1}{\frac{15}{100}} \rceil = \lceil \frac{100}{15} \rceil = 7$.

Es gilt also: Ab $n = 7$ ist der Abstand $|a_n - 0|$ kleiner als 0.16, d.h. $|a_7 - 0|, |a_8 - 0|, |a_9 - 0|, \ldots \leq \varepsilon$



Der Begriff des Grenzwerts ist eng verbunden mit dem folgenden Konzept.

Definition 11.1.7.

Sei $A \subset \mathbb{R}$ eine Menge reeller Zahlen.

- Wir nennen eine Zahl $x \in \mathbb{R}$ eine ***obere Schranke für*** A, falls für alle $a \in A$ gilt $a \leq x$.
- Analog heißt $y \in \mathbb{R}$ eine ***untere Schranke für*** A, falls für alle $a \in A$ gilt $a \geq y$.
- Die Menge A heißt ***nach oben/unten beschränkt***, falls sie eine obere/untere Schranke hat. Falls beides zutrifft, nennt man A einfach ***beschränkt***.
- Sei A eine nach oben beschränkte Menge. Wir nennen $x \in \mathbb{R}$ das ***Supremum von*** A, falls x eine obere Schranke von A ist und für jede obere Schranke z von A gilt $z \geq x$. Man schreibt dann $\sup(A) = x$ (verkürzend schreibt man manchmal $\sup A = x$).
- Entsprechend heißt $y \in \mathbb{R}$ das ***Infimum einer nach unten beschränkten Menge*** A, falls y eine untere Schranke von A ist und für jede untere Schranke z von A gilt $z \leq y$. Man schreibt dann $\inf(A) = y$ (verkürzend schreibt man manchmal $\inf A = y$).

Die folgende Tatsache werden wir nicht beweisen, weil dies eine genauere Beschäftigung mit den reellen Zahlen voraussetzen würde, als der Rahmen dieser Vorlesung erlaubt.

Fact 11.1.8.

Jede nach oben beschränkte Menge $A \subset \mathbb{R}$ hat ein Supremum, und jede nach unten beschränkte Menge hat ein Infimum.

Beispiel 11.1.9.

Sei A die Menge aller $x \in \mathbb{R}$ mit $x^2 \leq 3$.

Diese Menge ist beschränkt, denn jedes $x \in A$ erfüllt $-2 \leq x \leq 2$. Folglich hat A sowohl ein Supremum, nämlich $\sqrt{3}$ als auch ein Infimum und zwar $-\sqrt{3}$.

(Dieses Beispiel zeigt insbesondere, dass Fakt 11.1.8 in den rationalen Zahlen $\mathbb{Q}$ nicht zutrifft, denn $\pm\sqrt{3}$ sind irrational.)

Definition 11.1.10.

Wir nennen eine Folge $(a_n)_{n\in\mathbb{N}}$ ***nach oben/unten beschränkt***, falls die Menge $\{a_n : n \in \mathbb{N}\}$ diese Eigenschaft hat. Ferner heißt $(a_n)_{n\in\mathbb{N}}$

- *monoton wachsend*, falls für alle $n \in \mathbb{N}$ gilt: $a_n \leq a_{n+1}$
- ***streng** monoton wachsend*, falls für alle $n \in \mathbb{N}$ gilt: $a_n < a_{n+1}$
- *monoton fallend*, falls für alle $n \in \mathbb{N}$ gilt: $a_n \geq a_{n+1}$
- ***streng** monoton fallend*, falls für alle $n \in \mathbb{N}$ gilt: $a_n > a_{n+1}$

Beispiel 11.1.11.

- Die Folge $(a_n)_{n\in\mathbb{N}} = (1, 2, 3, 4, \ldots)$ ist
  - streng monoton wachsend denn es gilt $a_n < a_{n+1} = a_n + 1$ für alle $n \in \mathbb{N}$
  - nach unten beschränkt, denn es gilt $a_n \geq 1$ für alle $n \in \mathbb{N}$

  Hinweise: Die Folge ist *nicht* nach oben beschränkt.
  Die Folge ist auch "monoton wachsend" (ohne den Zusatz "streng") denn die schwächere Forderung "$a_n \leq a_{n+1}$" ist auch erfüllt!
- Die Folge $(a_n)_{n\in\mathbb{N}} = (\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots)$ mit $a_n := \frac{1}{2^n}$ ist
  - streng monoton fallend denn es gilt $a_n > a_{n+1} = a_n \cdot \frac{1}{2}$ für alle $n \in \mathbb{N}$
  - nach unten beschränkt, denn es gilt $a_n \geq 0$ für alle $n \in \mathbb{N}$
  - nach oben beschränkt, denn es gilt $a_n \leq 1$ für alle $n \in \mathbb{N}$

  Hinweis:
  Die Folge ist auch "monoton fallend" (ohne den Zusatz "streng") denn die schwächere Forderung "$a_n \geq a_{n+1}$" ist auch erfüllt!

Das folgende Konvergenzkriterium liefert eine qualitative Aussage über das *Konvergenzverhalten* einer Folge, d.h. wir erfahren ob eine Folge konvergiert oder nicht. Das Kriteriumc harakterisiert den Grenzwert zwar, gibt jedoch kein Berechnungsschema an (ist demnach nicht quantitative).

Proposition 11.1.12.

Sei $(a_n)_{n\in N}$ eine Folge.

- Wenn $(a_n)_{n\in N}$ monoton wachsend und nach oben beschränkt ist, dann konvergiert diese Folge gegen $\sup\{a_n : n \in \mathbb{N}\}$.
- Wenn $(a_n)_{n\in N}$ monoton fallend und nach unten beschränkt ist, dann konvergiert diese Folge gegen $\inf\{a_n : n \in \mathbb{N}\}$.

Beweis. Wir zeigen nur die erste Behauptung. Die zweite foglt aus dieser, wenn man zu der Folge $(-a_n)_{n\in\mathbb{N}}$ übergeht.

Sei also $s = \sup\{a_n : n \in \mathbb{N}\}$ und sei $\varepsilon > 0$. Wir möchten zeigen, dass s der Grenzwert der Folge $(a_n)_{n\in\mathbb{N}}$ ist, müssen also einen Index finden, so dass alle diesem Index folgenden Folgenglieder höchstens Abstand ε zu s haben.

Weil s das Supremum ist, gibt es ein N_ε, so dass $a_{N_\varepsilon} \geq s - \varepsilon$.

(Gäbe es das nicht, wäre $s - \varepsilon$ eine obere Schranke an $\{a_n : n \in \mathbb{N}\}$ und s nicht das Supremum von $\{a_n : n \in \mathbb{N}\}$.)

Für alle $n > N_\varepsilon$ gilt folglich $s \geq a_n \geq a_{N_\varepsilon} \geq s - \varepsilon$.

Demnach gilt für alle $n > N_\varepsilon$, dass $|a_n - s| \leq \varepsilon$, was zu zeigen war. □

Beispiel 11.1.13.

- Die Folge $(a_n)_{n\in\mathbb{N}} = (\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots)$ mit $a_n := \frac{n}{n+1}$ ist konvergent, denn:
  - Offensichtlich gilt $\frac{n}{n+1} \leq \frac{n}{n+1} + \frac{1}{n+1} = 1$ und damit ist die Folge nach oben beschränkt.
  - Weiter ist die Folge monoton wachsend, d.h. es gilt stets $a_n \leq a_{n+1}$ wegen:

$$\begin{aligned} & \tfrac{n}{n+1} && \leq && \tfrac{n+1}{n+2} && \mid \cdot (n+1)\cdot(n+2) \\ \Leftrightarrow\ & n\cdot(n+2) && \leq && (n+1)\cdot(n+1) && \\ \Leftrightarrow\ & n^2 + 2n && \leq && n^2 + 2n + 1 && \text{(eine wahre Aussage)} \end{aligned}$$

- Sei $0 \leq q < 1$. Die Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_n := q^n$ konvergiert, denn diese Folge ist monoton fallend und nach unten beschränkt durch 0.

11.1.1. Teilfolgen und Cauchyfolgen

Wir beginnen mit der Definition von Teilfolgen.

Definition 11.1.14.

Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge und $(m_n)_{n\in\mathbb{N}}$ eine streng monoton wachsende Folge mit $m_n \in \mathbb{N}$ für alle $n \in \mathbb{N}$. Dann ist $(a_{m_n})_{n\in\mathbb{N}}$ eine Folge, die wir ***Teilfolge von*** $(a_n)_{n\in\mathbb{N}}$ nennen.

Beispiel 11.1.15.

Betrachte die Folgen $(a_n)_{n\in\mathbb{N}} = (\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots)$ mit $a_n := \frac{1}{2^n}$ und $(m_n)_{n\in\mathbb{N}} = (1, 3, 5, 7, \ldots)$ die Folge der ungeraden natürlichen Zahlen. Dann ist $(a_{m_n})_{n\in\mathbb{N}} = (\frac{1}{2}, \frac{1}{8}, \frac{1}{32}, \ldots)$.

Lemma 11.1.16.

Jede Folge $(a_n)_{n\in\mathbb{N}}$ hat entweder eine monoton wachsende oder eine monoton fallende Teilfolge.

Beweis. Sei $\mathcal{B}$ die Menge aller Zahlen $n \in \mathbb{N}$, so dass $a_n > a_j$ für alle $j > n$, also

$$\mathcal{B} = \{n \in \mathbb{N} : a_n > a_j \ \ \forall j \in \mathbb{N}, j > n\}.$$

In Worten sammelt die Menge $\mathcal{B}$ alle Indizes derjenigen Folgenglieder, deren Wert echt größer als der von allen nachfolgenden Folgengliedern ist.

Wir betrachten zwei Fälle.

Fall 1: die Menge $\mathcal{B}$ ist unendlich. Sei $(m_n)_{n\in\mathbb{N}}$ streng monoton wachsend, so dass

$$\{m_n : n \in \mathbb{N}\} \subset B.$$

Dann ist die Folge $(a_{m_n})_{n\in\mathbb{N}}$ (streng) monoton fallend.

Fall 2: die Menge $\mathcal{B}$ ist endlich. Dann hat B eine oberer Schranke $n_0 \in \mathbb{N}$. Wir konstruieren die Folge $(m_n)_{n\in\mathbb{N}}$ induktiv, beginnend mit $m_1 = n_0 + 1$. Wenn m_n bereits definiert ist, definieren wir

$$C_{n+1} = \{k \in \mathbb{N} : a_k \geq a_{m_n}, k > m_n\}.$$

diese Menge ist nicht leer, weil $m_n \notin B$. Sei also $m_{n+1} = \min(C_{n+1})$. Dann ist $(a_{m_n})_{n\in\mathbb{N}}$ monoton wachsend.

□

Satz 11.1.17 (Bolzano-Weierstraß)**.**

Jede beschränkte Folge enthält (mindestens) eine konvergente Teilfolge.

Beweis. Folgt direkt aus Proposition 11.1.12 und Lemma 11.1.16. □

Können wir einer Folge irgendwie ansehen, ob sie konvergiert oder nicht, ohne notwendigerweise den Grenzwert zu kennen? Um dies zu beantworten, benötigen wir eine weitere

Definition 11.1.18.

Eine Folge $(a_n)_{n\in\mathbb{N}}$ heißt ***Cauchyfolge***, wenn

$$\forall \varepsilon \in \mathbb{R}, \varepsilon > 0 \ : \ \exists N \in \mathbb{N} \ : \ |a_n - a_m| \leq \varepsilon \quad \forall n, m \in \mathbb{N}, n, m \geq N$$

Die Definition der Cauchyfolge ähnelt der Definition des Grenzwertes einer Folge und tatsächlich gilt

Proposition 11.1.19.

Eine Folge $(a_n)_{n\in\mathbb{N}}$ konvergiert genau dann, wenn sie eine Cauchyfolge ist.

Beweis.

"$\Rightarrow$" Angenommen $(a_n)_{n\in\mathbb{N}}$ konvergiert gegen $z \in \mathbb{R}$. Sei $\varepsilon > 0$ und sei $N_\varepsilon \in \mathbb{N}$, so dass $|a_n - z| < \varepsilon$ für alle $n \geq N_\varepsilon$. Dann gilt für alle $n, m > N_\varepsilon$

$$|a_n - a_m| \leq |a_n - z| + |a_m - z| < 2\varepsilon.$$

Folglich ist $(a_n)_{n\in\mathbb{N}}$ eine Cauchyfolge.

"$\Leftarrow$" Nehmen wir also umgekehrt an, dass $(a_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist. Es gelten zwei Dinge:

- Die Folge $(a_n)_{n\in\mathbb{N}}$ ist beschränkt. (Denn wählt man $\varepsilon = 1$, dann gibt es ein N_1, so dass alle Folgenglieder a_n für $n \in \mathbb{N}$ kleiner gleich dem Maximum der ersten N_1 Folgenglieder und $a_{N_1} + 1$ sind.)
- Demnach existiert eine monotone Teilfolge $(a_{m_n})_{n\in\mathbb{N}}$, die nach Proposition 11.1.12 gegen eine Zahl $z \in \mathbb{R}$ konvergiert.

Sei nun $\varepsilon > 0$ und wähle N_ε so, dass $|a_{N_\varepsilon} - a_n| < \varepsilon$ für alle $n > N_\varepsilon$. Weil

$$\lim_{n\to\infty} a_{m_n} = z,$$

existiert ein $k \in \mathbb{N}$, so dass $m_k > N_\varepsilon$ und $|a_{m_k} - z| < \varepsilon$.
Für alle $n > m_k$ gilt folglich

$$|a_n - z| \leq |a_{m_k} - z| + |a_{m_k} - a_n| \leq 2\varepsilon.$$

Daraus folgt $\lim_{n\to\infty} a_n = z$.

□

11.2. Berechnen von Grenzwerten

Das folgende Lemma enthält implizit ein Rechenverfahren zum Berechnen von Grenzwerten von zusammengesetzten Funktionen. Im Prinzip darf man das Bilden des Grenzwerts an allen bekannten Rechenzeichen "zerteilen".

Um formal korrekt zu bleiben ist es wichtig, dass in der entsprechenden Berechnung zuerst in einer Nebenrechnung die Grenzwerte der Teilfunktionen berechnet werden, um diese *erst danach* zu einem Ganzen zusammenzusetzen:

Lemma 11.2.1.

Es seien $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ zwei konvergente Folgen mit Grenzwerten

$$\lim_{n\to\infty} a_n = a \quad \text{und} \quad \lim_{n\to\infty} b_n = b$$

Dann gelten für die zusammengesetzten Folgen:

- **Addition** $\lim\limits_{n\to\infty}(a_n + b_n) = a + b$ sowie
  $\lim\limits_{n\to\infty}(a_n - b_n) = a - b$
- **Multiplikation** $\lim\limits_{n\to\infty}(a_n \cdot b_n) = a \cdot b$

Gilt zusätzlich $b \neq 0$ so folgt

- **Division** $\lim\limits_{n\to\infty}\frac{a_n}{b_n} = \frac{a}{b}$

Beispiel 11.2.2.

Aus Beispiel 11.1.6 wissen wir bereits, dass $\lim_{n\to\infty}\frac{1}{n} = 0$ gilt.

Enstprechend folgern wir für $\frac{1}{n^3}$:

$$\lim_{n\to\infty}\frac{1}{n^2} = 0 \text{ wegen } \lim_{n\to\infty}\frac{1}{n^2} = \lim_{n\to\infty}\frac{1}{n}\cdot\frac{1}{n} = 0\cdot 0$$

$$\lim_{n\to\infty}\frac{1}{n^3} = 0 \text{ wegen } \lim_{n\to\infty}\frac{1}{n^3} = \lim_{n\to\infty}\frac{1}{n}\cdot\frac{1}{n^2} = 0\cdot 0$$

Induktiv lässt sich analog $\lim_{n\to\infty}\frac{1}{n^k} = 0$ für alle $k \in \mathbb{N}\setminus\{0\}$ zeigen.

Für rationale Funktionen (Brüche aus Polynomen) in $n \in \mathbb{N}$ gibt es ein einfaches Verfahren zum Berechnen des Grenzwertes:

1. Finde die größte im Nenner auftretende Potenz n^k und *kürze* den Bruch mit dieser.
2. Berechne den Grenzwert unter Verwendung von $\lim\limits_{n\to\infty}\frac{1}{n^k} = 0$ und $\lim\limits_{n\to\infty} n^k = \infty$ und

Beispiel 11.2.3.

Es sei $a_n := \dfrac{8\cdot n^2 + 3\cdot n^3}{3\cdot n + 2\cdot n^4}$. Dann gilt:

$$\lim_{n\to\infty}\frac{8\cdot n^2 + 3\cdot n^3}{3\cdot n + 2\cdot n^4} = \lim_{n\to\infty}\frac{(8\cdot\frac{1}{n^2} + 3\cdot\frac{1}{n})\cdot n^4}{(3\cdot\frac{1}{n^3} + 2\cdot 1)\cdot n^4} = \lim_{n\to\infty}\frac{(8\cdot\frac{1}{n^2} + 3\cdot\frac{1}{n})}{(3\cdot\frac{1}{n^3} + 2\cdot 1)} = \frac{0+0}{0+2} = 0$$

Denn es gelten: $\lim\limits_{n\to\infty}\frac{1}{n} = 0$, $\lim\limits_{n\to\infty}\frac{1}{n^2} = 0$ und $\lim\limits_{n\to\infty}\frac{1}{n^3} = 0$

Beispiel 11.2.4.

Es sei $a_n := \dfrac{8\cdot n^2 + 3\cdot n^4}{3\cdot n + 2\cdot n^4}$. Dann gilt:

$$\lim_{n\to\infty}\frac{8\cdot n^2 + 3\cdot n^4}{3\cdot n + 2\cdot n^4} = \lim_{n\to\infty}\frac{(8\cdot\frac{1}{n^2} + 3\cdot 1)\cdot n^4}{(3\cdot\frac{1}{n^3} + 2\cdot 1)\cdot n^4} = \lim_{n\to\infty}\frac{(8\cdot\frac{1}{n^2} + 3\cdot 1)}{(3\cdot\frac{1}{n^3} + 2\cdot 1)} = \frac{0+3}{0+2} = 1.5$$

Denn es gelten: $\lim\limits_{n\to\infty} \frac{1}{n^3} = 0$ und $\lim\limits_{n\to\infty} \frac{1}{n^2} = 0$.

Ist der Grad des Zählers größer als der Grad des Nenners, so kann das Konvergenzverhalten durch Abschätzungen bestimmt werden:

Beispiel 11.2.5.

Es sei $a_n := \dfrac{8 \cdot n^2 + 3 \cdot n^5}{3 \cdot n + 2 \cdot n^4}$. Dann gilt:

$$a_n = \frac{8 \cdot n^2 + 3 \cdot n^5}{3 \cdot n + 2 \cdot n^4} = \frac{(8 \cdot \frac{1}{n^2} + 3 \cdot n) \cdot n^4}{(3 \cdot \frac{1}{n^3} + 2 \cdot 1) \cdot n^4} = \frac{(8 \cdot \frac{1}{n^2} + 3 \cdot n)}{(3 \cdot \frac{1}{n^3} + 2 \cdot 1)} \geq \frac{8 \cdot 0 + 3 \cdot n}{3 \cdot 1 + 2 \cdot 1} = \frac{3}{5} \cdot n$$

Es gilt also $\lim\limits_{n\to\infty} a_n = \infty$, denn die Folge ist monoton wachsend und unbeschränkt.

Bemerkung 11.2.6.

Rechnen mit ∞ ist nicht möglich! Das Symbol ∞ steht nicht für eine Zahl, entsprechend versagen bei ∞ die üblichen Rechengesetze. Insbesondere der Wert von "$\frac{\infty}{\infty}$" ist nicht bestimmt.

a) "$\frac{\infty}{\infty}$" ist 0? $\quad \lim\limits_{n\to\infty} \dfrac{42 \cdot n^2}{n^3} = \lim\limits_{n\to\infty} \dfrac{42}{n} = 0$

b) "$\frac{\infty}{\infty}$" ist ∞? $\quad \lim\limits_{n\to\infty} \dfrac{42 \cdot n^3}{n^2} = \lim\limits_{n\to\infty} \dfrac{42 \cdot n}{1} = \infty$

c) "$\frac{\infty}{\infty}$" ist 42? $\quad \lim\limits_{n\to\infty} \dfrac{42 \cdot n^2}{n^2} = \lim\limits_{n\to\infty} \dfrac{42 \cdot 1}{1} = 42$

11.3. Reihen

Wir wenden uns nun speziellen und sehr wichtigen Folgen zu, den Reihen, welche über ihr Bildungsgesetz charakterisiert werden.

Definition 11.3.1.

Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge. Wir definieren eine weitere Folge

$$A_n = \sum_{k=1}^{n} a_n,$$

welche wir ***Reihe*** und deren Glieder wir ***Partialsummen*** nennen. Wenn die Folge $(A_n)_{n\in\mathbb{N}}$ gegen eine Zahl

$S \in \mathbb{R}$ konvergiert, schreiben wir

$$S = \sum_{k_1}^{\infty} = \lim_{n\to\infty} A_n.$$

Man sagt dann auch, die Reihe konvergiert. Nicht konvergente Reihen heißen divergent. Man verwendet die Schreibweise $\sum_{n_1}^{\infty} a_n$ auch, um die Reihe zu bezeichnen.

Bemerkung 11.3.2.

Vereinfacht ausgedrückt, ist eine *Reihe* also eine "Summe unendlich vieler Summanden". Wenn aber unendlich viele Werte addiert werden, kann der Wert dieser Summe auch unendlich groß werden und dadurch gar nicht existieren. Bei manchen Summen ist ihr Wert, oder sogar die Existenz des Wertes, unklar:

$$\begin{aligned} &1 \quad -1 \quad +1 \quad -1 \quad +1 \quad \pm\ldots \quad = ?\\ &1 \quad +\frac{1}{2} \quad +\frac{1}{3} \quad +\frac{1}{4} \quad +\frac{1}{5} \quad +\ldots \quad = ?\\ &1 \quad +\frac{1}{2^2} \quad +\frac{1}{3^2} \quad +\frac{1}{4^2} \quad +\frac{1}{5^2} \quad +\ldots \quad = ? \end{aligned}$$

Bei solchen "unendlichen Summen" müssen wir also tatsächlich Grenzwerte betrachten, wie wir sie von Folgen bereits kennen.

Die Reihe muss nicht bei $k = 0$ oder $k = 1$ beginnen, sondern kann bei jeder *ganzen* Zahl $m \in \mathbb{Z}$ beginnen: Analog zu obiger Definition definiert man dann $\sum_{k=m}^{\infty} a_k$.

Ändert man in einer Reihe (nur) *endlich viele* Summanden, so ändert sich das *Konvergenzverhalten* (Konvergenz oder Divergenz) nicht. Natürlich kann sich hierdurch der Wert der Reihe ändern (falls die die Reihe konvergiert, d.h. falls sie "überhaupt "einen Wert hat"). Gleiches gilt für das Weglassen oder Hinzufügen von *endlich vielen* Summanden.

Beispiel 11.3.3.

▶ Es gilt

$$1 \quad = \quad \sum_{k=2}^{\infty} \frac{1}{(k-1)\cdot k} \quad = \quad \frac{1}{2}+\frac{1}{6}+\frac{1}{12}+\frac{1}{20}+\ldots$$

Diese Reihe ist also *konvergent*. Denn wegen $\frac{1}{k-1} - \frac{1}{k} = \frac{k}{(k-1)k} - \frac{k-1}{(k-1)k} = \frac{k-k+1}{(k-1)\cdot k}$ (ein Trick!) folgt für die Partialsumme bis $N \in \mathbb{N}$:

$$\begin{aligned} \sum_{k=2}^{N} \frac{1}{(k-1)k} \quad &= \quad \sum_{k=2}^{N} \left(\frac{1}{(k-1)} - \frac{1}{k} \right) \\ &= \quad \underbrace{\frac{1}{1} - \frac{1}{2} \quad +\frac{1}{2} - \frac{1}{3} \quad +\frac{1}{3} - \frac{1}{4} +\ldots+ \frac{1}{N-1} - \frac{1}{N}}_{=0} = 1 - \frac{1}{N} \end{aligned}$$

Es folgt also

$$\sum_{k=2}^{\infty} \frac{1}{(k-1)k} = \lim_{N\to\infty} \left(\sum_{k=2}^{N} \frac{1}{(k-1)k} \right) = \lim_{N\to\infty} \left(1 - \frac{1}{N} \right) = 1$$

- Die Reihe $\sum_{k=0}^{\infty} k = 0 + 1 + 2 + 3 + 4 + 5 + \ldots$ ist *divergent*, denn die Folge der Partialsummen $0, 1, 3, 6, 10, 15, \ldots$ ist divergent. Genauer gilt $\sum_{k=0}^{\infty} k = \infty$ wegen

$$\sum_{k=0}^{N} k = \frac{N(N+1)}{2} \qquad \text{und} \qquad \lim_{N\to\infty} \left(\sum_{k=0}^{N} k \right) = \lim_{N\to\infty} \frac{N(N+1)}{2} = \infty$$

Die Reihe $\sum_{k=0}^{\infty} (-1)^k = 1 - 1 + 1 - 1 \pm \ldots$ ist *divergent*, denn die Folge der Partialsummen $1, 0, 1, 0, 1, \ldots$ ist divergent, weil sie zwei Häufungspunkte hat (nämlich 1 und 0). Hier lässt sich als "Wert" für die Reihe nichts angeben, im Gegensatz zur ersten Reihe in diesem Beispiel.

11.3.1. Konvergenzkriterien für Reihen

Wir werden nun zwei Kriterien kennen lernen, um die Konvergenz von Reihen nachzuweisen.

Proposition 11.3.4.

Die Reihe $\sum_{n=1}^{\infty} a_n$ konvergiert, wenn $\sum_{n=1}^{\infty} |a_n|$ konvergiert.

Beweis. Sei $A_n = \sum_{k=1}^{n} a_k$ und $B_n = \sum_{k=1}^{n} |a_k|$. Für $N \in \mathbb{N}$ und $n > N$ gilt

$$|A_n - a_N| = |\sum_{k=N+1}^{n} a_k| \leq \sum_{k=N+1}^{n} |a_k| = |B_n - B_N|.$$

Wenn $(B_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist, trifft dies also auch auf $(A_n)_{n\in\mathbb{N}}$ zu. □

Korollar 11.3.5.

Die Reihe $\sum_{n=1}^{\infty} a_n$ konvergiert, wenn es eine reelle Zahl $0 < x < 1$ gibt, so dass $|a_n| \leq q^{n-1}$ für alle $n \in \mathbb{N}$.

Beweis. Folgt aus Proposition 11.3.4 und Lemma 11.3.11, denn $\sum_{n=1}^{\infty} |a_n|$ konvergiert, weil $\sum_{n=1}^{\infty} |a_n| \leq \sum_{n=1}^{\infty} q^{n-1}$ und $\sum_{n=1}^{\infty} q^{n-1} = \frac{1}{1-q}$. □

Lemma 11.3.6 (Majorantenkriterium)**.**

Es sei $\sum_{n=0}^{\infty} b_n = b$ eine konvergente Reihe mit Grenzwert $b \in \mathbb{R}$.

Gilt für eine Folge $(a_n)_{n\in\mathbb{N}}$ die Abschätzung $0 \leq a_n \leq b_n$ für alle $n \in \mathbb{N}$, so ist die Reihe über die a_n **konvergent** und es gilt:

$$0 \leq \sum_{n=0}^{\infty} a_n \leq \sum_{n=0}^{\infty} b_n = b$$

Beweis. Es seien $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ zwei Folgen mit $0 \leq a_n \leq b_n$ und die Reihe über die b_n sei konvergent mit Grenzwert $b = \sum_{n=0}^{\infty} b_n$. Dann gilt für die Folge der Partialsummen $S_N := \sum_{n=0}^{N} a_n$:

- Die Folge S_N ist monoton wachsend, es gilt also $S_{N+1} \geq S_N$ für alle $N \in \mathbb{N}$:

$$S_{N+1} = \sum_{n=0}^{N+1} a_n \quad = \quad \underbrace{a_{N+1}}_{\geq 0} + \underbrace{\sum_{n=0}^{N} a_n}_{=S_N} \quad \geq \quad 0 + S_N$$

- Die Folge S_N ist nach oben beschränkt, denn es gilt $S_N \leq b$ für alle $N \in \mathbb{N}$:

$$S_N = \sum_{n=0}^{N} a_n \overset{\star}{\leq} \sum_{n=0}^{N} b_n \quad \leq \quad \sum_{n=0}^{N} b_n + \underbrace{\sum_{n=N+1}^{\infty} b_n}_{\geq 0} = b$$

Die Folge $(S_N)_{N\in\mathbb{N}}$ ist also monoton wachsend und nach oben beschränkt und damit konvergent. □

Beispiel 11.3.7.

Die Reihe $\sum_{i=1}^{\infty} \frac{1}{n^2}$ ist konvergent, denn die konvergente Reihe $1 = \sum_{n=2}^{\infty} \frac{1}{(n-1)\cdot n}$ aus 11.3.3 lässt sich als Majorante nutzen.

Um dies zu erreichen müssen wir die Folge $\frac{1}{(n-1)\cdot n}$ "vorne" ergänzen, weil dieser Bruch für $n = 0$ nicht definiert ist. Wir setzen:

$$b_n := \begin{cases} 1 & \text{falls } n = 1 \\ \dfrac{1}{(n-1)\cdot n} & \text{sonst} \end{cases}$$

Für die Folge $a_n := \frac{1}{n^2}$ und b_n gilt dann $0 \leq a_n \leq b_n$ für alle $n \in \mathbb{N}$, denn

$$a_1 = 1 = b_1 \qquad \text{und} \qquad a_n = \frac{1}{n\cdot n} \leq \frac{1}{(n-1)\cdot n} = b_n \quad \text{für } n \in \mathbb{N}\setminus\{0\}$$

Es gilt also

$$0 \leq \sum_{n=1}^{\infty} a_n \leq \sum_{n=1}^{\infty} b_n = 1 + \underbrace{\sum_{n=2}^{\infty} \frac{1}{(n-1)\cdot n}}_{=1 \text{ s. Bsp. 11.3.3}} = 2$$

11.3.2. Einige wichtige Reihen

Die folgenden Reihen sind in der Mathematik und Informatik wichtig.

Definition 11.3.8.

- Die ***geometrische Reihe*** hat die Form $\sum_{k=0}^{\infty} q^k$ mit $q \in \mathbb{R}$.
- Eine Folge $(a_n)_{n\in\mathbb{N}}$ deren Folgenglieder alle der Form $a_n = a_0 + n \cdot d$ für ein $a_0 \in \mathbb{R}$ und $d \in \mathbb{R}$ sind (die konstante Differenz zweier aufeinander folgende Folgenglieder), bezeichnen wir als ***arithmetische Folge***. Die ***arithmetische Reihe*** wird über arithmetische Folgen gebildet.
- Die ***harmonische Reihe*** wird gebildet über die Folge $a_n = \frac{1}{n}$ für alle $n \in \mathbb{N}$.

Lemma 11.3.9 (geometrische Reihe)**.**

Die Partialsummen der geometrischen Reihe sind für jedes $q \in \mathbb{R}$

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

Für $-1 < q < 1$ konvergiert die geometrische Reihe, es gilt:

$$\sum_{k=0}^{\infty} q^k = \frac{1}{1-q} \quad \text{für } -1 < q < 1$$

Für $1 \leq q$ gilt $\sum_{k=0}^{\infty} q^k = \infty$ und für $q \leq -1$ ist die geometrische Reihe divergent.

Beweis. Für die Partialsumme $S_n := \sum_{k=0}^{n} q^k$ gilt:

$$\begin{array}{rcccccc} 1 \cdot \sum_{k=0}^{n} q^k & = & 1 & +q & +q^2 & +\ldots & +q^n \\ -q \cdot \sum_{k=0}^{n} q^k & = & & -q & -q^2 & +\ldots & -q^n & -q^{n+1} \\ \hline 1 \cdot \left(\sum_{k=0}^{n} q^k\right) - q \cdot \left(\sum_{k=0}^{n} q^k\right) & = & 1 & & & & & -q^{n+1} \end{array}$$

Es gilt also $(1-q) \cdot S_n = 1 - q^{n+1}$. Teilen durch $(1-q)$ auf beiden Seiten liefert:

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

Für $-1 < q < 1$ gilt $\lim_{n\to\infty} q^{n+1} = 0$ und es folgt:

$$\sum_{k=0}^{\infty} q^k = \lim_{n\to\infty} \frac{1-q^{n+1}}{1-q} = \frac{1-0}{1-q}$$

□

Lemma 11.3.10 (arithmetische Reihe)**.**

Die Partialsummen der arthmetischen Reihe sind für eine arithmetische Folge $(a_n)_{n\in\mathbb{N}}$ und $a_0 \in \mathbb{R}$

$$\sum_{k=0}^{n} a_k = (n+1)a_0 + d\frac{n(n+1)}{2}.$$

Lemma 11.3.11 (arithmetische Reihe)**.**

Die harmonische Reihe divergiert.

12 Stetigkeit

In diesem Abschnitt behandeln wir Funktionen die man, anschaulich gesprochen, “zeichnen kann, ohne den Stift abzusetzen”. Um diese Intuition mathematisch zu erfassen, beginnen wir mit der Definition eines Konvergenzbegriffs für Funktionen.

12.1. Eine Konvergenz für reelle Funktionen

Definition 12.1.1.

Sei

- $u \in \mathbb{R}$ eine reelle Zahl,
- $X \subset \mathbb{R}$ eine Teilmenge der reellen Zahlen und
- $f : X \to \mathbb{R}$ eine Funktion von X in die reellen Zahlen.

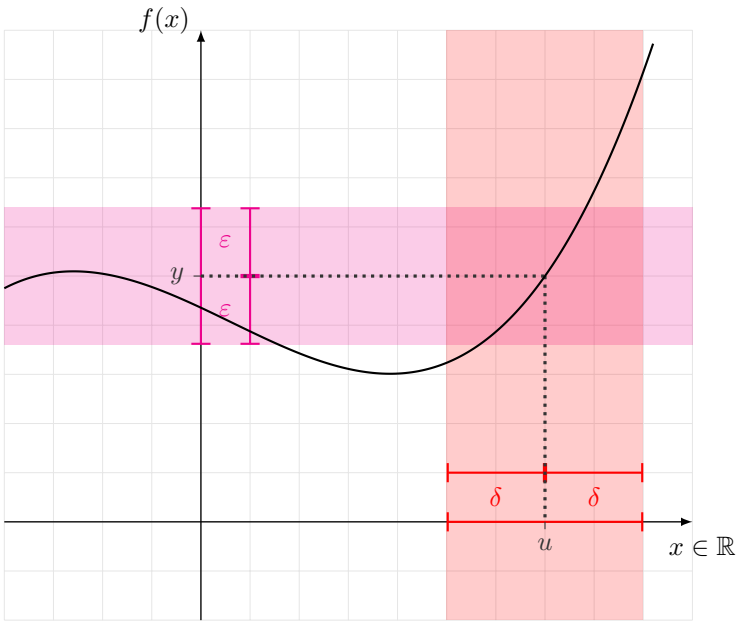
Wir sagen $f(x)$ ***konvergiert gegen*** $y \in \mathbb{R}$ ***für*** $x \to u$, falls die beiden folgenden Bedingungen erfüllt sind.

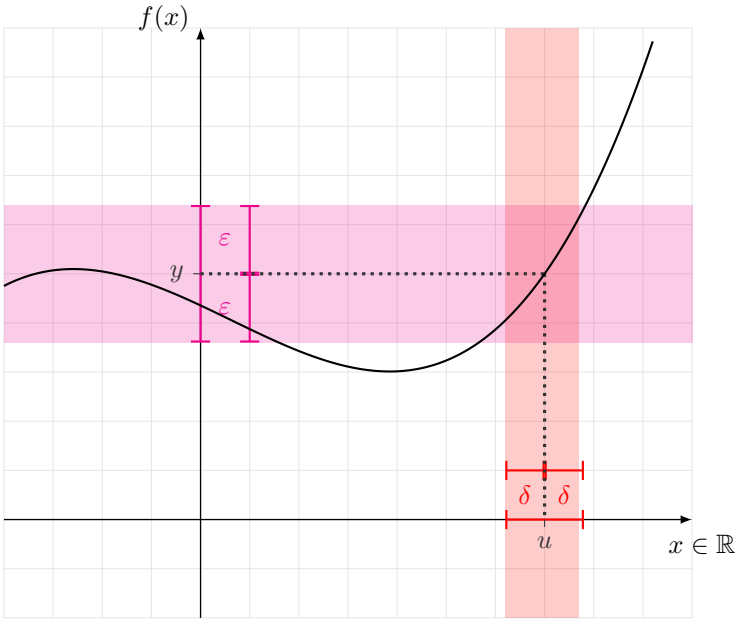
- Zu jedem $\delta > 0$ gibt es ein $x \in X$ mit $|x - u| < \delta$.
- Zu jedem $\varepsilon > 0$ gibt es ein $\delta > 0$, so dass für alle $x \in X$ mit $|x - u| < \delta$ gilt $|f(x) - y| < \varepsilon$.

Man schreibt auch kurz $\lim_{x \to u} f(x) = y$.

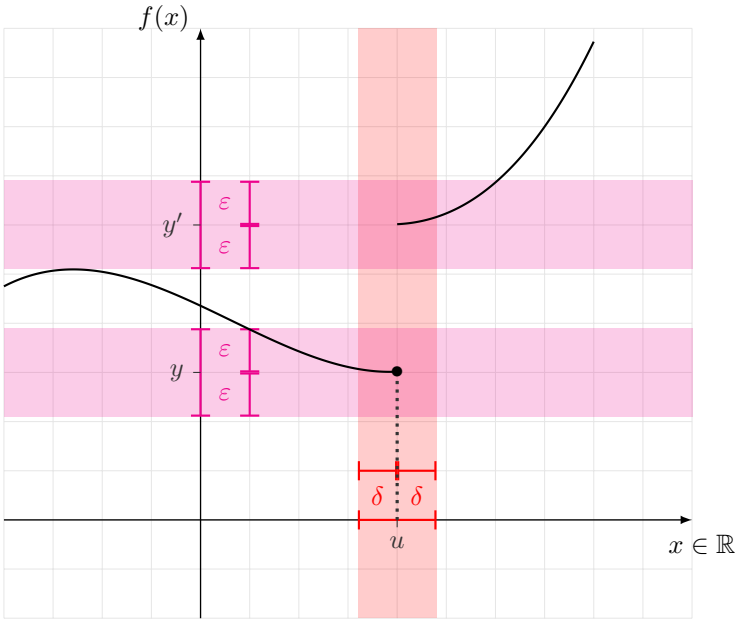
Im Folgenden Skizzen, welche die einzelnen Situationen beleuchten sollen.

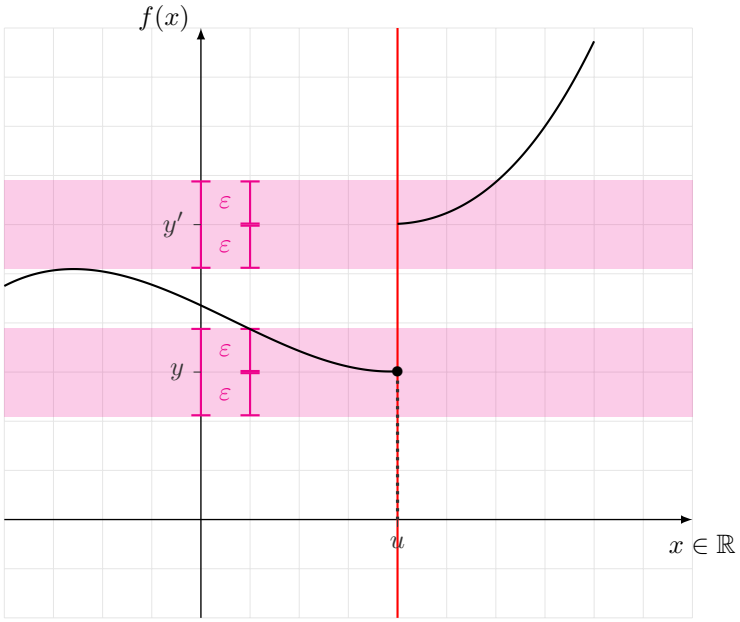
- $f(x)$ konvergiert gegen $y \in \mathbb{R}$ für $x \to u$. Für das in der ersten Abbildung gewählte ε ist das gewählte δ zu groß. In der zweiten Abbildung ist ein kleineres δ gewählt worden und die Bedingungen sind dann erfüllt.





- $f(x)$ konvergiert nicht gegen ein $y \in \mathbb{R}$ für $x \to u$. In der ersten Abbildung findet man, dass für das gewählte ε das gewählte δ ebenfalls zu groß ist. Jedoch, wie in der zweiten Abbildung angedeutet, gibt es kein $\delta > 0$, so dass die Bedingung erfüllt ist.





12.2. Verträglichkeit mit Verknüpfungen von Funktionen

Hat man zwei Funktionen in der Hand für welche die oben eingeführte Konvergenz vorliegt, stellt sich die Frage, ob die verknüpften Funktionen auch diese Eigenschaft haben. Zunächst eine Erinnerung und dann zwei Propositionen, die eine positive Antwort auf diese Frage geben.

Bemerkung 12.2.1.

Für zwei Funktionen $f, g : X \to \mathbb{R}$ ist bekanntlich $f + g : X \to \mathbb{R}$ die Funktion $x \mapsto f(x) + g(x)$. Analog ist $f \cdot g : X \to \mathbb{R}$ die Funktion $x \mapsto f(x) \cdot g(x)$.

Proposition 12.2.2.

Seien $f, g : X \to \mathbb{R}$ Funktionen und $u \in \mathbb{R}$. Wenn $\lim_{x\to u} f(x) = y$ und $lim_{x\to u} g(x) = z$, dann gilt

$$\lim_{x\to u} f(x) + g(x) = y + z \qquad \lim_{x\to u} f(x) \cdot g(x) = y \cdot z.$$

Beweis. Zu $\varepsilon > 0$ sei $\delta > 0$ so, dass $|f(x) - y| < \varepsilon$ und $|g(x) - z| < \varepsilon$, falls $|x - u| < \delta$. Dann gilt für solche x

$$|(f + g)(x) - (y + z)| \leq |f(x) - y| + |g(x) - z| < 2\varepsilon.$$

Daraus folgt die erste Behauptung.

Um die zweite Behauptung zu zeigen, bemerken wir, dass

$$\begin{aligned} |(f \cdot g)(x) - y \cdot z| &= |(f(x) - y) \cdot g(x) + y \cdot (g(x) - g(u))| \\ &\leq |g(x)| \cdot |f(x) - y| + |y| \cdot |g(x) - z|. \end{aligned} \tag{12.1}$$

Wir wählen also $\delta > 0$ klein genug, so dass für alle x mit $|x-u| < \delta$ gilt

$$|g(x)| \leq |z| + 1, \qquad |f(x) - y| < \varepsilon/(|z|+1) \qquad \text{und} \qquad |g(x) - z| < \varepsilon/(1+|y|).$$

Dann zeigt (12.1), dass $|f \cdot g(x) - y \cdot z| < 2\varepsilon$. □

Proposition 12.2.3.

Sein $f : X \to Y, h : Y \to \mathbb{R}$ Funktionen und $u \in X, v \in Y, z \in \mathbb{R}$ so, dass $\lim_{x\to u} f(x) = v$ und $\lim_{y\to v} h(y) = z$. Dann gilt $\lim_{x\to u} h \circ f(x) = z$.

Beweis. Zu jedem $\varepsilon > 0$ existiert ein $\delta > 0$, so dass für alle $y \in Y$ mit $|v-y| < \delta$ gilt $|h(y) - z| < \varepsilon$. Ferner gibt es ein $\gamma > 0$, so dass für alle $x \in X$ mit $|x-u| < \gamma$ gilt $|f(x) - v| < \delta$. Für diese x gilt also $|h(f(x)) - z| < \varepsilon$. □

12.3. Stetigkeit

Definition 12.3.1.

Sei $X \subset \mathbb{R}$, $f : X \to \mathbb{R}$ und $u \in X$. Wir nennen f ***stetig*** im Punkt u, falls

$$\lim_{x\to u} f(x) = f(u).$$

Ist ferner $S \subset X$, so heißt f stetig auf S, falls f stetig in jedem Punkt $u \in S$ ist.

Bemerkung 12.3.2.

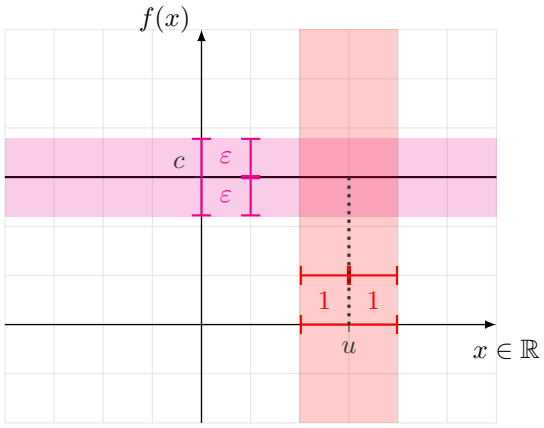
Bei dem Konzept der Stetigkeit handelt es sich zunächst einmal um eine "lokale" Eigenschaft. Die Frage, ob eine Funktion stetig ist, muss näher spezifiziert werden. Allgemein meint man damit, dass die Funktion auf ihrem ganzen Definitionsbereich stetig ist, also in jedem einzelnen Punkt. Eine Funktion kann auch auf einer Teilmenge ihres Definitionsbereiches stetig sein aber für manche Punkte im Definitionsbereich nicht stetig sein.

Beispiel 12.3.3.

- Sei $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto c$. Diese Funktion ist für alle $u \in \mathbb{R}$ stetig.
  Wähle dazu $u \in \mathbb{R}$ fest. Für jedes $\varepsilon > 0$ kann man $\delta = 1$ wählen und es ist

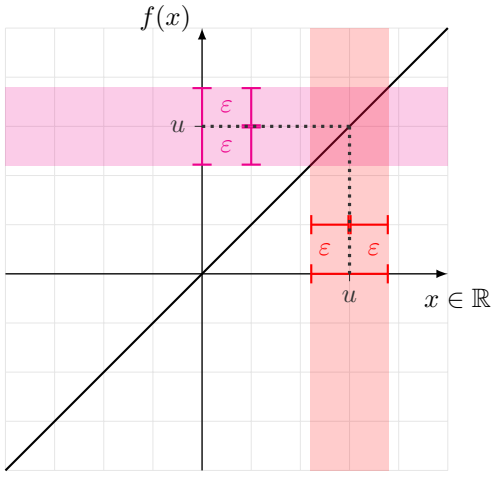
  $$|f(x) - f(u)| = |c - c| = 0 < \varepsilon \qquad \text{für alle } x \in \mathbb{R}$$

  und somit auch für alle $x \in \mathbb{R}$ mit $|x-u| < \delta = 1$.



- Sei $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto x$. Auch diese Funktion ist stetig für alle $u \in \mathbb{R}$.
  Wähle dazu $u \in \mathbb{R}$ fest. Für jedes $\varepsilon > 0$ findet man mit $\delta = \varepsilon$ ein δ, welches die notwendige Bedingung erfüllt. Denn es ist

$$|f(x) - f(u)| = |x - u| < \varepsilon \qquad \text{für alle } x \in \mathbb{R} \text{ mit } |x - u| < \delta = \varepsilon.$$



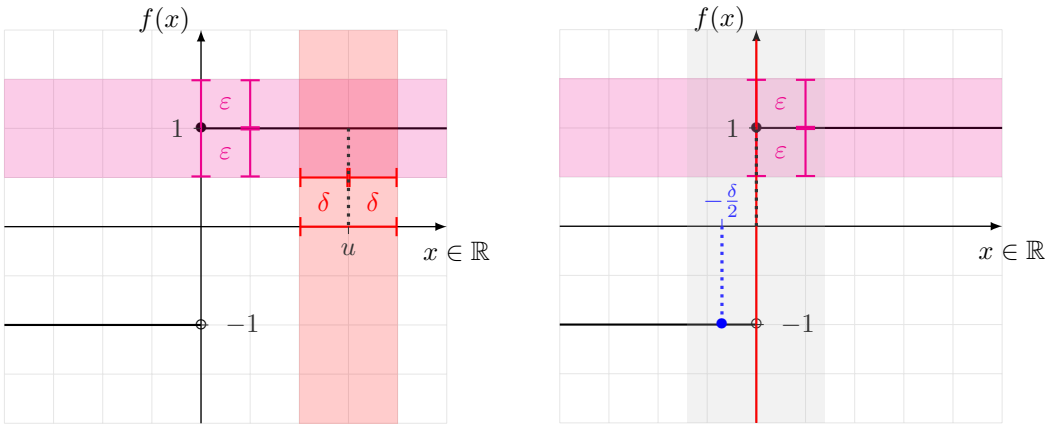
- Sei $f : \mathbb{R} \to \mathbb{R}$ mit

$$x \mapsto \begin{cases} -1 & \text{für } x < 0 \\ 1 & \text{für } x \geq 0. \end{cases}$$

  Diese Funktion ist stetig für alle $u \in \mathbb{R} \setminus \{0\}$. Für $u = 0$ ist f nicht stetig.
  Sei zunächst $u \in \mathbb{R} \setminus \{0\}$. Dann ist $|u - 0| < \delta$ für ein $\delta > 0$. Dann ist $f(u) = f(x)$ für alle $x \in \mathbb{R}$ mit $|x - u| < \delta$. Wir können also für alle $\varepsilon > 0$ dieses δ verwenden und es ist

$$|f(x) - f(u)| = 0 < \varepsilon \qquad \text{für alle } x \in \mathbb{R} \text{ mit } |x - u| < \delta.$$

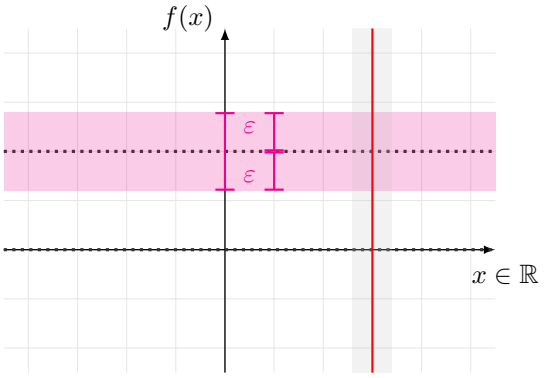
  Sei nun $u = 0$. Für $\varepsilon = \frac{1}{2}$ gibt es kein $\delta > 0$, so dass $|f(0) - f(x)| < \frac{1}{2}$ für alle $|x - 0| < \delta$. Denn man muss einfach nur $x = -\delta/2$ setzen - dann ist $f(x) = -1$ und somit $|f(0) - f(x)| = |1 - (-1)| = 2 \not< 1$.



▶ Sei $f : \mathbb{R} \to \mathbb{R}$ mit

$$x \mapsto \begin{cases} 1 & \text{für } x \in \mathbb{R} \setminus \mathbb{Q} \\ 0 & \text{für } x \in \mathbb{Q}. \end{cases}$$

Diese Funktion ist in keinem $x \in \mathbb{R}$ stetig. Um das einzusehen überlegt man sich, dass in jedem Intervall um eine reelle Zahl u rationale Zahlen enthalten sind.

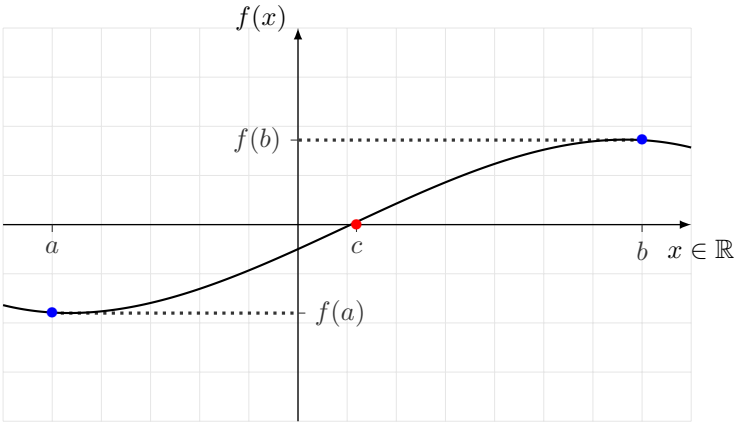


Bemerkung 12.3.4.

Mit den Aussagen in Abschnitt 12.2 (Proposition 12.2.2 und 12.2.3) und den Beispielen 12.3.3 haben wir nun schon eine breite Menge von stetigen Funktionen kennen gelernt.

12.4. Der Zwischenwertsatz

Der folgende Satz klingt zunächst mal offensichtlich, aber ihn zu beweisen braucht dennoch mehr Aufwand als erwartet. Gehen Sie auf Nummer sicher, die Aussage des Satzes wirklich zu durchdringen. In Worten sagt der Zwischenwertsatz, dass eine Funktion, welche auf einem Intervall stetig ist und der Funktionswert der unteren Intervallgrenze negativ und der rechten Intervallgrenze positiv ist in diesem Intervall den Wert 0 (mindestens einmal) annimmt.



Bemerkung 12.4.1.

Notation:

Seien $a, b \in \mathbb{R}$ reelle Zahlen. Wir bezeichnen mit

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

das ***abgeschlossene Intervall*** von a bis b, mit

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}$$

das ***offene Intervall*** von a bis b und mit

$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\} \qquad \text{bzw.} \qquad (a, b] = \{x \in \mathbb{R} : a < x \leq b\}$$

die ***halb-offene Intervall*** von a bis b.

Satz 12.4.2 ("Zwischenwertsatz")**.**

Seien $a < b$ reelle Zahlen und sei $f : [a, b] \to \mathbb{R}$ stetig auf dem gesamten Intervall $[a, b]$. Wenn $f(a) < 0$ aber $f(b) > 0$, dann existiert eine Zahl $c \in (a, b)$ mit $f(c) = 0$.

Beweis. Wir definieren eine Menge

$$Z = \{x \in [a, b] : f(x) < 0\}.$$

Diese Menge hat drei Eigenschaften:

- Z ist beschränkt (das Intervall $[a, b]$ ist beschränkt)
- Z ist nicht leer (a ist sicher in Z)
- Der Wert b ist nicht in Z enthalten

Sei $c = \sup Z$. Die Funktion f ist stetig in c. Wir wollen zeigen, dass $f(c) = 0$ ist. Dazu zeigen wir zwei Ungleichungen:

"$f(c) \leq 0$" Wir nehmen an, dass $f(c) > 0$. Dann setzen wir $\varepsilon = f(c)/2$ und wählen $\delta > 0$ so klein, dass $|f(x) - f(c)| < \varepsilon$ wenn $|x - c| < \delta$. Nach Definition des Supremums gibt es eine Zahl $x \in Z$ mit

$|x - c| < \delta$; folglich erhalten wir den Widerspruch

$$0 > f(x) \geq f(c) - \varepsilon \geq f(c) = 2 > 0.$$

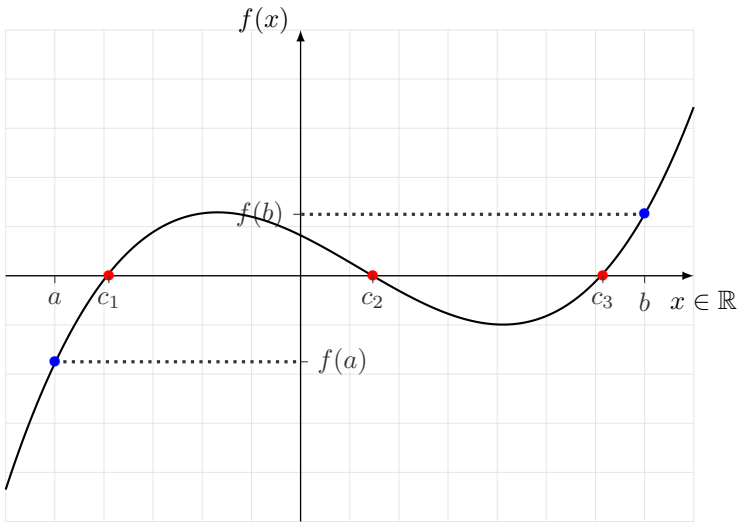
"$f(c) \leq 0$" Angenommen $f(c) < 0$. In diesem Fall setzen wir $\varepsilon = -f(c)/2 > 0$. Weil f stetig ist in c, gibt es eine Zahl $\delta > 0$, so dass $|f(c) - f(x)| < \varepsilon/2$ sofern $|x - c| < \delta$. Ferner gibt es, da $c = \sup Z < b$, eine Zahl $c < x < b$ mit $x - c| < \delta$. Weil $x \notin Z$, gilt $f(x) \geq 0$, und folglich erhalten wir den Widerspruch

$$0 \leq f(x) \leq f(c) + \varepsilon \leq f(c) = 2 < 0.$$

Die einzige verbleibende Möglichkeit ist also $f(c) = 0$. □

Bemerkung 12.4.3.

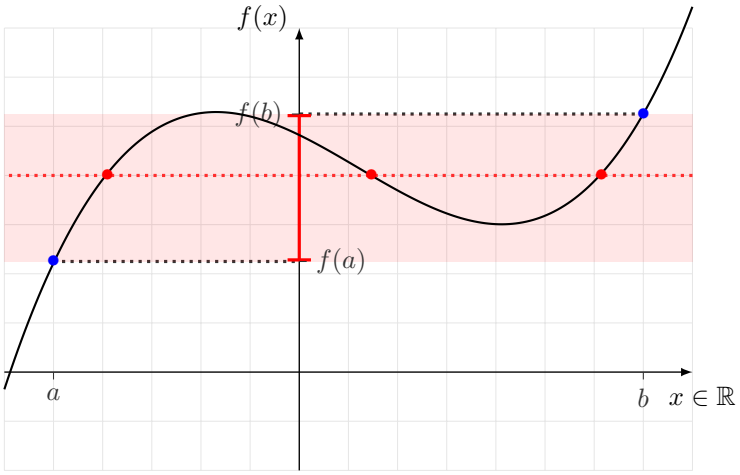
Die vom Zwischenwertsatz versprochene Nullstelle $c \in (a, b)$ ist nicht notwendigerweise eindeutig. Es gibt möglicherweise weiter Nullstellen $c_1, c_2, c_3, \ldots \in (a, b)$.



Korollar 12.4.4.

Seien $a < b$ reelle Zahlen und sei $f : [a, b] \to \mathbb{R}$ stetig auf dem gesamten Intervall $[a, b]$. Für jedes $y \in [\min\{f(a), f(b)\}, \max\{f(a), f(b)\}]$ existiert eine Zahl $c \in (a, b)$ mit $f(c) = y$.

Beweis. Man wendet den Zwischenwertsatz auf die Funktion $g(x) = f(x) - y$ bzw. $g(x) = -(f(x) - y)$ an. □


$f(x)$
$f(b)$
$f(a)$
a
b
$x \in \mathbb{R}$

13 Die Ableitung

Stetigkeit, d.h. dass eine Funktion keine “plötzlichen Sprünge” macht, ist ein einfaches aber wichtiges Konzept. Der Stetigkeitsbegriff erlaubt, aus dem Wert einer Funktion in einem Punkt u Schlüsse zu ziehen die Funkionswerte für x “in der Nähe” von u betreffend. Allerdings ist die Art von Schluss, die man ziehen kann, noch recht rudimentär. Um genauere Aussagen zu treffen, führen wir nun den Begriff der Differenzierbarkeit ein. Dieser erlaubt wesentlich genauere Aussagen über das lokale Verhalten einer Funktion: die Idee ist, eine Funktion lokal durch eine lineare Funktion zu approximieren. Der Nachteil ist, dass nicht jede stetige Funktion differenziert werden kann.

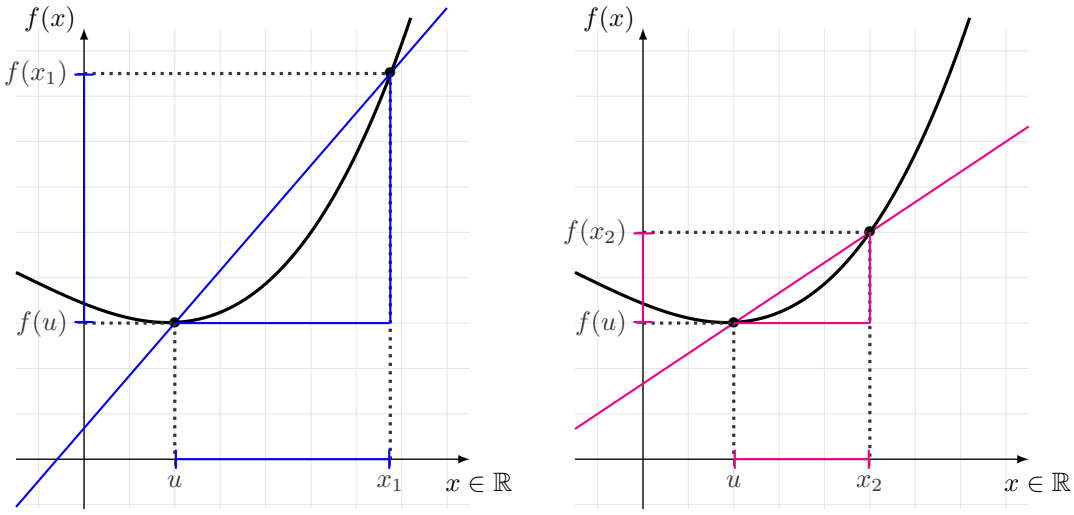
13.1. Definition

Definition 13.1.1.

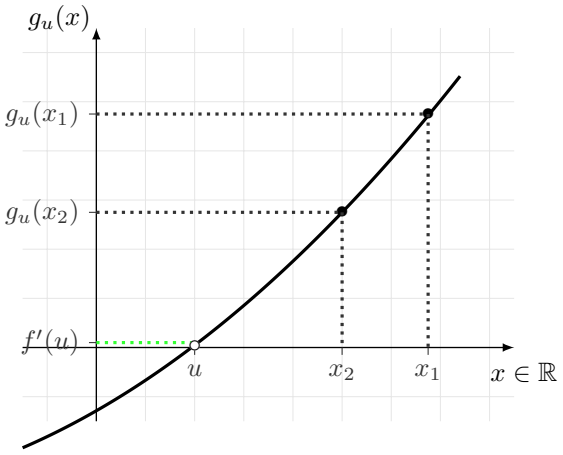
Sei $f : X \to \mathbb{R}$ eine Funktion und sei $u \in X$ ein Punkt, so dass es zu jedem $\delta > 0$ ein $x \in X \setminus \{u\}$ mit $|x - u| < \delta$ gibt. Wir sagen, dass die Funktion f differenzierbar ist im Punkt u, falls Folgendes gilt:

$$\text{Sei } g_u : X \setminus \{u\} \to \mathbb{R}, x \mapsto \frac{f(x) - f(u)}{x - u}. \text{ Dann konvergiert } g_u(x) \text{ für } x \to u.$$

In diesem Fall nennen wir $\lim_{x \to u} g_u(x)$ die ***Ableitung*** von f in u.



In der obigen Abbildung ist die Situation für festes u aber variables x skizziert, in diesem Fall für zwei verschiedene Werte x_1 und x_2. Für jedes fixe u aus dem Definitionsbereich von f erhält man eine eigene Funktion $g_u(x)$ (nicht zu verwechseln mit der Ableitung von f - es handelt sich nur um eine “Hilfsfunktion” mit welcher man die Ableitung in genau einem Punkt bestimmt.



Bemerkung 13.1.2.

Anschaulich gesprochen ist $\frac{f(x)-f(u)}{x-u}$ die Steigung der Geraden durch die Punkte $(x, f(x), (u, f(u)) \in \mathbb{R}^2$. Da wir den Limes $x \to u$ betrachten, können wir uns die Ableitung also als die Steigung der Funktion f im Punkt u vorstellen.

Notation: Für die Ableitung von f im Punkt u schreiben wir oft $f'(u)$ oder $\frac{df}{dx}(u)$. Wenn f auf der gesamten Menge X differenzierbar ist, können wir also f' (oder $\frac{df}{dx}$) als eine Abbildung $X \to \mathbb{R}$ auffassen.

Beispiel 13.1.3.

- Sei $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto c$. Diese Funktion ist für alle $u \in \mathbb{R}$ differenzierbar.
  Wähle dazu $u \in \mathbb{R}$ fest und betrachte
  $$g_u(x) = \frac{f(x) - f(u)}{x - u} = \frac{c - c}{x - u} = 0.$$
  Man prüft leicht nach, dass $g_u(x)$ gegen 0 konvergiert für $x \to u$.
  Es ist also $f'(u) = 0$ und allgemein $f'(x) = 0$ für alle $x \in \mathbb{R}$.
- Sei $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto x$. Diese Funktion ist für alle $u \in \mathbb{R}$ differenzierbar.
  Wähle dazu $u \in \mathbb{R}$ fest und betrachte
  $$g_u(x) = \frac{f(x) - f(u)}{x - u} = \frac{x - u}{x - u} = 1.$$
  Man prüft leicht nach, dass $g_u(x)$ gegen 1 konvergiert für $x \to u$.
  Es ist also $f'(u) = 1$ und allgemein $f'(x) = 1$ für alle $x \in \mathbb{R}$.

Proposition 13.1.4.

Wenn die Funktion $f : X \to \mathbb{R}$ im Punkt $u \in X$ differenzierbar ist, dann ist sie dort auch stetig.

Beweis. Sei $0 < \varepsilon < 1$. (Es reicht für kleine ε die Existenz eines $\delta > 0$ zu zeigen, für welches die Konvergenzbedingung (also Stetigkeitsbedingung) erfüllt ist. Für größere ε kann man das selbe δ wählen.)

Wähle $0 < \delta < \frac{\varepsilon}{2(1+|f'(u)|)}$ so klein, dass für alle $x \in X$ mit $|x-u| < \delta$ gilt

$$\left|g_u(x) - \lim_{x\to u} g_u(x)\right| = \left|\frac{f(x)-f(u)}{x-u} - f'(u)\right| < \varepsilon/2.$$

Das ist immer möglich, denn $f'(u)$ ist definiert, weil f in u differenzierbar ist - also die Funktion $g_u(x)$ für $x \to u$ gegen $f'(u)$ konvergiert.

Dann gilt aber auch

$$\begin{aligned}
|f(u)-f(x)| &= \left|\frac{f(x)-f(u)}{x-u}\cdot(x-u)\right| = \left|\frac{f(x)-f(u)}{x-u}\right|\cdot|(x-u)| \\
&= \left|\frac{f(x)-f(u)}{x-u} - f'(u) + f'(u)\right|\cdot|(x-u)| \\
&\leq \left(\underbrace{\left|\frac{f(x)-f(u)}{x-u} - f'(u)\right|}_{<\varepsilon/2} + |f'(u)|\right)\cdot\underbrace{|(x-u)|}_{<\delta} \\
&\leq \varepsilon\delta/2 + \delta|f'(u)|
\end{aligned}$$

Weil wir das δ geschickt gewählt haben gilt

$$|f(u)-f(x)| \leq \varepsilon^2/4 + \varepsilon/2$$

und weil $0 < \varepsilon < 1$ gilt

$$|f(u)-f(x)| \leq \varepsilon.$$

Also finden wir für jedes $\varepsilon > 0$ ein $\delta > 0$ so, dass $|f(u)-f(x)| \leq \varepsilon$ für alle $x \in \mathbb{R}$ mit $|x-u| < \delta$. Also konvergiert $f(x)$ gegen $f(u)$ für $x \to u$ und somit ist f stetig in u. □

13.2. Rechenregeln für Ableitungen

Ähnlich wie im Fall von stetigen Funktionen, kann man aus gegebenen differenzierbaren Funktionen neue basteln.

Proposition 13.2.1.

Angenommen die Funktionen $f_1, f_2 : X \to \mathbb{R}$ sind im Punkt $u \in X$ differenzierbar, dann ist die Funktion $f_1 + h : X \to \mathbb{R}, x \mapsto f_1(x) + f_2(x)$ differnzierbar in u und

$$(f_1+f_2)'(u) = f_1'(u) + f_2'(u).$$

Beweis. Es gilt nach Proposition 12.2.2, dass

$$\begin{aligned}\lim_{x\to u}\frac{(f_1+f_2)(x)-(f_1+f_2)(u)}{x-u} &= \lim_{x\to u}\frac{f_1(x)+f_2(x)-f_1(u)-f_2(u)}{x-u}\\ &= \lim_{x\to u}\frac{f_1(x)-f_1(u)+f_2(x)-f_2(u)}{x-u}\\ &= \lim_{x\to u}\left(\frac{f_1(x)-f_1(u)}{x-u}+\frac{f_2(x)-f_2(u)}{x-u}\right)\\ &= f_1'(u)+f_2'(u),\end{aligned}$$

wie behauptet. □

Beispiel 13.2.2.

Sei $f:\mathbb{R}\to\mathbb{R}$ mit $x\mapsto x+2$. Dann ist f für alle $u\in\mathbb{R}$ differenzierbar.

Es ist $f=f_1+f_2$ mit $f_1(x)=x$ und $f_2(x)=1$. Nach Beispiel 13.1.3 ist

$$f_1'(x)=1 \qquad \text{und} \qquad f_2'(x)=0.$$

Wähle nun $u\in\mathbb{R}$ fest. Dann ist nach Proposition 13.2.1

$$f'(u)=f_1'(u)+f_2'(u)=1+0=1.$$

Also gilt allgemein $f'(x)=1$.

13.2.1. Die Produktregel

Proposition 13.2.3.

Angenommen die Funktionen $f_1,f_2:X\to\mathbb{R}$ sind im Punkt $u\in X$ differenzierbar, dann ist die Funktion $f_1\cdot f_2:X\to\mathbb{R}, x\mapsto f_1(x)\cdot f_2(x)$ differnzierbar in u und

$$(f_1\cdot f_2)'(u)=f_1'(u)\cdot f_2(u)+f_1(u)\cdot f_2'(u).$$

Beweis. Es gilt

$$\begin{aligned}
\lim_{x\to u}\frac{(f_1\cdot f_2)(x)-(f_1\cdot f_2)(u)}{x-u} &= \lim_{x\to u}\frac{f_1(x)\cdot f_2(x)-f_1(u)\cdot f_2(u)}{x-u}\\
&= \lim_{x\to u}\frac{f_1(x)\cdot f_2(x)\overbrace{-f_1(u)\cdot f_2(x)+f_1(u)\cdot f_2(x)}^{=0}-f_1(u)\cdot f_2(u)}{x-u}\\
&= \lim_{x\to u}\frac{f_1(x)\cdot f_2(x)-f_1(u)\cdot f_2(x)-(f_1(u)\cdot f_2(u)-f_1(u)\cdot f_2(x))}{x-u}\\
&= \lim_{x\to u}\left(f_2(x)\frac{f_1(x)-f_1(u)}{x-u}-f_1(u)\frac{f_2(u)-f_2(x)}{x-u}\right)\\
&= \lim_{x\to u}\left(f_2(x)\frac{f_1(x)-f_1(u)}{x-u}+f_1(u)\frac{f_2(x)-f_2(u)}{x-u}\right).
\end{aligned}$$

Nach Proposition 13.1.4 ist $\lim_{x\to u} f_2(x) = f_2(u)$. Mit Proposition 12.2.2 ist also

$$\begin{aligned}
\lim_{x\to u}\frac{(f_1\cdot f_2)(x)-(f_1\cdot f_2)(u)}{x-u} &= \lim_{x\to u} f_2(x)\cdot\lim_{x\to u}\frac{f_1(x)-f_1(u)}{x-u}+f_1(u)\lim_{x\to u}\frac{f_2(x)-f_2(u)}{x-u}\\
&= f_1'(u)\cdot f_2(u)+f_1(u)\cdot f_2'(u),
\end{aligned}$$

wie behauptet. □

Beispiel 13.2.4.

- Sei $f:\mathbb{R}\to\mathbb{R}$ mit $x\mapsto x^2$. Dann ist f für alle $u\in\mathbb{R}$ differenzierbar.
  Es ist $f=f_1+f_2$ mit $f_1(x)=x$ und $f_2(x)=x$. Nach Beispielen 13.1.3 und 13.2.4 ist

  $$f_1'(x)=1 \qquad \text{und} \qquad f_2'(x)=1.$$

  Wähle nun $u\in\mathbb{R}$ fest. Dann ist nach Proposition 13.2.3

  $$f'(u)=f_1'(u)f_2(u)+f_1(u)f_2'(u)=1+0=u+u=2u.$$

  Also gilt allgemein $f'(x)=2x$.
- Sei $f:\mathbb{R}\to\mathbb{R}$ mit $x\mapsto x^3$. Dann ist f für alle $u\in\mathbb{R}$ differenzierbar.
  Es ist $f=f_1+f_2$ mit $f_1(x)=x^2$ und $f_2(x)=x$. Nach Beispiel 13.1.3 ist

  $$f_1'(x)=2x \qquad \text{und} \qquad f_2'(x)=1.$$

  Wähle nun $u\in\mathbb{R}$ fest. Dann ist nach Proposition 13.2.3

  $$f'(u)=f_1'(u)f_2(u)+f_1(u)f_2'(u)=2u\cdot u+u^2\cdot 1=3u^2.$$

  Also gilt allgemein $f'(x)=3x$.
- Allgemein lässt sich so induktiv herleiten, dass $f:\mathbb{R}\to\mathbb{R}$ mit $x\mapsto x^n$ für alle $u\in\mathbb{R}$ differenzierbar ist mit $f'(x)=nx^{n-1}$.
- Sei $f_1:\mathbb{R}\to\mathbb{R}$ eine beliebige differenzierbare Funktion und $f_2:\mathbb{R}\to\mathbb{R}$ mit $x\mapsto c$. Dann ist

$f = f_1 \cdot f_2 = c \cdot f_1$ für alle $u \in \mathbb{R}$ differenzierbar. Es gilt

$$f_2'(x) = 0$$

und somit ist

$$f'(x) = f_1'(x) \cdot f_2(x) + f_1(x) f_2'(x) = c \cdot f_1'(x).$$

13.2.2. Die Kettenregel

Proposition 13.2.5.

Angenommen die Funktion $f_1 : X \to Y$ ist im Punkt $u \in X$ differenzierbar und die Funktion $f_2 : Y \to \mathbb{R}$ ist differenzierbar im Punkt $v = f_1(u)$. Dann ist die Funktion $f_2 \circ f_1 : X \to \mathbb{R}, x \mapsto f_2(f_1(x))$ differnzierbar in u und

$$(f_2 \circ f_1)'(u) = f_2'(f_1(u)) \cdot f_1'(u).$$

Beweis. Wir führen die Kurzschreibweise $t = f_1(x) -_1 (u)$ ein. Es gilt

$$\frac{f_2 \circ f_2(x) - f_2 \circ f_1(u)}{x - u} = \frac{h(v+t) - h(v)}{x - u} \tag{13.1}$$

$$= \frac{h(v) + th'(v)) - h(v)}{x - u} + \frac{h(v+t) - h(v) - th'(v)}{x - u} \tag{13.2}$$

$$= \frac{th'(v)}{x - v} + \frac{h(v+t) - h(v) - th(v)}{x - u}. \tag{13.3}$$

Wir erhalten

$$\lim_{x \to u} \frac{th'(v)}{x - u} = \lim_{x \to u} \frac{h'(v)(f(x) - f(u))}{x - u} = h'(v) f'(u). \tag{13.4}$$

Ferner gilt, sofern $t \neq 0$,

$$\lim_{x \to u} \frac{h(v+t) - h(v) - th'(v)}{x - u} = \lim_{x \to u} \frac{t}{x - u} \left(\frac{h(v+t) - h(v)}{t} - h'(v) \right). \tag{13.5}$$

Nach Definitino der ableitung $h'(v)$ bzw. $f'(v)$ gilt

$$\lim_{s \to 0} \frac{h(v+s) - h(v)}{s} - h'(v) = 0, \qquad \lim_{x \to u} \frac{t}{x - u} = f'(u).$$

Also zeigt (13.5), dass

$$\lim_{x \to u} \frac{h(v+t) - h(v) - th'(v)}{x - u} = 0. \tag{13.6}$$

Schließlich folgt die Behauptung, indem man (13.4) und (13.6) in (13.1) einsetzt. □

Beispiel 13.2.6.

Sei $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto (x-1)^2$. Dann ist f für alle $u \in \mathbb{R}$ differenzierbar.

Es ist $f = f_2 \circ f_1$ mit $f_1(x) = x^3 - 1$ und $f_2(x) = x^2$. Es ist

$$f_1'(x) = 3x^2 \qquad \text{und} \qquad f_2'(x) = 2x.$$

Wähle nun $u \in \mathbb{R}$ fest. Dann ist nach Proposition 13.2.5

$$f'(u) = f_2'(f_1(u))f_1'(u) = 2(u^3-1) \cdot 3u^2 = 6(u^3-1)u^2$$

Also gilt allgemein $f'(x) = 6(x^3-1)x^2$.

13.2.3. Die Quotientenregel

Lemma 13.2.7.

Die Funktion $f : \mathbb{R} \setminus \{0\}$ mit $x \mapsto \frac{1}{x}$ ist differenzierbar. Es gilt

$$f'(x) = \frac{1}{x^2}.$$

Beweis. Wir zeigen zunächst, dass die Funktion f stetig in $u \in \mathbb{R} \setminus \{0\}$ ist. Denn

$$f(x) - f(u) = \frac{1}{x} - \frac{1}{u} = \frac{u-x}{xu}. \tag{13.7}$$

Wenn $|u-x|$ hinreichend klein ist, gilt $|x| \geq \frac{1}{2}|u|$. Dann zeigt (13.7)

$$|f(x) - f(u)| \leq \frac{|u-x|}{|ux|} \leq \frac{2|u-x|}{|u|^2}.$$

Folglich gilt

$$\lim_{x \to u} |f(x) - f(u)| = 0, \tag{13.8}$$

also ist f stetig im Punkt u.

Ferner folgt aus (13.7), dass

$$\frac{f(x) - f(u)}{x-u} = -\frac{1}{ux}. \tag{13.9}$$

Aus (13.8) und (13.9) ergibt sich schließlich

$$\lim_{x \to u} \frac{f(x) - f(u)}{x-u} = \lim_{x \to u} \frac{-1}{ux} = -\frac{1}{x^2}$$

wie behauptet. □

Mit Hilfe von Lemma 13.2.7 kann man die Quotientenregel beweisen.

Proposition 13.2.8.

Angenommen die Funktionen $f_1, f_2 : X \to \mathbb{R}$ sind im Punkt $u \in X$ differenzierbar. Wenn $f_2(x) \neq 0$ für alle $x \in X$, dann ist die Funktion $\frac{f_1}{f_2} : X \to \mathbb{R}, x \mapsto \frac{f_1(x)}{f_2(x)}$ differnzierbar in u und

$$\left(\frac{f_1}{f_2}\right)'(u) = \frac{f_1'(u) \cdot f_2(u) - f_1(u) \cdot f_2'(u)}{f_2(u)^2}.$$

Beweis. Proposition 13.2.3 zeigt, dass

$$\left(\frac{f_1}{f_2}\right)'(u) = \left(f_1 \cdot \frac{1}{f_2}\right)'(u) = f_1'(u) \cdot \frac{1}{f_2(u)} + f_1(u) \cdot \left(\frac{1}{f_2}\right)'(u). \tag{13.10}$$

Sei $h : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ mit $x \mapsto \frac{1}{x}$. Aus Proposition 13.2.5 folgt

$$\left(\frac{1}{f_2}\right)'(u) = (h \circ f_2)'(u) = f_2'(u) \cdot h'(f_2(u)) = f_2'(u) \cdot \left(-\frac{1}{f_2(u)^2}\right) = -\frac{f_2'(u)}{f_2(u)^2}. \tag{13.11}$$

Aus (13.10) und (13.10) folgt schließlich die Behauptung. □

Beispiel 13.2.9.

Sei $f : \mathbb{R} \setminus \{0, -3\} \to \mathbb{R}$ mit $x \mapsto \frac{(x-1)^2}{x^2+3x}$. Dann ist f für alle $u \in \mathbb{R} \setminus \{0, -3\}$ differenzierbar.

Es ist $f = \frac{f_1}{f_2}$ mit $f_1(x) = (x-1)^2$ und $f_2(x) = x^2 + 3x$. Es ist

$$f_1'(x) = 2(x-1) \qquad \text{und} \qquad f_2'(x) = 2x + 3.$$

Wähle nun $u \in \mathbb{R} \setminus \{0, -3\}$ fest. Dann ist nach Proposition 13.2.5

$$f'(u) = \frac{f_1'(u) \cdot f_2(u) - f_1(u) \cdot f_2'(u)}{f_2(u)^2} = \frac{2(u-1)(u^2+3u) - (u-1)^2(2u+3)}{(u^2+3u)^2}$$

Also gilt allgemein $f'(x) = 6(x^3 - 1)x^2$.

13.2.4. Satz über die Umkehrfunktion

Der Beweis des folgenden Satzes benötigt einige Überlegungen, die den Rahmen dieser Vorlesung sprengen. Er ist allerdings sehr nützlich, weshalb wir ihn zumindest formulieren.

Satz 13.2.10.

Sei $f : (a, b) \to (c, d)$ eine stetige bijektive Funktion, die im Punkt $u \in (a, b)$ differenzierbarist.

Dann ist die Umkehrabbildung $f^{-1} : (c, d) \to (a, b)$ im Punkt $v = f(u)$ differenzierbar mit Ableitung

$$\frac{1}{f'(u)}.$$

Beispiel 13.2.11.

Sei $f : (1,2) \to (1,4)$ mit $x \mapsto x^2$. Die Funktion f ist für alle $u \in (1,2)$ differenzierbar und bijektiv. Es ist $f^{-1} : (1,4) \to (1,2)$ mit $x \mapsto \sqrt{x}$. Es ist $f'(x) = 2x$. Also ist $\left(f^{-1}\right)'(x) = \frac{1}{2x}$ für $x \in (1,4)$.

13.3. Der Mittelwertsatz (der Differentialrechnung)

Was sagt die Ableitung über das lokale Verhalten der Funktion aus? Wir beginnen mit der folgenden Beobachtung.

Lemma 13.3.1.

Sei $f : [a,b] \to \mathbb{R}$ eine stetige Funktion. Dann ist $f([a,b]) = \{f(x) : x \in [a,b]\}$ beschränkt.

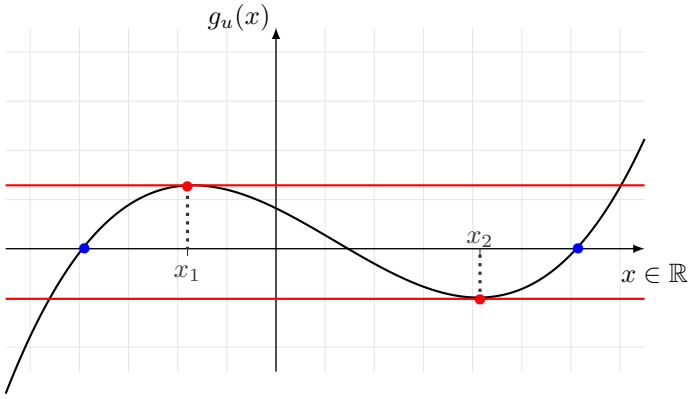
Beweis. Wir zeigen, dass $f([a,b])$ nach oben beschränkt ist, die Beschränktheit nach unten folgt analog.

Wir nehmen an, dass $f([a,b])$ nicht nach oben beschränkt ist.
Dann gibt es eine Folge

$$(x_n)_{n\in\mathbb{N}} \text{ mit } x_n \in [a,b] \text{ und } f(x_n) > n \text{ für alle } n \in \mathbb{N}.$$

Diese Folge $(x_n)_{n\in\mathbb{N}}$ ist beschränkt (es ist ja $x_n \in [a,b]$ für alle $n \in \mathbb{N}$. Demnach gibt es nach Satz **??** eine konvergente Teilfolge $(x_{m_n})_{n\in\mathbb{N}}$, welche gegen einen Wert $x^* \in [a,b]$ konvergiert.
Weil f stetig ist, folgt $f(x^*) > n$ für alle $n \in \mathbb{N}$. Denn setzen wir $\varepsilon = 1$ gibt es ein $\delta > 0$, so dass für alle $|x - x^*| < \delta$ gilt $|f(x) - f(x^*)| \leq 1$. Allerdings gibt es ein $N \in \mathbb{N}$, so dass für alle $n \geq N$ gilt, dass $|x_n - x^*| < \delta$. Also ist $f(x^*) \geq f(n) - 1$ für alle $n \in \mathbb{N}$, ein Widerspruch.

Also ist $f([a,b])$ nach oben beschränkt. □



Satz 13.3.2 ("Der Satz von Rolle")**.**

Sei $f : [a,b] \to \mathbb{R}$ eine differenzierbare Funktion mit $f(a) = f(b) = 0$. Dann gibt es ein $c \in (a,b)$ mit $f'(c) = 0$.

Beweis. Wir unterscheiden zwei Fälle.

Fall 1: Es gibt ein $d \in (a,b)$ mit $f(d) > 0$. Nach Lemma 13.3.1 ist $f([a,b]) = \{f(x) : x \in [a,b]\}$ nach oben beschränkt.

Nach Fakt 11.1.8 existiert also $s = \sup f([a,b])$.
Nach der Definition des Supremums gibt es zu jedem $n \in \mathbb{N}$ eine Zahl $y_n \in [a,b]$, so dass $|s - f(y_n)| < \frac{1}{n}$. Diese Folge $(y_n)_{n\in\mathbb{N}}$ ist beschränkt und hat nach Satz **??** eine konvergente Teilfolge, die gegen eine Zahl $c \in [a,b]$ konvergiert. Es gilt also $f(c) = s$. Weil $s > 0$ ist $c \neq a$ und $c \neq b$ also $c \in (a,b)$.
Wir zeigen nun, dass $f'(c) = 0$. Wieder unterscheiden wir zwei Fälle.

Fall 1.1: Es ist $f'(c) > 0$**.** Dann gäbe es eine kleines $\delta > 0$ so, dass mit $\varepsilon = f'(c)/2$ gilt

$$\frac{f(c+\delta) - f(c)}{\delta} \geq f'(c) - \varepsilon > 0.$$

Daraus folgt aber, dass $f(c+\delta) > f(c) = s$ ist, ein Widerspruch zu der Tatsache, dass $s = \sup f([a,b])$. Also folgt $f'(c) \leq 0$.

Fall 1.2: Es ist $f'(c) < 0$**.** Dann gäbe es entsprechend ein kleines $\delta > 0$ so, dass mit $\varepsilon = -f'(c)/2$ gilt

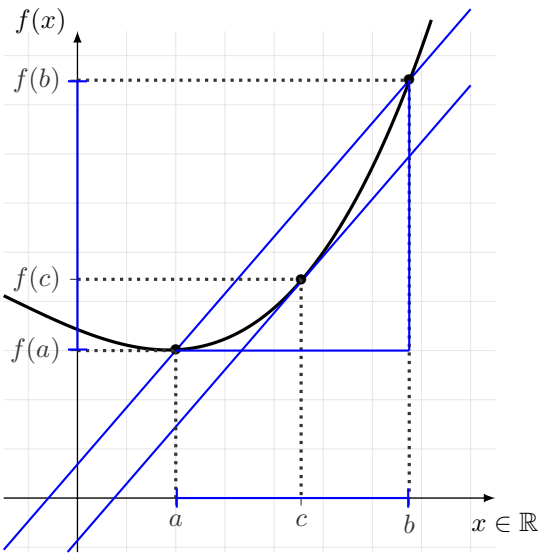
$$\frac{f(c-\delta) - f(c)}{-\delta} \geq -f'(c) - \varepsilon > 0.$$

Daraus folgt aber, dass $f(c-\delta) > f(c) = s$ ist, was wiederum ein Widerspruch zu der Tatsache, dass $s = \sup f([a,b])$ ergibt. Also folgt $f'(c) \geq 0$.

Es bleibt also nur die Möglichkeit, dass $f'(c) = 0$ ist.

Fall 2: Für alle $d \in (a,b)$ **ist** $f(d) \leq 0$**.** In diesem Fall wenden wir das Argument aus Fall 1 auf die Funktion $-f$ an und erhalten ein c mit $-f'(c) = 0$, also auch $f'(c) = 0$. Und ist $f(x) = 0$ für alle $x \in (a,b)$, dann folgt unmittelbar, dass $f'(x) = 0$ für alle $x \in (a,b)$.

□



Korollar 13.3.3 ("Mittelwertsatz der Differentialrechnung")**.**

Sei $f : [a,b] \to \mathbb{R}$ differenzierbar. Es gibt ein $c \in [a,b]$, so dass

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Beweis. Die Funktion

$$h : [a, b] \to \mathbb{R}, \qquad x \mapsto f(x) - f(a) - \frac{f(b) - f(a)}{b - a} \cdot (x - a)$$

erfüllt die Voraussetzungen des Satzes von Rolle. Denn

- es ist $h(a) = f(a) - f(a) - \frac{f(b)-f(a)}{b-a}(a - a) = 0$,
- es ist $h(b) = f(b) - f(a) - \frac{f(b)-f(a)}{b-a}(b - a) = 0$,
- h ist auf $[a, b]$ nach Proposition 13.2.1 differenzierbar, weil $f(x)$ und $(x - a)$ differenzierbar sind.

Folglich existiert ein $c \in [a, b]$ mit

$$0 = h'(c) = f'(c) - \frac{f(b) - f(a)}{b - a}.$$

Umstellen dieser Gleichung liefert die Behauptung. □

13.4. Extremstellen

Wir würden gerne Aussagen über die lokale Entwicklung einer Funktion treffen und dazu die Ableitung als Werkzeug verwenden. Beispielsweise den Zusammenhang von Steigung/Wachstum einer Funktion und dem Vorzeichen der Ableitung an dieser Stelle herstellen oder lokale Extremwerte mit Nullstellen der Ableitung charakterisieren. Im Kontext von Kurvendiskussionen wird dies in der Schule diskutiert.

Dazu benötigen wir zunächst folgende Begriffe, die den analogen Begrifflichkeiten im Kontext von Folgen sehr ähnlich sind.

Definition 13.4.1 ("Monotonie für Funktionen")**.**

Wir nennen eine Funktion

- ***monoton wachsend***, falls für je zwei reelle Zahlen $x, y \in \mathbb{R}$ mit $a \leq x < y \leq b$ gilt
$$f(x) \leq f(y).$$
- ***streng monoton wachsend***, falls für je zwei reelle Zahlen $x, y \in \mathbb{R}$ mit $a \leq x < y \leq b$ gilt
$$f(x) < f(y).$$
- ***monoton fallend***, falls für je zwei reelle Zahlen $x, y \in \mathbb{R}$ mit $a \leq x < y \leq b$ gilt
$$f(x) \geq f(y).$$
- ***streng monoton fallend***, falls für je zwei reelle Zahlen $x, y \in \mathbb{R}$ mit $a \leq x < y \leq b$ gilt
$$f(x) > f(y).$$

Beispiel 13.4.2.

- Sei $f : [0, 100] \to \mathbb{R}$ mit $x \mapsto x^2$. Dann ist f streng monoton wachsend.
  Denn für zwei reelle Zahlen $x, y \in \mathbb{R}$ mit $0 \leq x < y \leq 100$ gilt

$$f(x) = x^2 > y^2 = f(y),$$

  denn $y = x + \delta$ für ein $\delta > 0$ und somit ist

$$y^2 = (x + \delta)^2 = x^2 + 2\delta x + \delta^2 > x^2.$$

- Sei $f : [0, 100] \to \mathbb{R}$ mit $x \mapsto c$ für ein $c \in \mathbb{R}$. Dann ist f monoton wachsend und monoton fallend (aber nicht streng monoton wachsend/fallend).
  Denn für zwei reelle Zahlen $x, y \in \mathbb{R}$ mit $0 \leq x < y \leq 100$ gilt

$$f(x) = c \leq c = f(y) \qquad \text{und} \qquad f(x) = c \geq c = f(y).$$

- Sei $f : [0, 100] \to \mathbb{R}$ mit $x \mapsto x^2 - 2x$. Dann ist f weder monoton wachsend noch monoton fallend (insbesondere nicht streng monoton wachsend/fallend).
  Denn für $x = 0$ und $y = 1$ und $z = 2$ gilt

$$f(x) = f(0) = 0 > -1 = f(1) = f(y) \qquad \text{und} \qquad f(y) = f(1) = -1 < 0 = f(2) = f(z).$$

  Anmerkung: Die Funktion $f : [1, 100] \to \mathbb{R}$ mit $x \mapsto x^2 - 2x$ wiederum ist streng monoton wachsend.

Mit Hilfe des Mittelwertsatzes kann stellt man einen Zusammenhang zwischen Monotonie und dem Vorzeichen der Ableitung her.

Korollar 13.4.3.

Sei $f : [a, b] \to \mathbb{R}$ differenzierbar.

- Wenn $f'(c) \leq 0$ für alle $c \in [a, b]$ dann ist f monoton wachsend.
- Wenn $f'(c) < 0$ für alle $c \in [a, b]$ dann ist f streng monoton wachsend.
- Wenn $f'(c) \geq 0$ für alle $c \in [a, b]$ dann ist f monoton fallend.
- Wenn $f'(c) > 0$ für alle $c \in [a, b]$ dann ist f streng monoton fallend.

Beweis. Wir beweisen nur die erste Aussage, die anderen Aussagen werden analog bewiesen. Dazu verwenden wir das Beweisprinzip der Kontraposition. Wir möchten zeigen:

$$f'(c) \geq 0 \; \forall \, c \in [a, b] \qquad \Longrightarrow \qquad f \text{ ist monoton wachsend}$$

Wir zeigen jedoch gleichbedeutend

$$\neg \; (f \text{ ist monoton wachsend}) \qquad \Longrightarrow \qquad \neg \; (f'(c) \geq 0 \; \forall \, c \in [a, b])$$

also

$$f \text{ ist nicht monoton wachsend} \qquad \Longrightarrow \qquad \exists \, c \in [a, b] : f'(c) < 0 \, .$$

Wenn f nicht monoton wachsend ist, gibt es also $x, y \in [a, b]$ mit $a \leq x < y \leq b$ mit $f(x) > f(y)$. Da f auf $[a, b]$ differenzierbar ist, ist f insbesondere auf $[x, y]$ differenzierbar und es gibt nach dem Mittelwertsatz

(Korollar 13.3.3) ein $c \in [x, y]$ mit

$$f'(c) = \frac{f(y) - f(x)}{y - x} < 0$$

(da $y - x > 0$, weil $x < y$ und $f(y) - f(x) < 0$, weil $f(x) > f(y)$), was zu zeigen war. □

Wir definieren nun, was wir unter lokaler Extremität einer Funktion verstehen.

Definition 13.4.4 ("Lokales Extremum")**.**

Sei $f : [a, b] \to \mathbb{R}$ eine Funktion.

- Ein Punkt $c \in [a, b]$ heißt ***lokales Maximum*** von f, wenn es ein $\varepsilon > 0$ gibt, so dass für alle $x \in [a, b]$ mit $|x - c| < \varepsilon$ gilt $f(x) \leq f(c)$.
- Ein Punkt $c \in [a, b]$ heißt ***lokales Minimum*** von f, wenn es ein $\varepsilon > 0$ gibt, so dass für alle $x \in [a, b]$ mit $|x - c| < \varepsilon$ gilt $f(x) \geq f(c)$.

Wenn c ein lokales Minimum oder Maximum ist, nennt man c ein ***lokales Extremum***.

Liegt ein lokales Extremum vor, dann ist die Ableitung an dieser Stelle sicher gleich 0. Die Umkehrung gilt nicht allgemein. (Dass die Ableitung an einer Stelle 0 ist, ist nur eine notwendige Bedingung für das vorhanden sein eines lokalen Extremums, jedoch nicht hinreichend).

Korollar 13.4.5.

Sei $f : [a, b] \to \mathbb{R}$ differenzierbar. Wenn $c \in [a, b]$ ein lokales Extremum ist, gilt $f'(c) = 0$.

Beweis. Wir nehmen an, dass c ein lokales Maximum ist. Dann gibt es ein $\varepsilon > 0$, so dass für alle $x \in [a, b]$ mit $|x - c| < \varepsilon$ gilt $f(x) \leq f(c)$.

Wir unterscheiden nun zwei Fälle. Es gibt ein $\varepsilon \geq \delta > 0$, so dass für alle $x \in [a, b]$ mit $0 \leq c - x < \delta$ gilt f ist streng monoton wachsend.

□

13.5. Ausblick: Differentialrechnung im $\mathbb{R}^n$

Bisher haben wir uns mit Funktionen $f : X \to \mathbb{R}$ von einer Teilmenge $X \subset \mathbb{R}$ in die reellen Zahlen befasst. Häufig treten aber auch Funktionen $f : X \to \mathbb{R}^m$ von einer Teilmenge $X \subset \mathbb{R}^n$ in den $\mathbb{R}^m$ auf.

Wie können wir die Ableitung für solche Funktionen einführen? Zunächst beobachten wir, dass die Funktion $f : X \to \mathbb{R}^m$ in einzelne Funktion $f_i : X \to \mathbb{R}$, $i = 1, \ldots, m$, zerlegt werden kann. Denn f bildet jeden Punkt $x \in X$ auf einen m-dimensionalen Vektor

$$\begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}$$

ab.

Sei nun $x \in X$. Zu jeder Zahl $j = 1, \ldots, n$ betrachten wir die Menge $X_{j,x}$ aller $u \in \mathbb{R}$, so dass

$$x_{j,u} = \begin{pmatrix} x_1 \\ \vdots \\ x_{j-1} \\ u \\ x_{j+1} \\ \vdots \\ x_n \end{pmatrix} \in X.$$

[Innerhalb dieser Mengen kann man die j-te Koordinate des Vektors x durch u ersetzten, ohne die Menge X zu verlassen.] Dann erhalten wir zu jedem $i \in \{1, \ldots, m\}, x \in X$ und $j \in \{1, \ldots, n\}$ eine Funktion

$$f_{i,j,x} : X_{j,x} \to \mathbb{R}, \qquad u \mapsto f_i(x_{j,i}).$$

Falls diese Funktion differenzierbar ist im Punkt x_j, nennen wir ihre Ableitung die ***partielle Ableitung von*** f_i ***nach*** x_j ***im Punkt*** x, geschrieben als

$$\frac{\partial f_i}{\partial x_j}(x) = f'_{i,j,x}(x_j).$$

Die partielle Ableitung erhält man also, indem man f_i nach der j-ten Variable x_j differenziert und die anderen Variablen $x_h, h \neq j$, als Konstanten betrachtet. Sofern alle Ableitungen existieren, nennt man die $m \times n$-Matrix

$$Df(x) = \left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i=1,\ldots,m;j=1,\ldots,n}$$

die ***Jacobimatrix*** von f im Punkt x.

Wir haben gelernt, uns die Ableitung einer Funktion als Approximation der Funktion durch eine lineare Abbildung vorzustellen. Das Konzept der Jacobimatrix passt sehr gut in diese Vorstellung, weil eine Matrix ja nichts andere als eine lineare Abbildung ist. Die Abbildung, $Df : x \mapsto Df(x)$, die einem Punkt x die Jacobimatrix von f im Punkt x zuordnet (sofern diese existiert), nennen wir die ***Ableitung*** von f.

Beispiel 13.5.1.

▶ Die Funktion $f : \mathbb{R}^2 \to \mathbb{R}$ sei definiert durch

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = x_1^3 \cdot x_2^2 + 3 \cdot x_1 \cdot x_2.$$

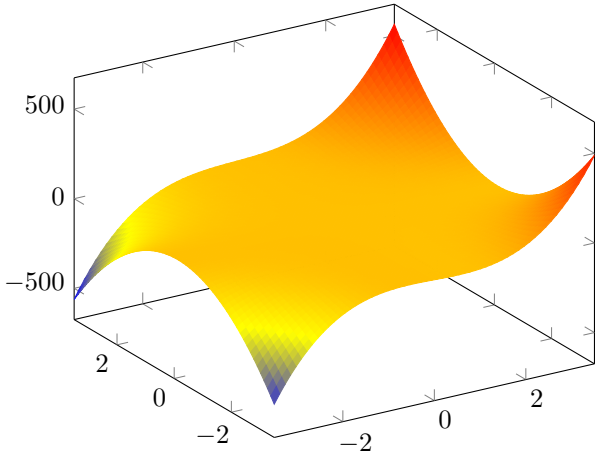
Ihre partiellen Ableitungen sind

$$\frac{\partial f}{\partial x_1}(x_1, x_2) = 3 \cdot x_1^2 \cdot x_2^2 + 3 \cdot x_2$$

$$\frac{\partial f}{\partial x_2}(x_1, x_2) = 2 \cdot x_1^3 \cdot x_2 + 3 \cdot x_1$$

Die Jacobimatrix ist also die 1×2-Matrix

$$Df(x) = (3 \cdot x_1^2 \cdot x_2^2 + 3 \cdot x_2 \quad 2 \cdot x_1^3 \cdot x_2 + 3 \cdot x_1).$$



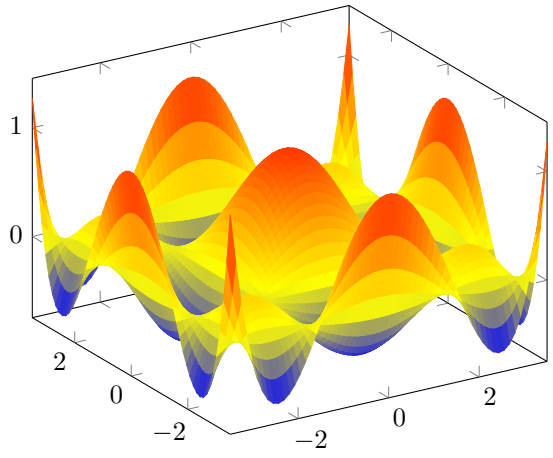
► Die Funktion $f : \mathbb{R}^2 \to \mathbb{R}$ sei definiert durch

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = 1 - \frac{x_1^2 + x_2^2}{2} + \frac{x_1^4 + x_2^4}{4} + \frac{x_1^2 \cdot x_2^2}{4} - \frac{x_1^2 \cdot x_2^4 + x_1^4 \cdot x_2^2}{48} + \frac{x_1^4 \cdot x_2^4}{576}.$$

Ihre partiellen Ableitungen sind

$$\frac{\partial f}{\partial x_1}(x_1, x_2) = x_1 + x_1^3 + \frac{x_1 \cdot x_2^2}{2} - \frac{x_1 \cdot x_2^4}{24} - \frac{x_1^3 \cdot x_2^2}{12} + \frac{x_1^3 \cdot x_2^4}{144}$$

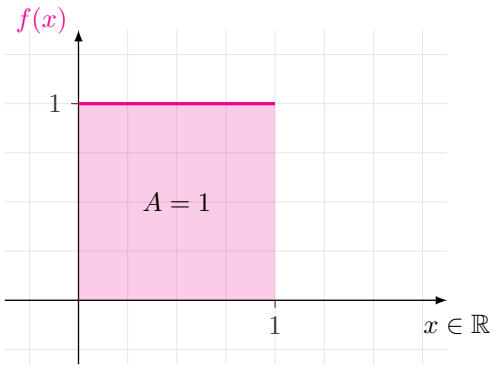
$$\frac{\partial f}{\partial x_2}(x_1, x_2) = x_2 + x_2^3 + \frac{x_1^2 \cdot x_2}{2} - \frac{x_1^2 \cdot x_2^3}{12} - \frac{x_1^4 \cdot x_2}{24} + \frac{x_1^4 \cdot x_2^3}{144}.$$



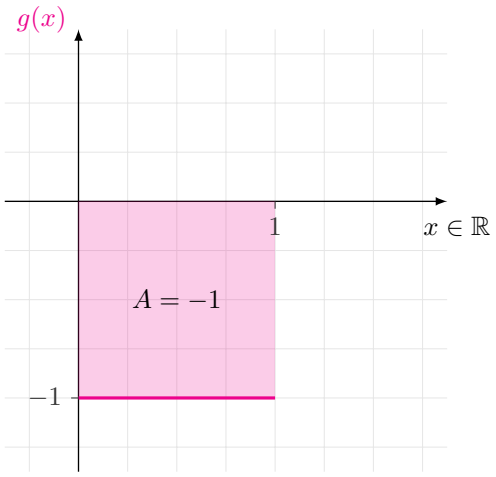
14 Das Integral

14.1. Definition

Für eine Funktion $f : [a, b] \to \mathbb{R}$ möchten wir die Fläche, die f mit der x-Achse einschließt, bestimmen. Ist beispielsweise f die Funktion $f : [0, 1] \to \mathbb{R}, x \mapsto 1$, so ist der Flächeninhalt 1.



Im Fall der Funktion $g : [0, 1] \to \mathbb{R}, x \mapsto -1$, ist der Flächeninhalt -1.



Für bestimmte besonders einfache Funktionen kann man den Flächeninhalt leicht bestimmen.

Definition 14.1.1 ("Treppenfunktion")**.**

Wir nennen eine Funktion $t : [a, b] \to \mathbb{R}$ eine ***Treppenfunktion***, wenn es Zahlen

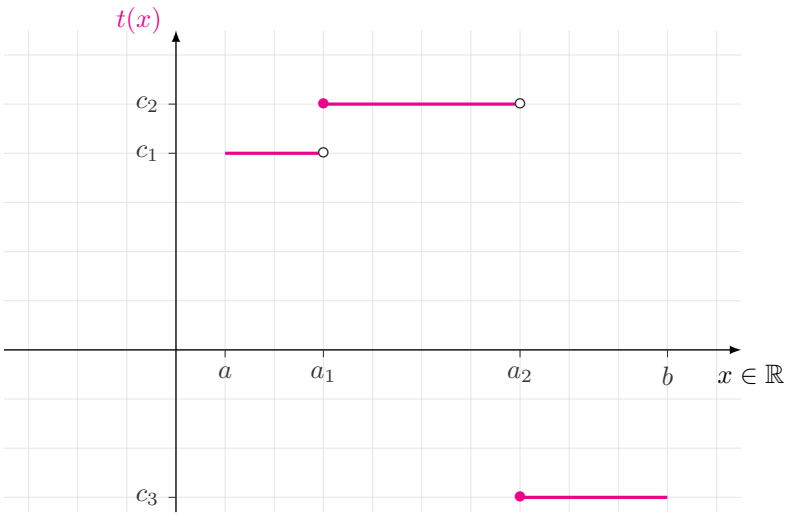
$$a = a_0 < a_1 < \cdots < a_k = b$$

und

$$c_1, \ldots, c_k \in \mathbb{R}$$

gibt, so dass

$$t(x) = c_i \qquad \text{für alle } x \in (a_{i-1}, a_i) \qquad (i = 1, \dots, k).$$



Beispiel 14.1.2.

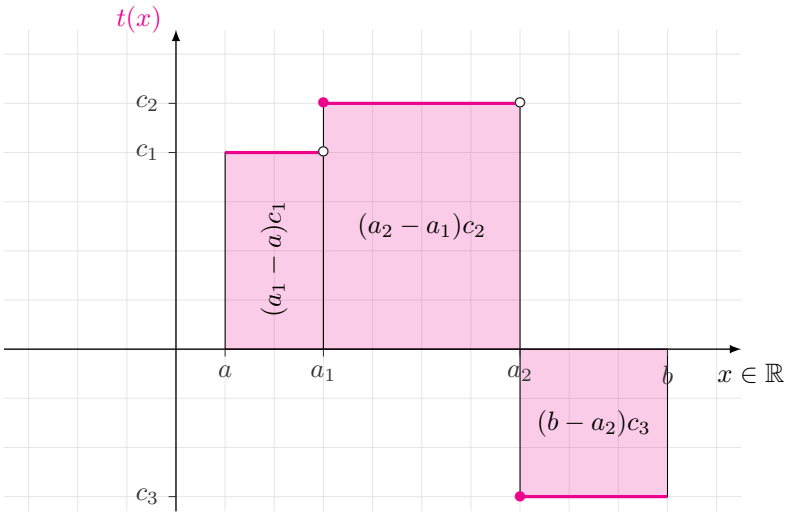
- ...

Für diese einfachen Treppenfunktionen definieren wir folgendes Symbol.

Definition 14.1.3 ("Integral von Treppenfunktionen")**.**

Sei $t : [a, b] \to \mathbb{R}$ eine Treppenfunktion. Dann sei

$$\int_a^b t(x)\mathrm{d}x = \sum_{i=1}^{k} c_i(a_i - a_{i-1}).$$

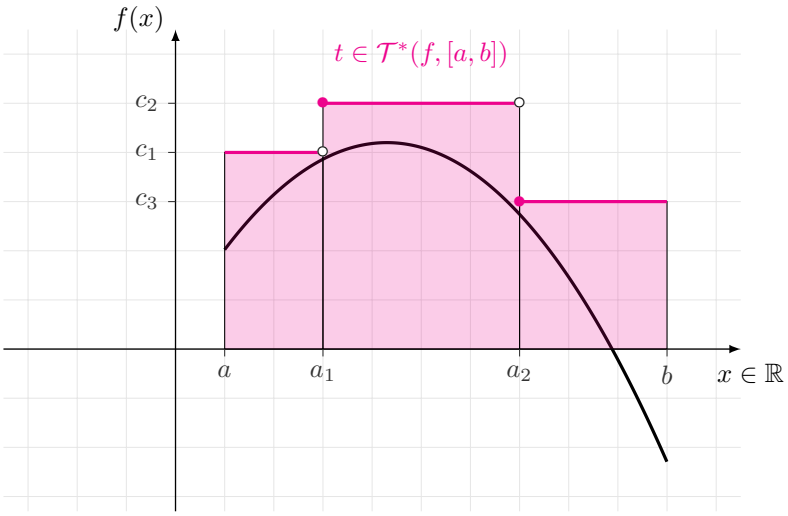


Für allgemeine Funktionen definieren wir das Integral mit Hilfe von Treppenfunktionen. Dazu müssen wir zunächst für jede allgemeine Funktion bestimmte Treppenfunktionen identifizieren.

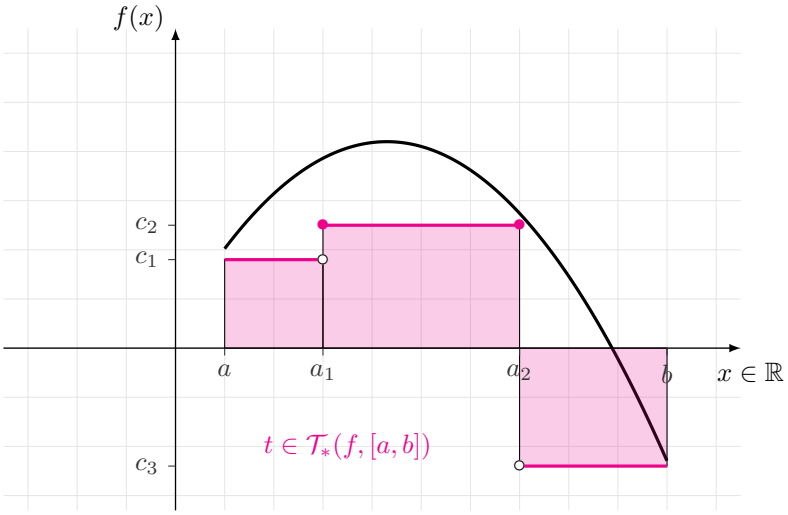
Definition 14.1.4.

Sei $f : S \to \mathbb{R}$ eine Funktion und seien a, b Zahlen, so dass $[a, b] \subset S$. Sei nun

- $\mathcal{T}^*(f, [a, b])$ die Menge aller Treppenfunktionen $t : [a, b] \to \mathbb{R}$, so dass $t(x) \geq f(x)$ für alle $x \in [a, b]$.



- $\mathcal{T}_*(f, [a, b])$ die Menge aller Treppenfunktionen $t : [a, b] \to \mathbb{R}$, so dass $t(x) \leq f(x)$ für alle $x \in [a, b]$.



Mit Hilfe der Mengen $\mathcal{T}^*(f, [a, b])$ und $\mathcal{T}_*(f, [a, b])$ können wir nun schlussendlich das Integral von f über einem Intervall definieren.

Definition 14.1.5 ("Integral")**.**

Wir nennen eine Funktion $f : [a, b] \to \mathbb{R}$ ***integrierbar*** auf $[a, b]$, falls

$$\inf \left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}^*(f, [a, b]) \right\} = \sup \left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}_*(f, [a, b]) \right\}.$$

In diesem Fall definieren wir das ***Integral von f über*** $[a, b]$, als

$$\int_a^b f(x)\mathrm{d}x = \sup \left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}_*(f, [a, b]) \right\}.$$

Bemerkung 14.1.6.

- Das Integralsymbol $\int$ ist ursprünglich ein "S" - und stand für die Summe der Integrale der einzelnen Treppenfunktionsabschnitte.
- Unter dem Integralsymbol steht die untere Intervallgrenze und oberhalb die obere Intervallgrenze.
- Das $\mathrm{d}x$ deutet an, dass über die Variable x integriert wird. Das ist dann besonders wichtig, wenn in der Funktion weitere Variablen auftauchen. Es streicht nochmal heraus, welche Variable die Funktionsvariable ist. Wird beispielsweise über eine Funktion integriert, deren Funktionsvariable y heißt, dann schreibt man $\mathrm{d}y$ hinter die zu integrierende Funktion.

  $$\int_{z_1}^{z_2} 3y^2 + 2x \mathrm{d}y$$

  In diesem Fall wird die Funktion $3y^2 + 2x$ über das Intervall $[z_1, z_2]$ integriert, wobei y die Funktionsvariable ist.
- Das Integralsymbol $\int$ und $\mathrm{d}x$ bilden eine Klammer. Alles was zwischen diesen beiden Symbolen steht gehört zu der Funktion, über welche integriert wird.
- Die Definition ist zunächst einmal alles andere als handlich. Das Supremum wird über unendlich viele Werte gebildet und in den meisten Fällen gar nicht von einer Treppenfunktion angenommen. Wie man Integrale dennoch berechnen kann, sehen wir in Abschnitt 14.3.1.

Die folgende Proposition formuliert nochmal, was wir intuitiv nun schon ahnen: Das Integral korrespondiert zu dem Flächeninhalt den Funktion und x-Achse einschließen.

Proposition 14.1.7.

Sei $f : S \to \mathbb{R}$ integrierbar. Dann entspricht für alle Zahlen $a, b \in \mathbb{R}$ mit $[a, b] \subset S$

$$\int_a^b f(x)\mathrm{d}x$$

dem (orientierten) Flächeninhalt, den f auf dem Intervall $[a, b]$ mit der x-Achse einschließt.

Beweis. Sei $g : S \to \mathbb{R}$ eine Funktion mit $[a, b] \subset S$. Dann bezeichne $A(g, [a, b])$ den (orientierten) Flächeninhalt, den die Funktion g auf dem Intervall $[a, b]$ mit der x-Achse einschließt.

Dann gilt für alle $t \in \mathcal{T}^*(f, [a, b])$, dass

$$\int_a^b t(x)\mathrm{d}x = A(t, [a, b]) \geq A(f, [a, b]).$$

Also ist $A(f, [a, b])$ eine untere Schranke an die Menge

$$\left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}^*(f, [a, b]) \right\}$$

und somit gilt nach der Definition des Infimums, dass

$$\int_a^b f(x)\mathrm{d}x = \inf \left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}^*(f, [a, b]) \right\} \geq A(f, [a, b]).$$

Umgekehrt gilt für alle $t \in \mathcal{T}_* f, [a,b])$, dass

$$\int_a^b t(x)\mathrm{d}x = A(t,[a,b]) \leq A(f,[a,b]).$$

Also ist $A(f,[a,b])$ eine obere Schranke an die Menge

$$\left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}_*(f,[a,b]) \right\}$$

und somit gilt nach der Definition des Supremums, dass

$$\int_a^b f(x)\mathrm{d}x = \sup \left\{ \int_a^b t(x)\mathrm{d}x : t \in \mathcal{T}_*(f,[a,b]) \right\} \geq A(f,[a,b]).$$

Also bleibt nur die Möglichkeit, dass

$$\int_a^b f(x)\mathrm{d}x = A(f,[a,b]),$$

wie behauptet. □

Bevor wir uns Beispiele anschauen, stellen wir uns die Frage, welche Funktionen integrierbar sind? Die Antwort ist tatsächlich nicht so einfach zu finden und sie sprengt den Rahmen dieser Vorlesung. Dennoch können wir integrierbare Funktionen charakterisieren. Dazu benötigen wir eine weitere Definition.

Definition 14.1.8 ("stückweise Stetigkeit")**.**

Wir nennen eine Funktion $f : [a,b] \to \mathbb{R}$ ***stückweise stetig***, wenn es Zahlen $c > 0$ und

$$a = a_0 < a_1 < \cdots < a_k = b$$

gibt, so dass f auf jedem Intervall (a_{i-1}, a_i) stetig ist für $i = 1, \ldots, k$ und $|f(x)| \leq c$ für alle $x \in [a,b]$.

Proposition 14.1.9.

Wenn $f : [a,b] \to \mathbb{R}$ stückweise stetig ist, ist f integrierbar auf $[a,b]$.

Der Beweis von Proposition 14.1.9 ist relativ aufwendig und übersteigt den Rahmen dieser Vorlesung, wir nehmen die Proposition dennoch dankbar zur Kenntnis.

Nun können wir uns endlich einem Beispiel zuwenden.

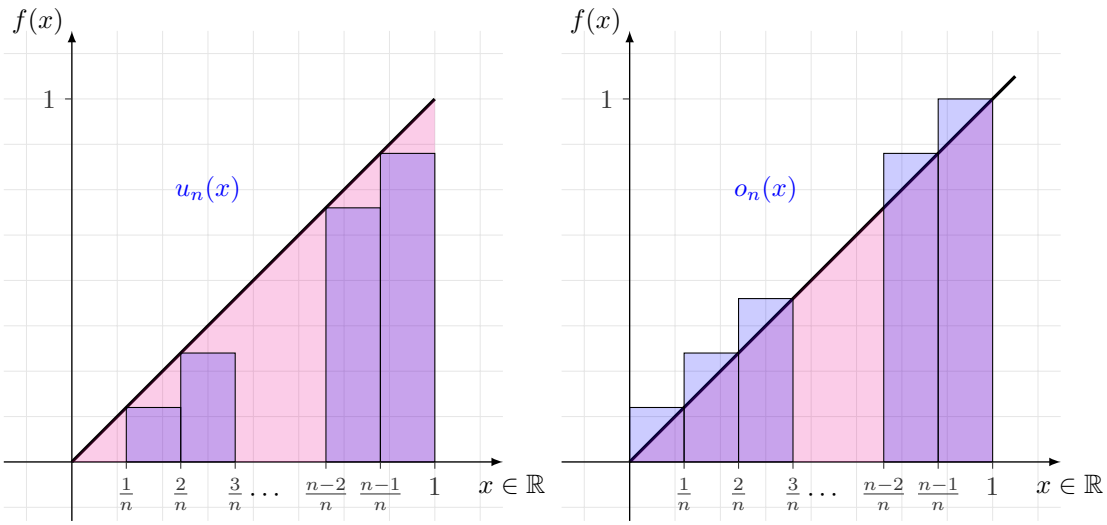
Beispiel 14.1.10.

Wir integrieren die Funktion $f : [0,1] \to \mathbb{R}, x \mapsto x$. Zu diesem Zweck konstruieren wir "untere" und "obere" Treppenfunktionen. Sei $n \geq 1$ eine natürliche Zahl. Wir erhalten eine untere Treppenfunktion u_n, indem wir definieren

$$u_n(x) = \frac{1}{n} \cdot \max \left\{ k \in \mathbb{Z} : \frac{k}{n} \leq x \right\}.$$

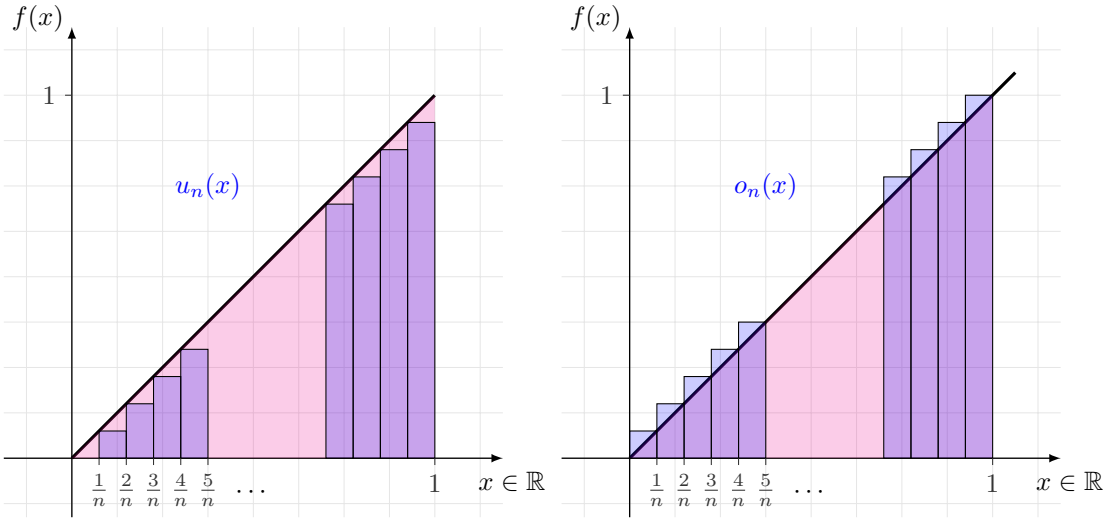
Entsprechend erhält man eine obere Treppenfunktion o_n mittels

$$o_n(x) = \frac{1}{n} \cdot \min \left\{ k \in \mathbb{Z} : \frac{k}{n} \geq x \right\}.$$



Die Integrale dieser Treppenfunktionen können wir leicht ausrechnen:

$$\int_0^1 u_n(x)\mathrm{d}x = \sum_{i=0}^{n-1} \frac{i}{n^2} = \frac{(n-1)n}{2n^2}, \qquad \int_0^1 o_n(x)\mathrm{d}x = \sum_{i=1}^{n} \frac{i}{n^2} = \frac{(n+1)n}{2n^2}$$



Weil dann aber

$$\lim_{n\to\infty} \int_0^1 u_n(x)\mathrm{d}x = \lim_{n\to\infty} \int_0^1 o_n(x)\mathrm{d}x = \frac{1}{2}$$

folgt

$$\int_0^1 f(x)\mathrm{d}x = \frac{1}{2}.$$

Wie schon in den vorherigen Kapiteln die entsprechenden Objekte, ist das Integral zumindest verträglich mit der Addition von Funktionen und der Multiplikation einer Funktion mit einem Skalar. Die Beweisen gehen direkt auf die Definition des Integrals zurück und wir führen sie hier nicht im Detail aus.

Proposition 14.1.11.

Seien $f_1 : [a, b] \to \mathbb{R}$, $f_2 : [a, b] \to \mathbb{R}$ integrierbare Funktionen. Sei $c \in \mathbb{R}$. Dann sind die Funktionen $f_1 + f_2$ und $c \cdot f_1$ integrierbar und

$$\int_a^b (f_1 + f_2)(x)\mathrm{d}x = \int_a^b f_1(x)\mathrm{d}x + \int_a^b f_2(x)\mathrm{d}x, \qquad \int_a^b (c \cdot f_1)(x)\mathrm{d}x = c \cdot \int_a^b f_1(x)\mathrm{d}x.$$

Wenn ferner $f_1(x) \leq f_2(x)$ für alle $x \in (a, b)$, dann gilt

$$\int_a^b f_1(x)\mathrm{d}x \leq \int_a^b f_2(x)\mathrm{d}x.$$

Bemerkung 14.1.12.

Wir schließen diesen Abschnitt mit einer Konvention und zwei kleinen Beobachtungen.

Definition 14.1.13. Wenn f auf $[a, b]$ integrierbar ist, dann ist

$$\int_b^a f(x)\mathrm{d}x = -\int_a^b f(x)\mathrm{d}x.$$

Wenn f auf $[a, b]$ integrierbar ist gitl für alle $c \in [a, b]$, dass

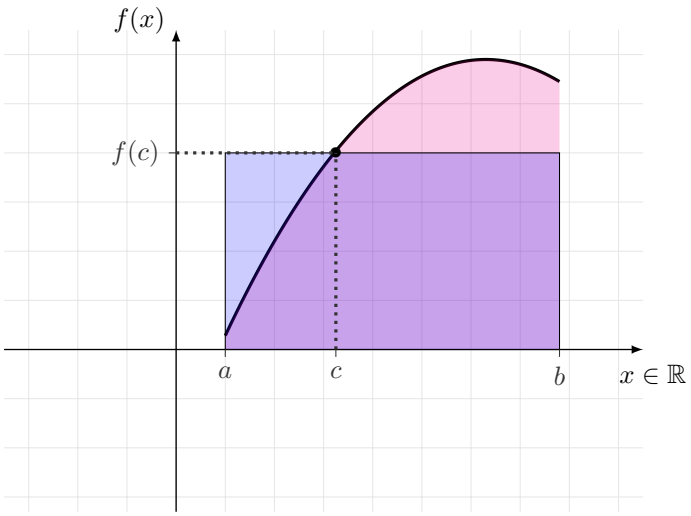
$$\int_c^c f(x)\mathrm{d}x = 0.$$

Wenn $a \leq b \leq c$ reelle Zahlen sind und f auf $[a, c]$ integrierbar ist, dann gilt

$$\int_a^c f(x)\mathrm{d}x = \int_a^b f(x)\mathrm{d}x + \int_b^c f(x)\mathrm{d}x.$$

14.2. Der Mittelwertsatz (der Integralrechnung)

Der Mittelwertsatz der Integralrechnung besagt: Das Integral über ein Intervall $[a, b]$ einer auf $[a, b]$ stetigen Funktion entspricht dem Produkt der Intervalllänge $b - a$ und dem Funktionswert einer Stelle $c \in [a, b]$. Der Betrag des Integrals entspricht also dem Volumen des Rechtecks mit Seitenlänge $b - a$ und $|f(c)|$, das Vorzeichen dem Vorzeichen von $f(c)$.



Proposition 14.2.1 ("Mittelwertsatz der Integralrechnung")**.**

Wenn f auf $[a, b]$ stetig, gibt es ein $c \in [a, b]$, so dass

$$\int_a^b f(x)\mathrm{d}x = (b - a) \cdot f(c).$$

Beweis. Da f stetig auf $[a, b]$ ist, ist f nach Proposition 14.1.9 dort auch integrierbar.

Wir betrachten die stetige Funktion $h : [a, b] \to \mathbb{R}, x \mapsto f(x)(b - a)$. Es gilt

$$\inf\{h(x) : x \in [a, b]\} \leq \int_a^b f(x)\mathrm{d}x \leq \sup\{h(x) : x \in [a, b]\}.$$

Nach dem Zwischenwertsatz gibt es also ein $c \in [a, b]$, so dass

$$(b - a) \cdot f(c) = h(c) = \int_a^b f(x)\mathrm{d}x,$$

wie behauptet. □

14.3. Der Hauptsatz der Differential- und Integralrechnung

Bislang haben wir nur Aussagen über die Existenz von Integralen bzw. integrierbaren Funktionen getroffen, aber kein praktisches Schema zur Berechnung von Integralen kennen gelernt. Das ändert sich nun. Dazu brauchen wir die folgende Definition.

Definition 14.3.1 ("Stammfunktion")**.**

Sei $S \subset \mathbb{R}$ und $f : S \to \mathbb{R}$ eine Funktion. Eine Funktion $F : S \to \mathbb{R}$, die auf S differenzierbar ist, heißt ***Stammfunktion*** von f, falls

$$f(x) = F'(x) \qquad \text{für alle } x \in S.$$

Beispiel 14.3.2.

Sei $f : [0,5] \to \mathbb{R}$ mit $x \mapsto c$.

Die Funktion $F_1 : [0,5] \to \mathbb{R}$ mit $x \mapsto c \cdot x$ ist auf $[0,5]$ differenzierbar und es ist $F_1'(x) = c = f(x)$ für alle $x \in [0,5]$. Sie ist also eine Stammfunktion auf f.

Allerdings ist auch die Funktion $F_2 : [0,5] \to \mathbb{R}$ mit $x \mapsto c \cdot x + 13$ auf $[0,5]$ differenzierbar und es ist $F_2'(x) = c = f(x)$ für alle $x \in [0,5]$. Sie ist also auch eine Stammfunktion auf f.

Wie Beispiel 14.3.2 zeigt, ist die Stammfunktion einer Funktion nicht eindeutig bestimmt, aber fast, wie die folgende Proposition zeigt.

Proposition 14.3.3.

Sei $S \subset \mathbb{R}$ und $f : S \to \mathbb{R}$ eine Funktion. Angenommen F_1, F_2 sind Stammfunktionen von f. Dann gibt es eine Zahl $c \in \mathbb{R}$, so dass

$$F_1(x) = F_2(x) + c \qquad \text{für alle } x \in S.$$

Beweis. Die Funktion $F_1 - F_2$ hat die Ableitung

$$(F_1 - F_2)'(x) = F_1'(x) - F_2'(x) = f(x) - f(x) = 0.$$

Nach Korollar 13.4.3 ist $F_1 - F_2$ also sowohl monoton wachsend als auch monoton fallend, also konstant. Das bedeutet, dass es eine Zahl $c \in \mathbb{R}$ gibt, so dass $F_1(x) - F_2(x) = c$ für alle $x \in S$. □

Satz 14.3.4 ("Hauptsatz der Differential- und Integralrechnung")**.**

Sei $f : [a,b] \to \mathbb{R}$ stetig. Dann ist

$$F : [a,b] \to \mathbb{R}, \qquad x \mapsto \int_a^x f(y)\mathrm{d}y$$

eine Stammfunktion von f.

Beweis. Sei $x \in [a,b]$. Falls $x < b$, gibt es nach Proposition 14.2.1 zu jeder hinreichend kleinen Zahle $z > 0$ ein $c^z \in [x, x+z]$, so dass

$$F(x+z) - F(x) = \int_a^{x+z} f(y)\mathrm{d}y - \int_a^x f(y)\mathrm{d}y = \int_x^{x+z} f(y)\mathrm{d}y = z \cdot f(c^z). \tag{14.1}$$

Weil f stetig ist, gilt

$$\lim_{z \to 0} f(c^z) = f(x).$$

Falls $x > a$, gibt es nach Proposition 14.2.1 zu jeder hinreichend kleinen Zahle $z > 0$ ein $c_z \in [x-z, x]$, so dass

$$F(x-z) - F(x) = \int_a^{x-z} f(y)\mathrm{d}y - \int_a^x f(y)\mathrm{d}y = \int_x^{x-z} f(y)\mathrm{d}y = -z \cdot f(c_z). \tag{14.2}$$

Wiedrum aufgrund der Stetigkeit von f ist, gilt

$$\lim_{z\to 0} f(c_z) = f(x).$$

Aus (14.1) und (14.2) folgt also

$$F'(x) = \lim_{z\to 0} \frac{F(x+z) - F(x)}{z} = f(x)$$

wie behauptet. □

14.3.1. Integrale berechnen

Mit Hilfe von Proposition 14.3.3 und Satz 14.3.4 ist es nun möglich, viele Integrale auszurechnen. Nun also das allgemeine Rezept.

Korollar 14.3.5.

Sei $f : [a, b] \to \mathbb{R}$ stetig und sei F eine Stammfunktion von f. Dann gilt

$$\int_a^b f(x)\mathrm{d}x = F(b) - F(a).$$

Beweis. Sei $G(y) = \int_a^y f(x)\mathrm{d}x$. Nach Satz 14.3.4 ist G eine Stammfunktion von f. Nach Proposition 14.3.3 existiert also eine Zahl $c \in \mathbb{R}$, so dass $F(x) = G(x) + c$ für alle $x \in [a, b]$. Daraus folgt, dass

$$F(b) - F(a) = G(b) - G(a) = \int_a^b f(x)\mathrm{d}x - \int_a^a f(x)\mathrm{d}x = \int_a^b f(x)\mathrm{d}x - 0 = \int_a^b f(x)\mathrm{d}x,$$

wie behauptet. □

Beispiel 14.3.6.

In Beispiel 14.1.10 haben wir ausgerechnet, dass $\int_0^1 x\mathrm{d}x = \frac{1}{2}$.

Mit Korollar 14.3.5 können wir dieses Integral einfacher ausrechnen. Denn die Funktion $f : [0, 1] \to \mathbb{R}, x \mapsto x$ hat die Stammfunktion $F : [0, 1] \to \mathbb{R}, x \mapsto \frac{1}{2} \cdot x^2$. Also erhalten wir

$$\int_0^1 x\mathrm{d}x = F(1) - F(0) = \frac{1}{2} \cdot 1^2 - \frac{1}{2} \cdot 0^2 = \frac{1}{2}.$$

14.3.2. Zwei "Integral-Berechnung-Tricks" für stetig differenzierbare Funktionen

Mit Hilfe von Korollar 14.3.5 gewinnen wir aus den Ableitungsregeln, insbesondere der Produkt- und der Kettenregel, Rechenregeln für das Integrieren. Um diese Regeln formulieren zu können, benötigen wir noch einen weiteren Begriff.

Definition 14.3.7 ("Stetige Differenzierbarkeit")**.**

Eine Funktion $f : S \to \mathbb{R}$ heißt ***stetig differenzierbar***, falls f auf S differenzierbar ist und die Ableitung $f' : S \to \mathbb{R}$ eine stetige Funktion ist.

Korollar 14.3.8 ('Partielle Integration")**.**

Seien $f_1, f_2 : [a, b] \to \mathbb{R}$ stetig differenzierbar. Dann gilt

$$\int_a^b f_1'(x) f_2(x) \mathrm{d}x = f_1(b) f_2(b) - f_1(a) f_2(a) - \int_a^b f_1(x) f_2'(x) \mathrm{d}x.$$

Beispiel 14.3.9.

Für das Beispiel setzen wir voraus, dass $\sin(x)$ und $\cos(x)$ stetig differenzierbar auf ganz $\mathbb{R}$ sind und dass $\frac{d}{\mathrm{d}x} sin(x) = cos(x)$ ist. Außerdem prüft man leicht nach, dass $f : \mathbb{R} \to \mathbb{R}, x \mapsto x$ stetig differenzierbar ist.

Man kann mit Hilfe der Partiellen Integration für je zwei Zahlen a und b das folgende Integral über $[a, b]$ berechnen

$$\int_a^b \cos(x) \cdot x \mathrm{d}x.$$

Setze dazu

$$f_1(x) = \sin(x) \qquad \text{und} \qquad f_2(x) = x.$$

Dann ist

$$f_1(x) = \sin(x) \qquad f_2(x) = x$$
$$f_1'(x) = \cos(x) \qquad f_2'(x) = 1.$$

und

$$\int_a^b \cos(x) \cdot x \mathrm{d}x = \int_a^b f_1'(x) f_2(x) \mathrm{d}x.$$

Nach Korollar 14.3.8 gilt also

$$\begin{aligned}\int_a^b \cos(x) \cdot x \mathrm{d}x &= f_1(b) f_2(b) - f_1(a) f_2(a) - \int_a^b f_1(x) f_2'(x) \mathrm{d}x \\ &= \sin(b) \cdot b - \sin(a) \cdot a - \int_a^b \sin(x) \cdot 1 \mathrm{d}x \\ &= \sin(b) \cdot b - \sin(a) \cdot a - \int_a^b \sin(x) \mathrm{d}x.\end{aligned}$$

Korollar 14.3.10 ('Substitutionsregel")**.**

Sei $f_1 : [c, d] \to \mathbb{R}$ stetig und $f_2 : [a, b] \to [c, d]$ stetig differenzierbar. Dann gilt

$$\int_a^b f_1(f_2(x)) f_2'(x) \mathrm{d}x = \int_{f_2(a)}^{f_2(b)} f_1(x) \mathrm{d}x.$$

Beispiel 14.3.11.

Das Integral

$$\int_a^b \sin(-7x+3)\mathrm{d}x$$

kann mit Hilfe der Substitutionsregel berechnet werden. Dazu setzt man

$$f_1(x) = \sin(x) \qquad \text{und} \qquad f_2(x) = -7x+3.$$

Dann ist

$$f_2'(x) = -7.$$

Also findet man

$$\begin{aligned}\int_a^b \sin(-7x+3)\mathrm{d}x &= \frac{1}{-7}\cdot\int_a^b \sin(-7x+3)\cdot(-7)\mathrm{d}x \\ &= \frac{1}{-7}\cdot\int_a^b f_1(f_2(x))f_2'(x)\mathrm{d}x.\end{aligned}$$

Nach Korollar 14.3.10 gilt also

$$\begin{aligned}\int_a^b \sin(-7x+3)\mathrm{d}x &= \int_{f_2(a)}^{f_2(b)} f_1(x)\mathrm{d}x \\ &= \int_{-7\cdot a+3}^{-7\cdot b+3} \sin(x)\mathrm{d}x.\end{aligned}$$

15 Die Komplexen Zahlen

15.1. Warum imaginäre Zahlen so heißen wie sie heißen

Dieses Kapitel widmet sich den *komplexen Zahlen*, einer Zahlenmenge, die zusammen mit Addition und Multiplikation einen *Zahlkörper* bildet. Die folgenden Zahlenmengen sind bereits bekannt:

- die *natürlichen* Zahlen $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$
- die *ganzen* Zahlen $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$
- die *rationalen* Zahlen $\mathbb{Q} = \{\frac{p}{q} \ : \ p, q \in \mathbb{Z}, q \neq 0\}$
- die *reellen* Zahlen $\mathbb{R} = \{a + 0, d_1 d_2 d_3 \ldots \ : \ a \in \mathbb{Z}$ und $\underbrace{(d_n)_{n\in\mathbb{N}} \text{ mit } d_k \in \{0, 1, \ldots 9\}}_{\text{Nachkomma-Ziffern}} \}$

Diese Mengen von Zahlen haben Entsprechungen in der echten Welt:

- Die natürlichen Zahlen entsprechen der Anzahl zählbarer Gegenstände.
- Brüche (rationale Zahlen) stehen für "Anteile eines geteilten Ganzen" (Pizza).
- Auch reelle Zahlen treten im Alltage auf. Zum Beispiel ist $\sqrt{2}$ die Länge der Diagonale in einem 1-mal-1 großen Quadrat (Fliese). Auch das Verhältnis der Seiten eines Blatt Papiers im DinA4-Format ist 1 zu $\sqrt{2}$.

Alle diese Zahlen bis hin zu den reellen Zahlen lassen sich also in der Umwelt anschaulich darstellen. Nicht so die imaginäre Einheit bzw. die komplexen Zahlen: Sie entsprechen den nicht ganz so greifbaren, abstrakten Lösungen von Polynomgleichungen. Man kann sich diese Zahlen zwar veranschaulichen, also auf ein Blatt Papier zeichnen, man findet Sie jedoch in der Natur nur hinter den Kulissen, im Wirken von physikalischen Gesetzen.

15.2. Definition

Die Klasse der reellen Zahlen ist sehr groß, trotzdem lernt man in der Schule, dass $a \cdot x^2 + b \cdot x + c = 0$ nur dann lösbar ist, falls ihre Diskriminante $\Delta = b^2 - 4ac$ nicht-negativ ist, da aus einer negativen Zahl keine Wurzel gezogen werden kann.

Beispielsweise hat die Gleichung $x^2 = -1$ keine *reelle* Lösung, was etwas unbefriedigend ist. Lässt sich nicht vielleicht doch irgendwie eine Zahl $\sqrt{-1}$ definieren? Die Antwort ist *jein*. Tatsächlich gibt es keine reelle Zahl $x \in \mathbb{R}$ mit $x^2 = -1$, hier wurde Ihnen also nichts vorenthalten, trotzdem konstruieren wir nun eine Lösung, indem wir uns eine entsprechende Zahl definieren.

15.2.1. Die imaginäre Einheit

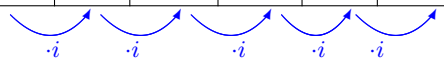
Definition 15.2.1.

Wir definieren eine Zahl i (genannt die imaginäre Einheit) so, dass $i^2 = -1$ gilt.

Die Zahl i ist in sofern imaginär, als dass sie keine *reelle* Zahl ist, und keine direkt greifbare Entsprechung in der "echten" Welt besitzt. Mit dieser neuen, zusätzlichen Zahl können nun die Lösungen für $x^2 = -1$ angeben, dies sind nämlich i und $-i$.

Aus der Regel $i^2 = -1$ lässt sich folgern, dass sich Potenzen von i wieder als ± 1 oder $\pm i$ schreiben lassen:

k	0	1	2	3	4	
i^k	i^0	i^1	i^2	i^3	i^4	$\dots$
Wert	1	i	-1	$-i$	1	$\dots$



Definition 15.2.2.

Eine Komplexe Zahl z hat die Form $z = a + i \cdot b$ dabei sind $a, b \in \mathbb{R}$ und i ist die *imaginäre Einheit*.

Für $z = a + i \cdot b$ ist $\mathsf{Re}(z) := a$ der *Realteil* von z und $\mathsf{Im}(z) := b$ der *Imaginärteil* von z.

Die Menge aller Komplexen Zahlen kürzt man ab mit $\mathbb{C} := \{a + i \cdot b \ : \ a, b \in \mathbb{R}\}$

Bemerkung 15.2.3.

Typischer Fehler:
Der Imaginärteil von $z = a + i \cdot b$ ist die **reelle** Zahl b und **nicht i** $\cdot b$.

Mit i können wir nun Lösungen für *alle* Polynomgleichungen angeben – nicht nur eine Lösung für $x^2 = -1$.

Satz 15.2.4.

Für das Polynom $x^2 + px + q$ mit $p, q \in \mathbb{R}$ sei $\left(\frac{p}{2}\right)^2 - q < 0$.

Dann hat die Gleichung $x^2 + px + q = 0$ die komplexen Lösungen

$$z_1 := -\frac{p}{2} + i \cdot \sqrt{\left|\left(\frac{p}{2}\right)^2 - q\right|} \quad \text{und} \quad z_2 = \overline{z}_1 := -\frac{p}{2} - i \cdot \sqrt{\left|\left(\frac{p}{2}\right)^2 - q\right|}$$

Den Beweis führt man durch einfaches Einsetzen und Nachrechnen unter Beachtung, dass hier gilt:

$$\left(\frac{p}{2}\right)^2 - q < 0 \quad \Rightarrow \quad \left|\left(\frac{p}{2}\right)^2 - q\right| = q - \left(\frac{p}{2}\right)^2$$

Beispiel 15.2.5.

Gesucht sind die Lösungen von $x^2 + 2x + 10 = 0$ mit der p-q-Formel ergibt sich:

$$x_{1,2} = -1 \pm \sqrt{1 - 10} = -1 \pm \sqrt{(-1) \cdot 9} = -1 \pm 3 \cdot \sqrt{-1}.$$

In reellen Zahlen gibt es hier keine Lösung, in komplexen Zahlen lauten die Lösungen $x_{1/2} = -1 \pm 3 \cdot i$.

Bemerkung 15.2.6.

Typischer Fehler: i ist *nicht* "$\sqrt{-1}$"
Obwohl es verführerisch aussieht, ist es **nie richtig "$i = \sqrt{-1}$"** zu schreiben. In Beispiel 15.2.5 *sieht es zwar so aus* als *hätte* man "$\sqrt{-1}$" durch i ersetzt, *trotzdem* ***gilt nicht "$i = \sqrt{-1}$"***.

Die Wurzelfunktion $\sqrt{x}$ liefert für $x \in \mathbb{R}$ mit $x \geq 0$ das *nicht-negative* y, für dass $y^2 = x$ gilt. Wegen der Einschränkung "*nicht-negativ*" funktioniert die Wurzelfunktion nicht bei -1:

- Die Lösungen für $y^2 = 16$ sind zum Beispiel 4 und -4,
  die Wurzelfunktion liefert aber nur die postive Lösung $\sqrt{16} = 4$.
- Die Lösungen für $y^2 = -1$ sind i und $-i$,
  aber hier ist (und bleibt!) unklar, wer "die positive" Lösung ist.

Sowohl i als auch $-i$ sind *weder* positiv *noch* negativ!

Auch das Argument "i hat kein Vorzeichen" zieht hier nicht, denn: Bei der Definition von $\mathbb{C}$ hätte man (statt die Zahl i zu wählen) ebenso gut die komplexen Zahlen über $j := (-i)$ definieren können! Dann hätte die Zahl j (also eigentlich $-i$) "kein Vorzeichen".

Ein anderes, etwas schwierigeres Argument für $i \neq \sqrt{-1}$ ist das Folgende:

Wäre $\sqrt{-1}$ eine echte Zahl, so dürfte man also aus -1 die Wurzel ziehen, d.h. für die entstehende Zahl $\sqrt{-1}$ müsste dann die übliche Wurzelrechenregel $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b}$ gelten.

($\star$) Annahme: Es gelte $i = \sqrt{-1}$.
($\star\star$) Dann gilt die Wurzelrechenregel $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b}$ auch für $a = b = -1$.

$$\begin{array}{lrcl} \text{Es gilt dann also:} & 1) & 1 & = & \sqrt{(-1)\cdot(-1)} \\ & 2) & \overset{\star\star}{\Leftrightarrow} \; 1 & = & \sqrt{(-1)} \cdot \sqrt{(-1)} \\ & 3) & \overset{\star}{\Leftrightarrow} \; 1 & = & i \cdot i \\ & 4) & \Leftrightarrow \; 1 & = & -1 \end{array}$$

Während hier 1) unstrittig wahr ist, ist 4) unstrittig falsch, d.h. die Annahme $i = \sqrt{-1}$ führt zu einem Widerspruch (und zwar durch ($\star\star$), das direkt aus $i = \sqrt{-1}$ folgt).

15.2.2. Rechnen mit komplexen Zahlen

Das Rechnen mit komplexen Zahlen folgt im Wesentlichen den Rechenregeln für reele Zahlen, d.h. auch hier gilt beispielsweise die Regel "Punkt- vor Strichrechnung". Für das Multiplizieren von komplexen Zahlen benötigt man zum einen ein gutes Verständnis der Binomischen Formeln und zum anderen die einfache Einsicht, dass sich Potenzen von i wieder als ± 1 oder $\pm i$ schreiben lassen:

Addition in $\mathbb{C}$

$$\begin{array}{rll} & a + & b \cdot i \\ + & c + & d \cdot i \\ \hline = & (a+c) + & (b+d) \cdot i \end{array}$$

Addition von Polynomen

$$\begin{array}{rll} & a + & b \cdot x \\ + & c + & d \cdot x \\ \hline = & (a+c) + & (b+d) \cdot x \end{array}$$

Multiplikation in $\mathbb{C}$

$$\begin{aligned} & (a + b \cdot i) \cdot (c + d \cdot i) \\ \hline = \; & a \cdot c + (a \cdot d + c \cdot b)\, i + b \cdot d \cdot \underbrace{i^2}_{=-1} \\ = \; & a \cdot c - b \cdot d + (a \cdot d + c \cdot b)\, i \end{aligned}$$

Multiplikation von Polynomen

$$\begin{aligned} & (a + b \cdot x) \cdot (c + d \cdot x) \\ \hline = \; & a \cdot c + (a \cdot d + c \cdot b)\, x + b \cdot d \cdot x^2 \end{aligned}$$

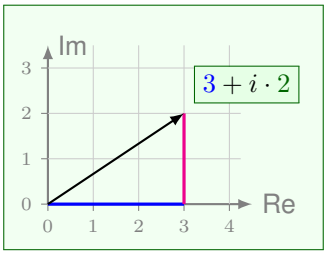
15.3. Komplexe Zahlen als kartesische Vektoren

Die Menge der komplexen Zahlen $\mathbb{C}$ lässt sich auffassen als ein zwei-dimensionaler reeller Vektorraum.

Jeder Zahl $z = a + i \cdot b$ kann man einen Vektor $\begin{pmatrix} \mathsf{Re}(z) \\ \mathsf{Im}(z) \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ zuordnen. Im zugehörigen $\mathbb{R}^2$ bezeichnet man die x_1-Achse mit Re und die x_2-Achse mit Im. Den entstehenden besonderen $\mathbb{R}^2$ nennt man die "*komplexe Zahlenebene*" oder auch die "Gaussche Zahlenebene".

Beide Koordinaten-Achsen (auch die Im-Achse!) werden mit Zahlen aus $\mathbb{R}$ beschriftet.

(Die Zahl $z := 2i$ liegt beispielsweise als Vektor $\begin{pmatrix} 0 \\ 2 \end{pmatrix}$ auf der Im-Achse bei Achsenabschnitt "2" (d.h. bei $\mathsf{Im}(2i) = 2$). Der *Wert* der komplexen Zahl z ist aber weiterhin $2i$ und damit komplex.)



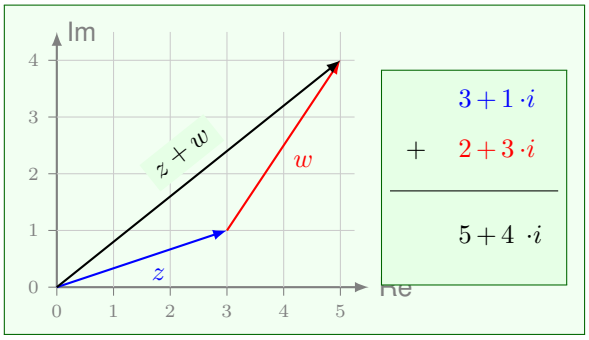
Die Addition von zwei Komplexen Zahlen durch *getrenntes* Addieren von jeweils zwei Realteilen und zwei Imaginärteilen läuft ganz analog zur Addition von Vektoren im R^2 ab. Wie dort so entspricht auch in $\mathbb{C}$ die Addition dem *Aneinanderhängen* der Zahlen bzw. Vektoren:

Addition in $\mathbb{C}$

$$\begin{array}{rll} & a + & b \cdot i \\ + & c + & d \cdot i \\ \hline = & (a+c) + & (b+d) \cdot i \end{array}$$

Addition von Vektoren

$$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a+c \\ b+d \end{pmatrix}$$



Jede Zahl $z \in \mathbb{C}$ hat als Vektor eine Länge und einen Winkel (zur Re-Achse):

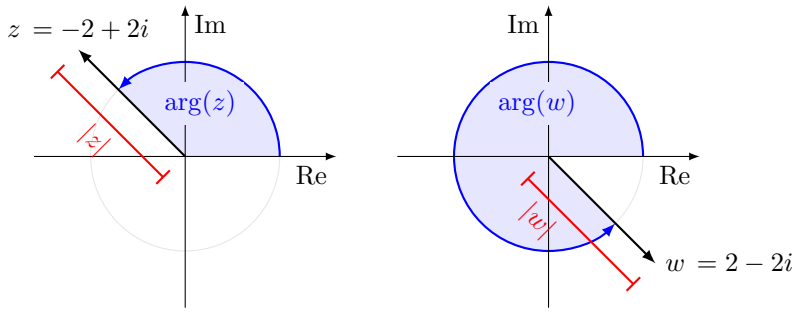
Definition 15.3.1.

Der *Betrag* einer komplexen Zahl $z = a + b \cdot i$ ist die Länge des Vektors $\begin{pmatrix} a \\ b \end{pmatrix}$, es gilt $|z| := \sqrt{a^2 + b^2}$.

Das Argument $\arg(z) \in [0, 2\pi)$ einer komplexen Zahl $z \in \mathbb{C}$ ist der Winkel, der zwischen der Re-Achse und der Strecke von 0 nach z eingeschlossen wird.

Beispiel 15.3.2.

- Für die Zahl $z = -2 + 2i$ ist $|z| = \sqrt{2^2 + 2^2} = 2 \cdot \sqrt{2}$ und $\arg(z) = \frac{3}{4}\pi$.
- Für die Zahl $w = 2 - 2i$ ist $|z| = \sqrt{2^2 + 2^2} = 2 \cdot \sqrt{2}$ und $\arg(z) = 2\pi - \frac{\pi}{4} = \frac{7}{4}\pi$.



Bemerkung 15.3.3.

Achtung: Winkel vs. Argument
Man beachte, dass nach obiger Definition für $\arg(z)$ stets $0 \leq \arg(z) < 2\pi$ gilt.

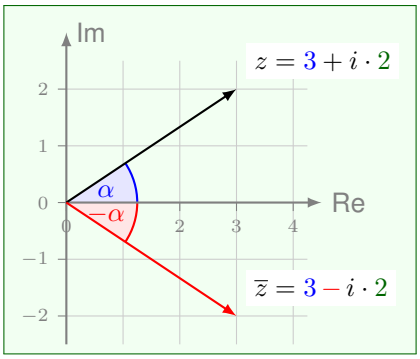
Gibt man jedoch Winkel an, so sind zwei Winkel äquivalent, wenn sie sich nur um ein Vielfaches von 2π unterscheiden.

Das Bogenmaß ordnet dem vollen Kreis den Wert 2π zu, weil der Kreisumfang des Einheitskreises (der Kreis mit Radius $r = 1$) Umfang $2\pi r = 2\pi$ hat.

15.4. Konjugiert komplexe Zahlen und Division

Definition 15.4.1.

Für eine komplexe Zahl $z = a + b \cdot i$, bezeichnet man mit $\overline{z} = a - b \cdot i$ die zu z *konjugiert komplexe Zahl*, die aus z durch Spiegelung an der reellen Achse hervorgeht.



Offensichtlich haben z und $\overline{z}$ die selbe Länge, aber entgegengesetzte Winkel. Es gelten:

$$|\overline{z}| = |z| \qquad \text{und} \qquad \arg(\overline{z}) = 2\pi - \arg(z).$$

Konjugieren und rechnen mit komplexen Zahlen ist vertauschbar. Bei Summen und Produkten kann das Konjugieren also vor oder nach dem Addieren bzw. Multiplizieren geschehen. Genauer gelten für $z, w \in \mathbb{C}$:

$$\overline{(z+w)} = \overline{z} + \overline{w} \qquad \text{und} \qquad \overline{(z \cdot w)} = \overline{z} \cdot \overline{w}$$

15.4.1. Verwendung

Das Konjugieren einer komplexen Zahl z wird "beim Berechnen von reellen Zahlen aus z" genutzt. Mit Hilfe der dritten Binomischen Formel gilt für $z = a + b \cdot i$:

$$z \cdot \overline{z} = (a + b \cdot i) \cdot (a - b \cdot i) = a^2 - (i \cdot b)^2 = a^2 + b^2$$

Dies kannn beim Teilen durch komplexe Zahlen verwendet werden: Um auf einen reellen Nenner zu kommen, erweitert man einen komplexwertigen Bruch $\frac{w}{z}$ mit $\overline{z}$, dem komplex Konjugietrten des Nenners.

Beispiel 15.4.2.

Für $z = 4 + 3i$ und $w = 1 + i$ gilt:

$$\frac{w}{z} = \frac{w \cdot \overline{z}}{z \cdot \overline{z}} = \frac{(1+i) \cdot (4 - 3 \cdot i)}{(4 + 3 \cdot i) \cdot (4 - 3 \cdot i)} = \frac{7 + i}{4^2 + 3^2} = \frac{7}{25} + \frac{1}{25} \cdot i$$

Lemma 15.4.3.

Für $z = a + b \cdot i$ und $w = c + d \cdot i$ gelten:

$$\frac{w}{z} = \frac{ca + db}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2} \cdot i$$

Das Ergebnis der Division $\frac{w}{z}$ ist also stets wieder eine komplexe Zahl.

Beweis. Man rechnet nach

$$\frac{w}{z} = \frac{w \cdot \overline{z}}{z \cdot \overline{z}} = \frac{(c + d \cdot i) \cdot (a - b \cdot i)}{(a + b \cdot i) \cdot (a - b \cdot i)} = \frac{ca + db}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2} \cdot i.$$

□

Die zu z konjugierte Zahl wird benötigt, um aus z die Größen $\mathrm{Re}(z)$, $\mathrm{Im}(z)$ und $|z|$ zu berechnen.

Lemma 15.4.4 (Berechnungen mittels $\overline{z}$)**.**

Für $z = a + ib$ gelten:

$$\mathsf{Re}(z) = a, \qquad \mathsf{Im}(z) = b \qquad \text{und} \qquad |z| = = \sqrt{a^2 + b^2}.$$

Beweis. Man rechnet nach

$$\mathsf{Re}(z) = \frac{z + \overline{z}}{2} = \frac{(a + i \cdot b) + (a - i \cdot b)}{2} = \frac{2a}{2} = a$$

$$\mathsf{Im}(z) = \frac{z - \overline{z}}{2i} = \frac{(a + i \cdot b) - (a - i \cdot b)}{2i} = \frac{2bi}{2i} = b$$

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{(a + i \cdot b) \cdot (a - i \cdot b)} = \sqrt{a^2 - (i \cdot b)^2} = \sqrt{a^2 + b^2}.$$

□

15.5. Polardarstellung komplexer Zahlen

Anstatt Real- und Imaginärteil einer komplexen Zahl z zu kennen, reicht es auch ihren Betrag r, d.h. den Abstand vom Ursprung und den Winkel α, den die Strecke vom Ursprung zu z mit der reellen Achse einschließt, zu kennen.

Definition 15.5.1.

Die *Polarkoordinaten* einer komplexen Zahl $z \in \mathbb{C} \setminus \{0\}$ bestehen aus dem Paar $(r, \alpha) \in \mathbb{R}^2$ mit

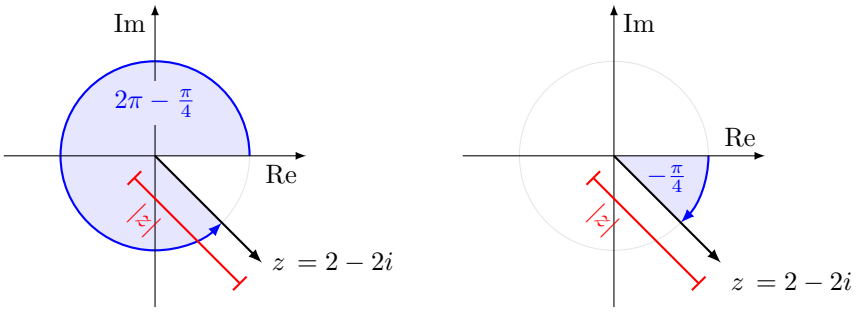
- Länge $r \geq 0$, d.h. $r := |z|$ und
- Winkel $\alpha \in \mathbb{R}$ so dass α äquivalent zu $\arg(z)$ ist, d.h. $\alpha = \arg(z) + k \cdot 2\pi$ mit $k \in \mathbb{Z}$.

Für $z = 0$ sind die Polarkoordinaten von der Form $(0, \alpha)$, dabei ist der Winkel α beliebig.

Beispiel 15.5.2.

Für die Zahl $z = 2 - 2i$ ist $|z| = 2 \cdot \sqrt{2}$ und $\arg(z) = 2\pi - \frac{\pi}{4}$.

Als Polarkoordinaten kommen beispielsweise in Frage: $(2\sqrt{2}\ ,\ 2\pi - \frac{\pi}{4})$ aber auch $(2\sqrt{2}\ ,\ -\frac{\pi}{4})$



Lemma 15.5.3 (Umrechnen von Polarkoordinaten in kartesische Koordinaten)**.**

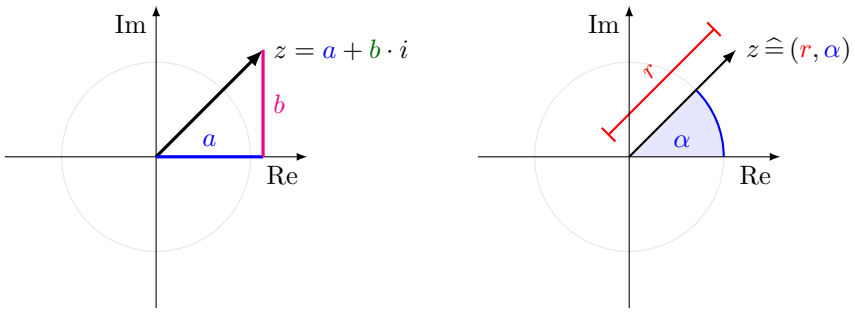
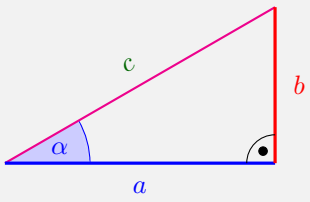


Abbildung 15.1.: Kartesische vs. Polarkoordinaten Darstellung einer komplexen Zahl

Liegt z in Polarkoordinaten $z \mathrel{\widehat{=}} (r, \alpha)$ vor, so gilt $z = r \cdot \cos(\alpha) + r \cdot \sin(\alpha) \cdot i$, d.h.

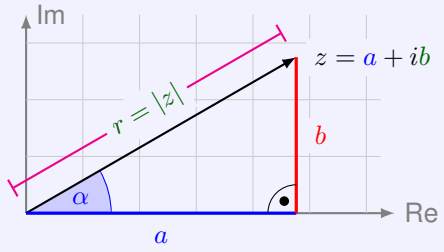
$$\begin{aligned} \mathsf{Re}(z) &= r \cdot \cos(\alpha) \\ \mathsf{Im}(z) &= r \cdot \sin(\alpha) \end{aligned}$$

Schulwissen: rechtwinkliges Dreieck



$$\cos(\alpha) = \frac{\text{Ankathete}}{\text{Hypothenuse}} = \frac{a}{c} \quad \Rightarrow \quad a = c \cdot \cos(\alpha)$$
$$\sin(\alpha) = \frac{\text{Gegenkathete}}{\text{Hypothenuse}} = \frac{b}{c} \quad \Rightarrow \quad b = c \cdot \sin(\alpha)$$

Komplexe Zahlen



$$\mathsf{Re}(z) = \quad a = r \cdot \cos(\alpha)$$
$$\mathsf{Im}(z) = \quad b = r \cdot \sin(\alpha)$$

Lemma 15.5.4 (Umrechnen von kartesischen Koordinaten in Polarkoordinaten)**.**

Sind die kartesischen Koordinaten $z = a + b \cdot i \neq 0$ bekannt, so können die zugehörigen Polarkoordinaten (r, α) wie folgt berechnet werden:

$$r = |z| = \sqrt{a^2 + b^2} \qquad \alpha = \begin{cases} \arccos\left(\frac{a}{r}\right) & \text{falls } b \geq 0 \\ -\arccos\left(\frac{a}{r}\right) & \text{falls } b < 0 \end{cases}$$

dabei ist $\arccos(x)$ die Umkehrfunktion des Cosinus.

15.5.1. Multiplizieren und Dividieren in Polarkoordinaten

Für zwei komplexe Zahlen ist die Multiplikation in Polarkoordinatendarstellung erheblich einfacher als in kartesischen Koordianten. Kurz gesagt gilt:

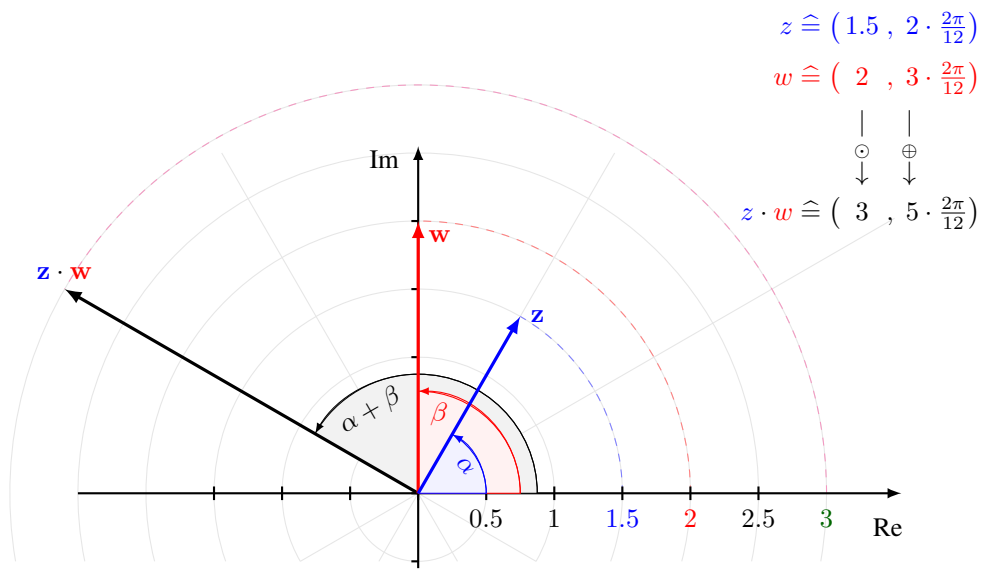
Längen werden multipliziert und Winkel werden addiert.

Lemma 15.5.5.

Es seien $z, w \in \mathbb{C}$ mit $z \mathrel{\widehat{=}} (r, \alpha)$ und $w \mathrel{\widehat{=}} (R, \beta)$. Dann gilt für das Produkt und den Quotienten:

$$z \cdot w \mathrel{\widehat{=}} (r \cdot R\ ,\ \alpha + \beta) \qquad \text{und} \qquad \frac{w}{z} \mathrel{\widehat{=}} \left(\frac{R}{r}\ ,\ \beta - \alpha\right)$$

Beispiel 15.5.6.

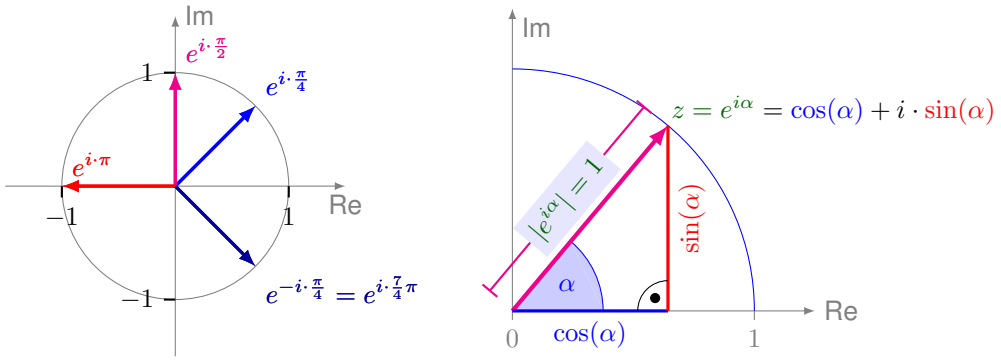


Den Beweis werden wir mit der Eulerschen Darstellung einer komplexen Zahl führen, dafür benötigen wir das Verhalten der Funktion e^x beim Einsetzen von rein komplexen Zahlen $i \cdot \alpha$:

Lemma 15.5.7.

Für $\alpha \in \mathbb{R}$ gilt stets $e^{i\cdot\alpha} = \cos(\alpha) + i \cdot \sin(\alpha)$. Insbesondere gelten: $e^{i\cdot\pi} = -1$ und $e^{i\cdot\frac{\pi}{2}} = i$

Die Zahl $e^{i\alpha}$ ist die Zahl auf dem Einheitskreis mit Winkel α:



Beweis. Die Taylorreihentwicklungen von $e^x, \cos(x)$ und $\sin(x)$ lauten:

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \dots \\ \cos(x) &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} \pm \dots \\ \sin(x) &= x - \frac{x^3}{3!} + \frac{x^5}{5!} \pm \dots \end{aligned}$$

Setzt man in e^x die Zahl $i \cdot \alpha$ ein so erhält man (wegen $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i, \dots$):

$$\begin{aligned} e^{i\alpha} &= 1 + i\cdot\alpha + i^2\cdot\frac{\alpha^2}{2!} + i^3\cdot\frac{\alpha^3}{3!} + i^4\cdot\frac{\alpha^4}{4!} + i^5\cdot\frac{\alpha^5}{5!} + \dots \\ &= 1 + i\cdot\alpha - \frac{\alpha^2}{2!} - i\cdot\frac{\alpha^3}{3!} + \frac{\alpha^4}{4!} + i\cdot\frac{\alpha^5}{5!} \pm \dots \Big\} = \Big\{ \cos(\alpha) + i\cdot\sin(\alpha) \end{aligned}$$

Es gilt also $e^{i\cdot\alpha} = \cos(\alpha) + i \cdot \sin(\alpha)$ □

Satz 15.5.8 (Eulerdarstellung)**.**

Für eine komplexe Zahl $z \in \mathbb{C}$ mit Polarkoordinaten $z \mathrel{\widehat{=}} (r, \alpha)$ gilt: $z = r \cdot e^{i\cdot\alpha}$

Umgekehrt gilt $r \cdot e^{i\cdot\alpha} \mathrel{\widehat{=}} (r, \alpha)$, d.h. $r \cdot e^{i\cdot\alpha}$ hat die Länge r und den Winkel α.

Beweis. Die Zahl $z \mathrel{\widehat{=}} (r, \alpha)$ lässt sich nach Lemma 15.5.3 schreiben als

$$z = r \cdot \cos(\alpha) + i \cdot r \cdot \sin(\alpha) = r \cdot \underbrace{(\cos(\alpha) + i \cdot \sin(\alpha))}_{e^{i\alpha}} ,$$

d.h. es gilt $z = r \cdot e^{i\alpha}$.

Für die Zahl $r \cdot e^{i\cdot\alpha}$ gilt:

$$\left|r \cdot e^{i\cdot\alpha}\right| = r \cdot |\cos(\alpha) + i\sin(\alpha)| = r \cdot \underbrace{\sqrt{\cos(\alpha)^2 + \sin(\alpha)^2}}_{=1}$$

Darüberhinaus hat $e^{i\cdot\alpha}$ nach Lemma 15.5.7 den Winkel α, und entsprechend hat $r \cdot e^{i\cdot\alpha}$ den Winkel α. □

Jetzt können wir Lemma 15.5.5 beweisen.

Beweis. [Beweis von Lemma 15.5.5.] Es gelten $z = r \cdot e^{i\cdot\alpha}$ und $w = R \cdot e^{i\cdot\beta}$ und es folgt:

$$z \cdot w = r \cdot e^{i\cdot\alpha} \cdot R \cdot e^{i\cdot\beta} = r \cdot R \cdot e^{i\cdot(\alpha+\beta)}$$

Die letzte Zahl hat offensichtlich den Betrag (Länge) $r \cdot R$ und den Winkel $\alpha + \beta$. Es gilt also

$$z \cdot w \mathrel{\widehat{=}} (r \cdot R, \alpha + \beta).$$

Für den Quotienten gilt aber

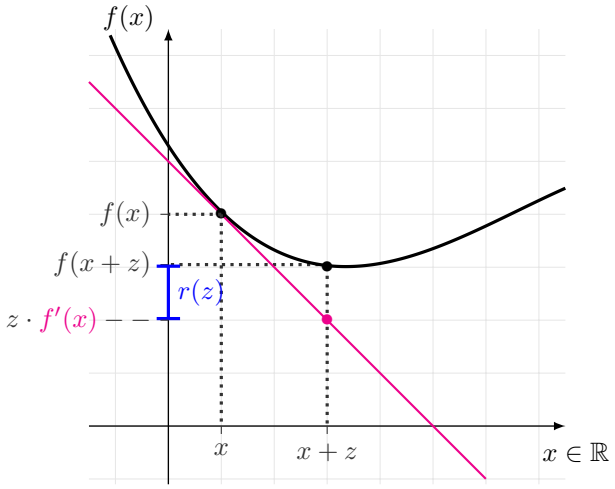
$$\frac{w}{z} = \frac{R \cdot e^{i\cdot\beta}}{r \cdot e^{i\cdot\alpha}} = \frac{R \cdot e^{i\cdot\beta}}{r} \cdot e^{-i\alpha} = \frac{R}{r} \cdot e^{i(\beta-\alpha)}.$$

Die letzte Zahl hat offensichtlich den Betrag (Länge) $\frac{R}{r}$ und den Winkel $\beta - \alpha$. Demnach gilt $\frac{w}{z} \mathrel{\widehat{=}} (\frac{R}{r}, \beta - \alpha)$.
□

16 Taylorentwicklung

Für eine Funktion $f : (a, b) \to \mathbb{R}$ haben wir gesehen, dass die Ableitung f' eine "lokale Approximation" von f durch eine lineare Funktion darstellt: Für $z \in \mathbb{R}$ ist

$$f(x + z) = f(x) + z \cdot f'(x) + r(z), \qquad \text{wobei } \lim_{z \to 0} r(z) = 0.$$



Es stellt sich die Frage, ob sich diese Approximation verbessern lässt. Dazu wiederholen wir den Vorgang des Ableitens, also des lokal-linear Approximierens, leiten also die Ableitung selbst wiederum ab.

16.1. Höhere Ableitungen

Konkreter ist die Ableitung, falls f auf dem gesamten Intervall (a, b) differenzierbar ist, eine Funktion $f' : (a, b) \to \mathbb{R}$. Diese Funktion ist nicht notwendigerweise differenzierbar (und in der Tat womöglich nicht einmal stetig). Aber wenn sie es ist, kann man sie wiederum differenzieren und erhält eine weitere Funktion $f'' : (a, b) \to \mathbb{R}$. Diese nennen wir die ***zweite Ableitung*** von f. Induktiv kann man auf diese Art selbstverständlich auch die dritte, vierte, ... Ableitung definieren. Allgemein bezeichnen wir die k***-te Ableitung*** von f durch $f^{[k]}$. Wir nennen f k***-mal stetig differenzierbar***, wenn die Ableitungen $f^{[1]}, \ldots, f^{[k]}$ existieren und $f^{[k]} : (a, b) \to \mathbb{R}$ eine stetige Funktion ist.

Also: Können wir mit Hilfe der höheren Ableitungen von f eine noch genauere lokale Approximation erhalten?

16.2. Das Taylorpolynom

Die Antwort ist ja! Dazu definieren wir Polynome, welche die Rolle der Approximation übernehmen.

Definition 16.2.1 ("Taylorpolynom")**.**

Sei $f : (a, b) \to \mathbb{R}$ eine k-mal differenzierbare Funktion und $x \in (a, b)$. Wir definieren das ***k*-te Taylorpolynom von *f* im Punkt** x als

$$t_k(y) = f(x) + \sum_{j=1}^{k} \frac{f^{[j]}(x)}{j!} \cdot y^j.$$

Bemerkung 16.2.2.

Wie man leicht nachrechnet gilt

$$t_k(0) = f(x), \qquad t_k^{[j]}(0) = f^{[j]}(x) \text{ für } 1 \leq j \leq k.$$

Mit anderen Worten: Die ersten k Ableitungen von t im Punkt 0 stimmen mit den ersten k Ableitungen von f im Punkt x überein.

Die folgende Aussage quantifiziert, wie gut das Taylorpolynom t die Funktion f approximiert.

Satz 16.2.3 ("Taylor-Formel")**.**

Angenommen die Funktion $f : (a, b) \to \mathbb{R}$ ist $(k+1)$-mal stetig differenzierbar. Sei t_k das k-te Taylorpolynom von f im Punkt $x \in (a, b)$, und sei $z \in (a, b)$. Dann gibt es ein $a \in [0, 1]$, so dass

$$f(z) = t_k(z - x) + \frac{f^{[k+1]}(y)}{(k+1)!} \cdot (z - x)^{k+1}, \qquad \text{wobei } y = (1 - a) \cdot x + a \cdot z.$$

Der Beweis der Taylor-Formel geht über den Rahmen dieser Vorlesung hinaus. Wir sehen stattdessen einige wichtige Beispiele.

16.3. Beispiele

16.3.1. Die Exponentialfunktion

Die Ableitung der Exponentialfunktion $exp(x)$ ist, einfach die Exponentialfunktion selbst, d.h. $exp'(x) = exp(x)$. Folglich ist die Exponen- tialfunktion k-mal differenzierbar für jede natürliche Zahl k; man sagt, sie ist beliebig oft differenzierbar. Ferner ist $exp(0) = 1$. Das k-te Taylorpolynom im Punkt $x = 0$ ist also

$$t_k(y) = \exp(0) + \sum_{j=1}^{k} \frac{\exp(0)}{j!} \cdot y^j = \sum_{j=0}^{k} \frac{y^j}{j!}$$

mit der Konvention, dass $y^0 = 1$ für alle y. Mit Satz 16.2.3 erhalten wir nun

Proposition 16.3.1.

Für jede reelle Zahl y gilt

$$\exp(y) = \sum_{j=0}^{\infty} \frac{y^j}{j!}.$$

Beweis. Satz 16.2.3 zeigt, dass für jedes $y \in \mathbb{R}$

$$\exp(y) = t_k(y) + r_k(y), \qquad \text{wobei}$$

$$r_k(y) = \frac{\exp(a_k \cdot y)}{(k+1)!} \dot{y}^{k+1}, \qquad \text{für ein } a_k \in [01].$$

Unser Ziel ist es zu zeigen, dass

$$\exp(y) = \lim_{k\to\infty} t_k(y).$$

Das bedeutet, wir müssen zeigen, dass

$$\lim_{k\to\infty} r_k(y) = 0. \tag{16.1}$$

Sei dazu ℓ die kleinste natürliche Zahl, die größer als $|y|$ ist. Dann können wir $r_k(y)$ für $k > \ell$ großzügig abschätzen durch

$$|r_k(y)| \le \exp(\ell) \cdot \frac{\ell^{k+1}}{(k+1)!} \le \exp(\ell) \cdot \ell^{\ell+1} \cdot \frac{\ell^{k-\ell}}{\prod_{j=\ell+1}^{k} j} = \frac{\exp(\ell) \cdot \ell^{\ell+1}}{\prod_{j=\ell+1}^{k} \frac{j}{\ell}}. \tag{16.2}$$

Der Zähler des letzten Ausdrucks ist unabhängig von k. Andererseits wird für große k der Nenner in (16.2) auch beliebig groß. Also folgt (16.1) aus (16.2). □

16.3.2. Die trigonometrischen Funktionen $\sin$ und $\cos$

Die trigonometrischen Funktionen $\sin$, $\cos$ lassen eine ganz ähnliche Reihenentwicklung zu. Weil

$$\sin'(x) = \cos(x) \qquad \text{und} \qquad \cos'(x) = -\sin(x),$$

erhalten wir

$$\cos^{[k]}(0) = \begin{cases} (-1)^{k/2} & \text{falls } k \text{ gerade ist,} \\ 0 & \text{falls } k \text{ ungerade ist.} \end{cases}$$

Das $2k$-te Taylorpolynom von $\cos(x)$ im Punkt 0 ist also

$$\sum_{j=0}^{k} \frac{(-1)^j}{(2j)!} \cdot y^{2j}.$$

Entsprechend erhält man

$$\sin^{[k]}(0) = \begin{cases} (-1)^{(k-1)/2} & \text{falls } k \text{ ungerade ist,} \\ 0 & \text{falls } k \text{ gerade ist.} \end{cases}$$

Das $(2k+1)$-te Taylorpolynom von $\sin(x)$ im Punkt 0 ist also

$$\sum_{j=0}^{k} \frac{(-1)^{2j+1}}{(2j+1)!} \cdot y^{2j+1}.$$

Proposition 16.3.2.

Für jede reelle Zahl y gilt

$$\cos(y) = \sum_{j=0}^{\infty} \frac{(-1)^j}{(2j)!} \cdot y^j, \qquad \sin(y) = \sum_{j=0}^{\infty} \frac{(-1)^j}{(2j+1)!} \cdot y^{2j+1}$$

Der Beweis von Proposition 16.3.2 beruht auf einem ähnlichem Argument wie der von Proposition 16.3.1; wir verzichten auf die Details. Die folgenden Abbildungen zeigen, wie die Taylorentwicklung uns immer bessere Approximationen an die Funktion $\cos(x)$ beschert. Dabei sind die Taylorpolynome $t_2(x), t_4(x)$ und $t_6(x)$ im Punkt 0 gezeichnet.