Mathematik II für Studierende der Informatik

Markus Junker (Mathematisches Institut, Universität Freiburg)

Sommersemester 2019 – Version von 18. September 2020

Inhaltsverzeichnis

Kapitel 0: Grundlagen

1 Voraussetzungen

Inhaltliche Voraussetzungen zum Verständnis des Skripts sind mathematische Grundkenntnisse z. B. aus der Vorlesung „Mathematik I für Studierende der Informatik und der Ingenieurwissenschaften“. Als Nachschlagewerk kann weitgehend meine „Einführung in Sprache und Grundbegriffe der Mathematik“ dienen.

Insbesondere wird Folgendes vorausgesetzt:

- Ein Grundverständnis der Zahlbereiche $\mathbb{N}$ (natürliche Zahlen einschließlich 0), $\mathbb{Z}$ (ganze Zahlen), $\mathbb{Q}$ (rationale Zahlen), $\mathbb{R}$ (reelle Zahlen) und $\mathbb{C}$ (komplexe Zahlen).
  Elementares Rechnen in diesen Zahlbereichen, einschließlich Rechnen mit Polynomen.
- Kenntnis des mathematischen Mengenbegriffs und der grundlegenden mengentheoretischen Operationen wie *Schnitt*, *Vereinigung*, *kartesisches Produkt*, *leere Menge*, *Teilmenge*, *Potenzmenge* ... sowie der zugehörigen Schreibweisen.
- Kenntnis des allgemeinen Relations- und Funktionsbegriffs und insbesondere des Konzepts einer Ordnungsrelation. Darstellung von Funktionen durch ihren Graph sowie grundlegende Konzepte wie *Bild*, *Urbild*, *injektiv*, *surjektiv*, *bijektiv* und zugehörige Notationen.
- Kenntnis von elementaren reellen Funktionen wie Sinus, Cosinus, Exponentialfunktion und Logarithmus.
- Kenntnis der Binärdarstellung ganzer Zahlen.
- Beweisprinzipien wie vollständige Induktion, Beweis durch Widerspruch etc.

2 Äquivalenzrelationen

binäre Relation

Definition 2.1 *Sei M eine Menge. Eine zweistellige Relation oder binäre Relation R auf M ist eine Eigenschaft von Paaren von Elementen von M. Sie wird üblicherweise mit ihrem* Graphen *identifiziert, d. h. mit der Teilmenge der Paare in $M^2 = M \times M$, auf die die Eigenschaft zutrifft. Eine binäre Relation auf M wird daher oft direkt als Teilmenge von M^2 definiert.*

Trifft R auf (a, b) zu, so schreibt man Rab oder auch aRb oder $(a, b) \in R$.

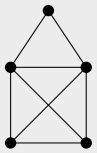
- Auf $M = \mathbb{N}$ sind die Ordnungsrelationen $<$, $\leqslant$, $>$ und $\geqslant$ Beispiele binärer Relationen.

  Es gilt etwa $2 < 3$, d. h. die durch $<$ ausgedrückte Eigenschaft „kleiner als“ trifft auf das Paar $(2, 3)$ zu. Dagegen gilt $2 < 2$ nicht, d. h. die „Kleiner-Eigenschaft“ trifft auf das Paar $(2, 2)$ nicht zu. Der Graph der Kleiner-Relation ist die Menge $\{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a < b\}$.

  Man kann zwar jede der vier Relationen auf einfache Weise aus jeder anderen gewinnen; es sind aber dennoch vier verschiedene Relationen.

- Ein weiteres Beispiel einer binären Relation auf $\mathbb{N}$ ist die *Teilbarkeitsrelation*, die mit einem senkrechten Strich $\mid$ bezeichnet wird: $a \mid b$ trifft genau dann zu, wenn die Zahl a die Zahl b ohne Rest teilt. Es gilt also zum Beispiel $3 \mid 15$, aber nicht $3 \mid 14$. Dafür schreibt man $3 \nmid 14$.

- Eine besondere Relation ist die *Gleichheits-* oder *Identitätsrelation* $=$, die auf genau diejenigen Paare zutrifft, deren beiden Komponenten gleich sind. Zu beachten ist hierbei, dass links und rechts des Gleichheitszeichens in der Regel nur Namen für Elemente stehen (z. B. Rechenausdrücke) und nicht die Elemente selbst. So gilt z. B. in den natürlichen Zahlen $3 + 5 = 8$, weil darin sowohl „$3 + 5$“ als auch „8“ Bezeichnungen desselben Elements sind. Betrachtet man dagegen Zeichenketten, arbeitet also beispielsweise im Monoid $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +\}^*$ (siehe Abschnitt 3.2), so sind „$3 + 5$“ und „8“ verschiedene Wörter über der gegebenen Symbolmenge, d. h. in diesem Fall hat man $3 + 5 \neq 8$.
- Ein *(ungerichteter) Graph* besteht aus einer Menge G von „Ecken“ (auch „Knoten“, engl. *vertices*), die teilweise durch „Kanten“ (engl. *edges*) verbunden sind. Zwei Ecken stehen in Kantenrelation E zueinander, wenn sie durch eine Kante verbunden sind.



Definition 2.2 *Eine binäre Relation R heißt* reflexiv, symmetrisch, transitiv

- *reflexiv, falls für alle $m \in M$ gilt, dass Rmm;*
- *symmetrisch, falls für alle $m_1, m_2 \in M$ aus Rm_1m_2 folgt, dass Rm_2m_1;*
- *transitiv, falls für alle $m_1, m_2, m_3 \in M$ aus Rm_1m_2 und Rm_2m_3 folgt, dass Rm_1m_3.*

Die oben betrachteten Relationen $=$, $\leqslant$, $\geqslant$ und $|$ sind reflexiv, $<$ und $>$ und die Kantenrelation E im Beispielgraph sind nicht reflexiv. ($<$ und $>$ sind sogar *irreflexiv*, d. h. es gilt nie $m < m$ bzw. $m > m$. Auch Graphen werden häufig so definiert, dass E irreflexiv ist.)

Gleichheits- und Kantenrelation sind symmetrisch, die anderen angegeben Beispiele nicht.

Alle betrachteten Relationen außer der Kantenrelation im Beispielgraph sind transitiv.

Definition 2.3 *Eine Äquivalenzrelation auf M ist eine reflexive, symmetrische und transitive binäre Relation auf M. Die Äquivalenzklasse (oder kurz: Klasse) von $m \in M$ bzgl. einer Äquivalenzrelation $\sim$ ist $m/_\sim := \{m' \in M \mid m \sim m'\}$.* Äquivalenzrelation und -klassen

Äquivalenzrelationen sind Relationen, die sich in gewisser Weise ähnlich wie die Gleichheitsrelation verhalten. Man wählt daher gerne dem Gleichheitszeichen ähnliche Symbole wie $\sim$, $\approx$, $\cong$, $\equiv$. Anstelle von $\sim$ wird in der Bezeichnung der Äquivalenzklassen natürlich immer das Zeichen eingesetzt, mit dem die jeweils betrachtete Äquivalenzrelation notiert wird.
Für die (Äquivalenz-)Klassen einer Äquivalenzrelation gibt es keine Standardnotation. Andere Schreibweisen sind $[m]_\sim$, $[\![m]\!]_\sim$, $[m]$ oder auch, falls die Äquivalenzrelation aus dem Zusammenhang bekannt ist, $[\![m]\!]$ oder $\overline{m}$.

Definition 2.4 *Eine Partition einer Menge M ist eine Menge paarweise disjunkter, nichtleerer Teilmengen („Blocks“) von M, die M überdecken (d. h. deren Vereinigung ganz M ist).* Partition

Lemma 2.5 *Die Äquivalenzklassen bilden eine Partition von M.*

Die Äquivalenzklassen von Elementen m, m' sind also entweder gleich (nämlich genau dann, wenn $m \sim m'$) oder disjunkt (wenn $m \not\sim m'$).

BEWEIS: Die Überdeckungseigenschaft von M folgt sofort aus der Reflexivität, da $m \in m/_\sim$.

Falls $m/_\sim$ und $m'/_\sim$ nicht disjunkt sind, gibt es ein $q \in m/_\sim \cap m'/_\sim$, für das also $m \sim q$ und $m' \sim q$ gilt. Mit Symmetrie und Transitivität von $\sim$ folgt daraus, dass $m \sim m'$. Sei nun $r \in m'/_\sim$, d. h. $m' \sim r$. Wiederum mit Transitivität ergibt sich daraus $m \sim r$, d. h. $r \in m/_\sim$, und somit $m'/_\sim \subseteq m/_\sim$. Da die Situation vollkommen symmetrisch in m und m' ist, gilt auch $m/_\sim \subseteq m'/_\sim$, also Gleichheit der Klassen. □

Umgekehrt liefert jede Partition von M eine Äquivalenzrelation, deren Äquivalenzklassen gerade die Blocks der Partition sind: Zwei Elemente sind genau dann äquivalent, wenn sie im selben Block liegen. Dies ist ein Spezialfall der folgenden Situation (mit N = Menge der Blocks):

Lemma 2.6 *Wenn $f : M \to N$ eine Abbildung ist, dann definiert*

$$m \sim_f m' : \iff f(m) = f(m')$$

eine Äquivalenzrelation $\sim_f$. Jede Äquivalenzrelation ist von dieser Form.

BEWEIS: Offensichtlich ist $\sim_f$ reflexiv, symmetrisch und transitiv, da die Gleichheitsrelation auf der rechten Seite der Definition von $\sim_f$ es ist.
Wenn umgekehrt $\sim$ eine Äquivalenzrelation auf M ist, nimmt man für N die Menge der Äquivalenzklassen von $\sim$ und für f die Abbildung, die jedem Element seine Äquivalenzklasse zuordnet, also $f(m) = m/_\sim$. Dann gilt: $m \sim m' \iff m/_\sim = m'/_\sim \iff f(m) = f(m')$. □

Jede Abbildung $f : M \to N$ zerlegt sich in drei Schritte:

	surjektiv		bijektiv		injektiv	
M	$\longrightarrow$	$M/_{\sim_f}$	$\longrightarrow$	$\mathrm{Bild}(f)$	$\longrightarrow$	N
m	$\mapsto$	$m/_{\sim_f}$	$\mapsto$	$f(m)$	$\mapsto$	$f(m)$

Im ersten Schritt werden also Blöcke in M zusammengefasst, im zweiten Schritt werden sie in Elemente von N „umbenannt“ und im dritten Schritt wird nur noch der Bildbereich auf ganz N erweitert.

Definition 2.7 *Eine Äquivalenzrelation $\approx$ auf M ist* feiner *als eine Äquivalenzrelation $\sim$ auf M, wenn jede Äquivalenzklasse von $\approx$ in einer Äquivalenzklasse von $\sim$ enthalten ist.*
(Äquivalente Definition: Für alle $m, m' \in M$ folgt aus $m \approx m'$ auch $m \sim m'$).

Alternative Sprechweisen sind: $\approx$ verfeinert $\sim$ bzw. $\sim$ ist gröber als $\approx$.

Bemerkung 2.8 Wenn $\sim_1$ und $\sim_2$ Äquivalenzrelation auf M sind, dann gibt es eine gröbste Äquivalenzrelation, die $\sim_1$ und $\sim_2$ verfeinert, und eine feinste Äquivalenzrelation, die gröber als $\sim_1$ und $\sim_2$ ist. Zudem ist die Identität die feinste aller Äquivalenzrelationen und die Äquivalenzrelation mit M als einziger Klasse die gröbste aller Äquivalenzrelationen auf M. Die Menge der Äquivalenzrelationen auf M bildet daher einen sogenannten *beschränkten Verband*.

Definition 2.9 *Sei $\sim$ eine Äquivalenzrelation auf M und $K \subseteq M$ eine Äquivalenzklasse. Ein Element $m \in K$ heißt Vertreter oder Repräsentant der Klasse K. Ein Vertreter- oder Repräsentantensystem von $\sim$ ist eine Teilmenge von M, die aus jeder Äquivalenzklasse von $\sim$ genau einen Vertreter enthält.*

Repräsentant, Repräsentantensystem

Ein in der Mathematik sehr häufiges Verfahren besteht darin, Äquivalenzklassen als neue mathematische Objekte einzuführen. Darin kann man einen Abstraktionsprozess sehen: Die Äquivalenzrelation drückt eine gemeinsame Eigenschaft aus; die Äquivalenzklasse steht für das jeweils Gemeinsame. Man kann etwa auf einer Menge von Gegenständen die Äquivalenzrelation „gleiche Form“ (oder „gleiche Farbe“) betrachten. Die Äquivalenzklassen entsprechen dann den Formen bzw. Farben, für die man u. U. noch keine Namen hat. In der Mathematik würde man dann die Äquivalenzklassen als die Formen bzw. Farben definieren.

Zusätzlich soll die Menge der Klassen einer Äquivalenzrelation oft zu einer mathematischen Struktur werden, indem sie z. B. eine binäre Operation $\circ$ der Ausgangsmenge „erbt“. Dafür gibt es zwei grundlegende Möglichkeiten:

- Man definiert für zwei Äquivalenzklassen K_1 und K_2 die Verknüpfung $K_1 \circ K_2$, indem man dafür die Äquivalenzklasse von $k_1 \circ k_2$ für beliebige Vertreter k_i von K_i nimmt. Dies funktioniert allerdings nur, wenn die Definition vertreterunabhängig (auch: wohldefiniert) ist, d. h. wenn das Ergebnis nicht von der Wahl der Vertreter abhängt.
- Man definiert die Relation wie oben, aber für Vertreter k_i aus einem ausgewählten Vertretersystem.

Während die erste Methode einen (bisweilen langwierigen) Beweis der Vertreterunabhängigkeit benötigt, hat man bei der zweite Methode oft mehr Arbeit, wenn man Eigenschaften der Operation nachweisen möchte. Ein bekanntes Beispiel soll dies alles verdeutlichen:

Die rationalen Zahlen $\mathbb{Q}$ können als Äquivalenzklassen von Paaren ganzer Zahlen eingeführt werden. Genauer betrachtet man auf der Menge $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ die Äquivalenzrelation

$$(m_1, n_1) \sim (m_2, n_2) : \Longleftrightarrow \; m_1 \cdot n_2 = m_2 \cdot n_1.$$

(Die Reflexivität der Relation sieht man sofort und die Symmetrie ist in die Definition eingebaut. Für die Transitivität muss man ein bisschen arbeiten: Wenn $m_1 \cdot n_2 = m_2 \cdot n_1$ und $m_2 \cdot n_3 = m_3 \cdot n_2$, folgt $m_1 \cdot n_2 \cdot m_2 \cdot n_3 = m_2 \cdot n_1 \cdot m_3 \cdot n_2$. Nun ist entweder $m_2 \neq 0$ und man kann beide Seiten durch $m_2 \cdot n_2$ kürzen und erhält die Transitivität. Oder es ist $m_2 = 0$, dann müssen aber $m_1 = m_3 = 0$ gelten und die Transitivität folgt ebenfalls.) Die Äquivalenzklasse von (m, n) entspricht dabei dem Bruch $\frac{m}{n}$. Ein Beispiel für ein Vertretersystem ist $\{(m, n) \mid n > 0, m \text{ und } n \text{ teilerfremd}\}$, was der gekürzten Darstellung von Brüchen mit positivem Nenner entspricht.

Wenn man nun die Addition von Brüchen defineren will, kann man dies mit Hilfe des positiven größten gemeinsamen Teilers ggT auf diesem Vertretersystem tun durch

$$(m, n) + (m', n') := \left(\frac{mn' + m'n}{\mathrm{ggT}(mn' + m'n, nn')}, \frac{nn'}{\mathrm{ggT}(mn' + m'n, nn')} \right)$$

oder auf beliebigen Repräsentanten durch

$$(m, n) + (m', n') := (mn' + m'n, nn').$$

Letzteres ist als Definition viel einfacher, aber überhaupt nur sinnvoll, wenn das Ergebnis nicht von der Wahl der Repräsentanten abhängt. Dies bedeutet: Falls $(m_1, n_1) \sim (m_2, n_2)$ und $(m_1', n_1') \sim (m_2', n_2')$, dann muss $(m_1, n_1) + (m_1', n_1') \sim (m_2, n_2) + (m_2', n_2')$ gelten.

Man kann in diesem Beispiel leicht nachrechnen, dass dies stimmt: Denn nach Voraussetzung ist $m_1 n_2 = m_2 n_1$ und $m_1' n_2' = m_2' n_1'$. Also ist

$$\begin{aligned}(m_1 n_1' + m_1' n_1) \cdot n_2 n_2' &= m_1 n_1' n_2 n_2' + m_1' n_1 n_2 n_2' \\ &= m_2 n_2' n_1 n_1' + m_2' n_2 n_1 n_1' = (m_2 n_2' + m_2' n_2) \cdot n_1 n_1'\end{aligned}$$

Andererseits sieht man mit der zweiten Definition schnell, dass

$$\big((m,n) + (m',n')\big) + (m'',n'') = \cdots = (mn'n'' + nm'n'' + nn'm'', nn'n'')$$

also dass die Addition assoziativ ist, da der rechte Ausdruck symmetrisch in den drei Summanden ist. Mit der ersten Definition ist dies etwa mühsamer.

2.1 Erste Annäherung an Vektorräume

Vektoren stellen eine mathematische Modellisierung gewisser Aspekte zunächst der Ebene bzw. des 3-dimensionalen Raumes dar. In der Schule werden Vektoren häufig als gerichtete Strecken („Pfeile“) – in der Ebene oder im Raum – eingeführt. Solch eine gerichtete Strecke ist durch zwei Punkte, den Anfangs- und den Endpunkt, bestimmt. Auf diesen gerichteten Strecken möchte man zwei Operationen betrachten: die Hintereinandersetzung („Addition“) und die Streckung bei Beibehaltung des Anfangspunkts („Skalarmultiplikation“). Während man die Streckung für beliebigen Strecken betrachten kann, funktioniert die Hintereinandersetzung nur, wenn der Endpunkt der ersten Strecke der Anfangspunkt der zweiten ist. Andernfalls müsste man die zweite Strecke so verschieben, dass dies stimmt. Daher betrachtet man als Pfeile die „gerichteten Strecken modulo Parallelverschiebung“, d. h. man definiert zwei gerichtete Strecken als „gerichtet parallel“, wenn sie durch eine Parallelverschiebung (der Ebene bzw. des Raumes) ineinander übergehen. Dies ist eine Äquivalenzrelation und die Vektoren („Pfeile“) sind die Äquivalenzklassen, auf denen man nun die beiden Operationen einführen kann, die repräsentanten-unabhängig sind.

Alternativ kann man ein Reporäsentantensystem wählen, indem man einen beliebigen Punkt als Urspung wählt und nur gerichtete Strecken betrachtet, die von diesem Punkt ausgehen.

Schließlich kann man die Ebene bzw. den Raum noch „koordinatisieren“ und erhält dadurch eine algebraische Beschreibung der Strecken durch die Koordianten der Endpunkte. Dies wird der Zugang in dieser Vorlesung sein.

[*wird noch etwas ausgeführt...*]

3 Grundlegende algebraische Strukturen

3.1 Strukturen und Operationen

Informelle Definition: Eine algebraische Struktur besteht aus einer nicht-leeren Grundmenge M mit einer oder mehreren *Operationen/ Verknüpfungen*[1], die typischerweise gewisse „schöne“ Eigenschaften haben. Die Operationen können *innere Operationen* sein, das sind Funktionen/Abbildungen[1] $M^n \to M$, oder *äußere Operationen*, dies sind z. B. Abbildungen der Art $R \times M \to M$ für eine feste Struktur R, etwa den Körper $\mathbb{R}$ der reellen Zahlen. Außerdem können in einer Struktur bestimmte Elemente durch feste Namen benannt sein (solche Elemente heißen auch „*Konstanten*“).

Bei inneren Operation $\alpha : M^n \to M$ heißt n die *Stelligkeit* der Operation. Es ist also $\alpha : M \to M$ eine *einstellige* oder *unäre* Operation, $\alpha : M^2 \to M$ eine *zweistellige* oder *binäre* Operation; $\alpha : M^3 \to M$ eine *dreistellige* oder *ternäre* Operation, usw. Der mathematische Formalismus erlaubt es auch, *nullstellige* Operationen $\alpha : M^0 \to M$ zu betrachten, Da $M^0 = \{\emptyset\}$ eine einelementige Menge ist, kann man eine nullstellige Operation mit dem Bild dieses Elementes, also mit einer Konstanten identifizieren.

In den wichtigen mathematischen Strukturen werden in der Regel ein- und zweistellige Operationen sowie Konstanten betrachtet. Drei- und höherstellige Operationen, die nicht aus einfacheren Operationen zusammengesetzt sind, kommen selten vor.

1. Die Struktur $(\mathbb{Z}, +)$: Hier bilden die ganzen Zahlen $M = \mathbb{Z}$ die Grundmenge; die Addition „$+$“ : $M \times M \to M$ ist darauf eine zweistellige innere Operation.
2. Die Struktur $(\mathbb{Z}, \cdot, 1)$: die ganzen Zahlen $M = \mathbb{Z}$ mit der Multiplikation „$\cdot$“ : $M \times M \to M$ und der Konstanten 1 als ausgezeichnetem Element.
3. Die Struktur $(\mathbb{Z}, +, \cdot)$: Hier betrachtet man die ganzen Zahlen $\mathbb{Z}$ mit zwei zweistelligen Operationen (Addition und Multiplikation) gleichzeitig.
4. Die Menge der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ als Grundmenge M mit der zweistelligen Operation „$\circ$“, d. h. der Hintereinanderausführung von Funktionen, als zweistelliger innerer Operation.
5. Die Menge $M = A^*$ aller Wörter über einem Alphabet A. Wörter sind endliche Folgen von Symbolen. Eine zweistellige Verknüpfung auf A^* ist die *Konkatenation*, das Hintereinanderschreiben zweier Wörter.

Definition 3.1 *Folgende wichtige Eigenschaften von zweistelligen Operationen* $\circ : M^2 \to M$ *und* $* : M^2 \to M$ *werden wir betrachten:*

kommutativ
assoziativ
distributiv
neutrales Elem.
inverses Elem.

- $\circ$ *heißt kommutativ, wenn für alle* $m_1, m_2 \in M$ *gilt:*

$$m_1 \circ m_2 = m_2 \circ m_1$$

- $\circ$ *heißt assoziativ, wenn für alle* $m_1, m_2, m_3 \in M$ *gilt:*

$$m_1 \circ (m_2 \circ m_3) = (m_1 \circ m_2) \circ m_3$$

[1] Diese Begriffe benutzte ich jeweils synonym.

- $\circ$ *heißt distributiv über* $*$*, wenn für alle* $m_1, m_2, m_3 \in M$ *gilt:*

  $$m_1 \circ (m_2 * m_3) = (m_1 \circ m_2) * (m_1 \circ m_3) \text{ und } (m_2 * m_3) \circ m_1 = (m_2 \circ m_1) * (m_3 \circ m_1)$$

- $\circ$ *besitzt ein neutrales Element, falls es ein* $n \in M$ *gibt, so dass für alle* $m \in M$ *gilt:*

  $$n \circ m = m \circ n = m$$

- *Falls* $\circ$ *ein neutrales Element* $n \in M$ *besitzt, so heißt* $m' \in M$ *inverses Element (oder kurz: Inverses) von* $m \in M$ *(bezüglich* $\circ$*), falls*

  $$m \circ m' = m' \circ m = n$$

  Das Element m *heißt invertierbar, falls es ein Inverses besitzt.*

Die zweistelligen Operationen in den Beispielen 1, 2 sind kommutativ, in 4 und 5 nicht; alle vier sind assoziativ. Im Beispiel 3 ist $\cdot$ distributiv über $+$; die Zahl 0 ist neutrales Element bezüglich der Addition und die Zahl 1 neutrales Element bezüglich der Multiplikation. Im Beispiel 4 ist die identische Abbildung $\mathrm{id}_{\mathbb{R}}$ neutrales Element bezüglich der Komposition; die Funktion $x \mapsto \frac{1}{2}x$ ist inverses Element der Funktion $x \mapsto 2x$.

Wichtige Strukturen sind Vektorräume (engl. *vector spaces*), Gruppen (*groups*), Ringe (*rings*) und Körper (*fields*). Diese werden nun in den weiteren Kapiteln Thema sein: Vektorräume vor allem in Kapitel I, die anderen Strukturen in Kapitel II der Vorlesung.

3.2 Monoide

Definition 3.2 *Ein Monoid besteht aus einer nicht-leeren Grundmenge* M *mit einer assoziativen, zweistelligen Verknüpfung* $\circ$ *, die ein neutrales Element* $e \in M$ *besitzt. Ein Monoid* $(M, \circ)$ *heißt kommutatives Monoid, wenn die Verknüpfung* $\circ$ *zusätzlich kommutativ ist.* Monoid

„Monoid“ ist sächlich („das Monoid“) und wird „Mono-id“ mit Betonung auf der letzten Silbe ausgesprochen. Die Zeichen $\circ$ und e stehen als Platzhalter für die Verknüpfung und ein festes Element; in einem konkreten Monoid können dafür andere Zeichen stehen, etwa $+$ und 0 im Monoid $(\mathbb{N}, +)$ der natürlichen Zahlen bezüglich der Addition oder $\cdot$ und 1 im Monoid $(\mathbb{N}, \cdot)$ der natürlichen Zahlen bezüglich der Multiplikation.

Lemma 3.3 *Das neutrale Element* e *ist eindeutig bestimmt, denn eine beliebige binäre Operation kann nicht zwei oder mehrere neutrale Elemente haben.*

Beweis: Falls e und e' neutrale Elemente der Verknüpfung $\circ$ sind, so gilt $e = e \circ e'$, da e' neutrales Element ist, und $e \circ e' = e'$, da e neutrales Element ist, zusammen also $e = e'$. □

Verschiedene Operationen haben dagegen in der Regel auch unterschiedliche neutrale Elemente. So sind die natürlichen Zahlen $\mathbb{N}$ sowohl bezüglich der Addition ein Monoid – mit neutralem Element 0 – als auch bezüglich der Multiplikation – mit neutralem Element 1.

- Die natürlichen Zahlen $\mathbb{N}$ bilden mit der Addition $+$ ein kommutatives Monoid mit neutralem Element 0.
- Die natürlichen Zahlen $\mathbb{N}$ bilden mit der Multiplikation $\cdot$ ein kommutatives Monoid mit neutralem Element 1.
- Die echt positiven natürlichen Zahlen $\mathbb{N} \setminus \{0\}$ bilden mit der Multiplikation $\cdot$ ein kommutatives Monoid mit neutralem Element 1.
- Die Abbildungen $\mathrm{Abb}(A, A)$ einer Menge A in sich selbst bilden unter der Komposition $\circ$, d. h. der Hintereinanderausführung von Abbildungen, ein Monoid, dessen neutrales Element die identische Abbildung id_A ist. Wenn A mindestens zwei Elemente $a \neq b$ besitzt, ist diese Monoid nicht kommutativ, wie man an den konstanten Abbildungen $x \mapsto a$ und $x \mapsto b$ sieht, die nicht miteinander vertauschen.
- Wenn A eine Menge ist (in diesem Kontext auch *Alphabet* genannt), bildet die Menge A^* der endlichen Folgen von Elementen aus A (die „*Wörter über A*“) mit der *Konkatenation* (d. h. dem Hintereinandersetzen) $\frown$ ein Monoid. Mit $A = \{a, b, c\}$ ist also z. B. $abaac \frown ccb = abaacccb$. Das neutrale Element ist das *leere Wort*, d. h. die Folge der Länge 0, das oft mit λ oder ε bezeichnet wird. Wenn A mindestens zwei Elemente enthält, ist A^* nicht kommutativ.
- Die echt positiven natürlichen Zahlen $\mathbb{N} \setminus \{0\}$ bilden mit der Addition $+$ kein Monoid, da es kein neutrales Element gibt.
- Die natürlichen Zahlen $\mathbb{N}$ bilden mit der Exponentiation kein Monoid, da die Exponentiation nicht assoziativ ist, denn z. B. ist $2^{(3^2)} = 2^9 = 512$, aber $(2^3)^2 = 8^2 = 64$. Zudem gibt es zwar ein „rechtsneutrales Element“ (da $n^1 = n$ für alle $n \in \mathbb{N}$), aber kein „linksneutrales Element“.

Bemerkungen zur notationellen Bezeichnung einer Struktur: Wenn die Menge M mit der Verknüpfung $\circ$ ein Monoid bildet, schreibt man dafür üblicherweise $(M, \circ)$ oder manchmal $(M, \circ, e)$, wenn man das durch die Verknüpfung ja festgelegte neutrale Element hervorheben möchte. Wenn man sauber arbeitet, unterscheidet man notationell zwischen der Struktur und der zugrundeliegenden Menge und schreibt dann gerne für die Struktur den entsprechenden Buchstaben in einem anderen Schriftart, also z. B. $\mathcal{M}$ oder $\mathfrak{M}$ für ein Monoid mit Grundmenge M. Oft erlaubt man sich aber die notationelle Unsauberkeit, für die Struktur und die Grundmenge das gleiche Symbol (hier z. B. M) zu verwenden.

Bei der Angabe eines Monoids entfällt bisweilen die Angabe der Verknüpfung, wenn aus dem Kontext heraus offensichtlich ist, welche gemeint ist, oder wenn es eine besonders natürliche Verknüpfung gibt. Wenn man z. B. vom Monoid der Wörter über einem Alphabet spricht oder dem Monoid der Abbildungen einer Menge in sich selbst, meint man die oben angegebenen Standardbeispiele. Das doppelte Beispiel der natürlichen Zahlen – einmal mit Addition und einmal mit Multiplikation – zeigt aber, dass man i. a. auf die Angabe der Verknüpfung nicht verzichten kann. Hier wäre es angebracht, etwa $\mathcal{N}_+$ für das Monoid $(\mathbb{N}, +)$ und $\mathcal{N}_\times$ für das Monoid $(\mathbb{N}, \cdot)$ zu schreiben.

Wenn mehrere (abstrakte) Monoide gleichzeitig betrachtet werden, werden oft die gleichen Symbole für die Verknüpfungen und die neutralen Elemente gebraucht. Es kann also vorkommen, dass man Monoide $(M, \circ, e)$ und $(N, \circ, e)$ betrachtet. Zur Verdeutlichung schreibt man dann manchmal $\circ_M$ für Verknüpfung und e_M für das neutrale Element von M und analog $\circ_N$ und e_N für die Verknüpfung und das neutrale Element von N.

Analoge Bemerkungen zur Notation gelten für alle weiteren betrachteten algebraischen Strukturen!

Lemma 3.4 (a) *Wenn $(M, \circ)$ ein Monoid ist und m ein invertierbares Element ist, dann ist seine Inverses eindeutig bestimmt und wird m^{-1} geschrieben.*

(b) *Sind $m, m_1, m_2 \in M$ invertierbare Elemente, dann sind auch m^{-1} und $m_1 \circ m_2$ invertierbar und es gilt:*

$$(m^{-1})^{-1} = m \quad \textit{und} \quad (m_1 \circ m_2)^{-1} = (m_2^{-1}) \circ (m_1^{-1})$$

Per Konvention soll die einstellige Operation $^{-1}$ stärker binden als das zweistellige $\circ$.
Es ist also $m_1 \circ m_2^{-1}$ als $m_1 \circ (m_2^{-1})$ zu lesen und nicht als $(m_1 \circ m_2)^{-1}$.

Beweis: (a) Sind m' und m'' beides Inverse zu m, so gilt

$$m' = m' \circ e = m' \circ (m \circ m'') = (m' \circ m) \circ m'' = e \circ m'' = m''$$

(b) Wegen $m \circ m^{-1} = e = m^{-1} \circ m$ ist m ein Inverses zu m^{-1} und wegen

$$(m_1 \circ m_2) \circ (m_2^{-1} \circ m_1^{-1}) = \cdots = m_1 \circ e \circ m_1^{-1} = \cdots = e$$

und analog $(m_2^{-1} \circ m_1^{-1}) \circ (m_1 \circ m_2) = e$ ist $m_2^{-1} \circ m_1^{-1}$ Inverses zu $m_1 \circ m_2$. □

Mit der im nächsten Abschnitt eingeführten Definition wird man sehen, dass die invertierbaren Elemente in einem Monoid also eine Gruppe bilden.

Bemerkungen zur Schreibweise iterierter Verknüpfungen: Wegen der Assoziativität kann man in einem Monoid bei iterierten Verknüpfungen Klammern weglassen, falls es nur auf das Ergebnis der Berechnung ankommt. Im einfachsten Fall steht also $m_1 \circ m_2 \circ m_3$ gleichermaßen für $(m_1 \circ m_2) \circ m_3$ und $m_1 \circ (m_2 \circ m_3)$, da beide Ausdrücke das gleiche Ergebnis liefern, also das gleiche Element im Monoid bezeichnen.
Entsprechend kann man eine beliebige größere Anzahl n von Monoid-Element $m_i \in M$ verknüpfen zu $m_1 \circ \cdots \circ m_n$. Für $n = 3$ ist dies also genau $m_1 \circ m_2 \circ m_3$, für $n = 4$ ist es $m_1 \circ m_2 \circ m_3 \circ m_4$, etc. Der Ausdruck $m_1 \circ \cdots \circ m_n$ soll aber für alle n eine Bedeutung haben. Für kleine n sind zunächst analoge Bildungen gemeint: Falls $n = 2$, steht der Ausdruck für $m_1 \circ m_2$, falls $n = 1$ einfach für m_1. Schließlich bleibt der Fall $n = 0$: Man kann sich überlegen, dass die einzig sinnvolle Auswertung des Ausdrucks $m_1 \circ \cdots \circ m_n$ im Fall $n = 0$ das neutrale Element e ist; man kann dies aber auch als eine Konvention sehen. Wichtig ist in beiden Sichtweisen, dass erst dadurch Rechengesetze wie

$$(m_1 \circ \cdots \circ m_k) \circ (m_{k+1} \circ \cdots \circ m_n) = m_1 \circ \cdots \circ m_n$$

für alle $k = 0, 1, \ldots, n, n+1$ gelten!
Statt $m_1 \circ \cdots \circ m_n$ schreibt man auch $\bigcirc_{i=1}^{n} m_i$ mit einem „großen“ Verknüpfungssymbol $\bigcirc$. Falls die Verknüpfung als Summe $+$ oder Produkt $\cdot$ geschrieben wird, nimmt man für das „große Verknüpfungssymbol“ in der Regel $\sum$ bzw. $\prod$.

3.3 Gruppen

Definition 3.5 *Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist, d. h. eine Gruppe besteht aus einer nicht-leeren Grundmenge G und einer zweistelligen Verknüpfung $\circ$ auf G (der „Gruppenoperation“), die* Gruppe

- assoziativ *ist,*

- *ein* neutrales Element $e \in G$ *besitzt*
- *und bezüglich der es* inverse Elemente *gibt, d. h. zu jedem* $g \in G$ *gibt es ein Element* $h \in G$ *mit* $h \circ g = g \circ h = e$.

Eine Gruppe $(G, \circ)$ *heißt kommutative Gruppe*[2]*, wenn die Verknüpfung* $\circ$ *auch* kommutativ *ist.*

Das bezüglich der Gruppenoperation zu $g \in G$ inverse Element ist nach Lemma 3.4 eindeutig bestimmt und wird im Allgemeinen mit g^{-1} bezeichnet. Es gibt für Gruppen allerdings mehrere gebräuchliche Notationen:

	Verknüpfung	neutrales Element	inverses Element
allgemein:	$\circ$	e	g^{-1}
multiplikativ:	$\cdot$	1	g^{-1}
additiv:	$+$	0	$-g$

Die additive Schreibweise ist im allgemeinen kommutativen Gruppen vorbehalten. Bei der multiplikativen Schreibweise lässt man den Multiplikationspunkt auch gerne weg. In konkreten Gruppen kann die Gruppenverknüpfung natürlich auch mit einem anderen Symbol bezeichnet sein, ebenso das neutrale Element und die Inversenabbildung

- $(\mathbb{Z}, +, 0)$ ist kommutative Gruppe.
- $(\mathbb{Q}, +, 0)$, $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ und $(\mathbb{Q}^{>0}, \cdot, 1)$ mit $\mathbb{Q}^{>0} = \{q \in \mathbb{Q} \mid q > 0\}$ sind kommutative Gruppen.
- $(\mathbb{R}, +, 0)$, $(\mathbb{R} \setminus \{0\}, \cdot, 1)$ und $(\mathbb{R}^{>0}, \cdot, 1)$ mit $\mathbb{R}^{>0} = \{r \in \mathbb{R} \mid r > 0\}$ sind kommutative Gruppen.
- $(\mathbb{C}, +, 0)$ und $(\mathbb{C} \setminus \{0\}, \cdot, 1)$ sind kommutative Gruppen.
- Ein wichtiges Beispiel einer Gruppe ist die *verallgemeinerte Uhren-Arithmetik*, d. i. die kommutative Gruppe $\mathbb{Z}_m = \big(\{0, \ldots, m-1\}, +_m, 0\big)$, wobei

  $$x +_m y := \text{Rest von } x + y \text{ bei Division durch } m = \begin{cases} x + y & \text{falls } x + y < m \\ x + y - m & \text{falls } x + y \geqslant m \end{cases}$$

  (Für $n = 12$ rechnet man auf diese Art mit Uhrzeiten: „*8 Uhr + 5 Stunden = 1 Uhr*“).
- $(\mathrm{Sym}(A), \circ, \mathrm{id})$ ist eine Gruppe, die symmetrische Gruppe über A. Hierbei bezeichnet $\mathrm{Sym}(A)$ die Menge der Permutationen von A, d. h. der Bijektionen von einer Menge A in sich selbst, und $\circ$ ist die Komposition von Abbildungen. Wenn A mindestens drei Elemente enthält, ist die symmetrische Gruppe über A nicht kommutativ.
- Die triviale Gruppe besteht nur aus einem Element, ihrem neutralen Element. Genau genommen gibt es viele verschiedene Realisierungen der trivialen Gruppe: Zum Beispiel besteht $(\mathbb{Z}_1, +_1)$ nur aus einem Element und auch $\mathrm{Sym}(A)$ für eine einelementige Menge A. Alle diese Realisierungen sind aber untereinander *isomorph*, d. h. (informell) nur verschiedene Bezeichnungen für dieselbe Gruppe. Die mathematische Präzisierung der „Isomorphie“ folgt in Teil II.

[2] oder auch Abelsche Gruppe, nach dem norwegischen Mathematiker Niels Henrik Abel (1802–1829)

- Ist $(M, \circ, 1)$ ein Monoid, dann bildet die Menge M^* der in M invertierbaren Menge nach Lemma 3.4 eine Gruppe.
- Zu jeder Struktur M gibt es die Automorphismengruppe $\mathrm{Aut}(M)$, welche aus den „strukturerhaltenden“ Permutationen von M besteht mit der Komposition von Funktionen als Gruppenoperation. Was genau „strukturerhaltend“ bedeutet, wird noch an Beispielen klar werden.

Die folgenden Strukturen sind keine Gruppen:

- $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$, denn kein Element außer 1 und -1 hat ein Inverses.
- $(\mathbb{Q}, \cdot, 1)$, denn 0 hat kein Inverses.

Die Gruppentafel ist eine Tabelle, in der alle möglichen Verknüpfungen zweier Elemente der Gruppe aufgeführt sind. Eine Gruppe ist kommutativ, wenn die Gruppentafel mit der Diagonale von links oben nach rechts unten eine Symmetrieachse besitzt. Bei nicht-kommutativen Gruppen muss man klarstellen, in welcher Reihenfolge die Verknüpfung in der Tabelle aufzufassen ist.

- Zu $\mathbb{Z}_4$ ist die Gruppentafel:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Allgemeiner kann man natürlich für jede zweistellige Verküpfung solch eine Verknüpfungstafel aufstellen. Wenn man etwas das Monoid $\mathrm{Abb}(A, A)$ für die zwei-elementige Menge $A = \{a, b\}$ betrachtet, so besteht $\mathrm{Abb}(A, A)$ aus den folgenden vier Abbildungen: $\mathrm{id}_A : x \mapsto x$, $c_a : x \mapsto a$, $c_b : x \mapsto b$ und $\tau : a \mapsto b, b \mapsto a$. Hierfür ist die Verküpfungstafel:

$\circ$	id_A	c_a	c_b	τ
id_A	id_A	c_a	c_b	τ
c_a	c_a	c_a	c_a	c_a
c_b	c_b	c_b	c_b	c_b
τ	τ	c_b	c_a	id_A

  mit der Konvention, dass in der Tafel $f \circ g$ dargestellt ist, wobei f in der ersten Spalte und g in der obersten Zeile angegeben ist. Dieses Monoid ist nicht kommutativ, was man an der fehlenden Symmetrie der Verküpfungstafel sieht. Daher ist es wichtig anzugeben, in welcher Reihenfolge die Verküpfung aufzufassen ist.
- Die kleinste nicht-kommutative Gruppe ist $\mathrm{Sym}(B)$ für eine drei-elementige Menge B. diese Gruppe hat sechs Elemente. Als Übung kann man die Gruppentafel aufstellen.

Man sieht bei genauerem Hinschauen, dass manche der in den Beispielen angegebenen Gruppen von einfachen Beispielen für Monoide herstammen. Diese Monoide wurden so verändert, dass sie auch die

Anforderungen an Gruppen erfüllen. Man kann zum einen versuchen, fehlende inverse Elemente hinzuzunehmen (Beispiel: Konstruktion von $(\mathbb{Z}, +)$ aus $(\mathbb{N}, +)$). Dies ist aber nicht immer möglich. Manchmal genügt es dann, wenige störende Elemente wegzulassen (Beispiel: Konstruktion von $(\mathbb{Q}^{>0}, \cdot)$ aus $(\mathbb{N}, \cdot)$ unter Weglassen der Null). Zum andern erhält man manchmal aus Monoiden interessante Gruppen, indem man die Elemente herausgreift, die bereits Inverse haben (Beispiel: $\mathrm{Sym}(A)$ in $\mathrm{Abb}(A, A)$).

Zur Zahl 0 in $(\mathbb{N}, \cdot)$ kann man kein inverses Element hinzunehmen, ohne die Assoziativität aufzugeben. Denn gäbe es in einer Erweiterung ein Element 0^{-1}, müsste z. B.

$$1 = 0 \cdot 0^{-1} = (2 \cdot 0) \cdot 0^{-1} = 2 \cdot (0 \cdot 0^{-1}) = 2 \cdot 1 = 2$$

gelten.

Ähnlich sieht man bei Abbildungen, dass es kein (Links-)Inverses für h geben kann, wenn $h \circ g_1 = h \circ g_2$ für $g_1 \neq g_2$ gilt, und kein (Rechts-)Inverses, wenn $g_1 \circ h = g_2 \circ h$ gilt.

3.4 Ringe

Definition 3.6 *Ein Ring besteht aus einer nicht-leeren Menge R, zwei zweistelligen Verknüpfungen $\oplus$ und $\otimes$ auf R und Elementen e_+ und $e_\times$, für die gilt:* Ring

- $(R, \oplus, e_+)$ *ist eine kommutative Gruppe;*
- $(R, \otimes, e_\times)$ *ist ein Monoid;*
- $\otimes$ *ist distributiv über* $\oplus$*, d. h. es gelten die* Distributivgesetze*:*

$$\begin{aligned}(r_1 \oplus r_2) \otimes s &= (r_1 \otimes s) \oplus (r_2 \otimes s)\\ s \otimes (r_1 \oplus r_2) &= (s \otimes r_1) \oplus (s \otimes r_2)\end{aligned} \qquad \text{für alle } r_1, r_2, s \in R$$

Ein Ring $(R, \oplus, \otimes)$ heißt kommutativer Ring, wenn $\otimes$ zusätzlich kommutativ *ist.*

Genauer handelt es sich hier um *Ringe mit Eins* oder *unitäre Ringe*. Es gibt ein allgemeineres Konzept von Ring, bei dem es kein neutrales Element der Multiplikation zu geben braucht. Bei der Lektüre anderer Skripte oder Bücher muss man daher vorsichtig sein, da eine andere Definition benutzt sein könnte.

In einem kommutativen Ring folgt natürlich jedes der Distributivgesetze aus dem anderen.

> In der Regel schreibt man $+$ und $\cdot$ für die Verknüpfungen $\oplus$ und $\otimes$ und nennt sie Addition und Multiplikation und schreibt 0 und 1 für die Elemente e_0 und e_1 und nennt sie Null und Eins. Das werde ich von nun an so tun!
>
> Zur Ersparnis von Klammern führt man die üblichen „Vorfahrtsregel“ *Punkt vor Strich* ein. Außerdem lässt man den Multiplikationspunkt gerne weg. Das erste Distributivgesetz kann man also kurz als $(r_1 + r_2)s = r_1 s + r_2 s$ schreiben.

Aus den Axiomen für Ringe ergibt sich, dass $r \cdot 0 = 0 \cdot r = 0$ für alle $r \in R$ ist. Denn es gilt $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$. Also ist

$$0 = r \cdot 0 + (-(r \cdot 0)) = r \cdot 0 + r \cdot 0 + (-(r \cdot 0)) = r \cdot 0 + 0 = r \cdot 0,$$

und analog für die vertauschte Reihenfolge.

Ähnlich sieht man, dass $(-r) \cdot s = r \cdot (-s) = -(r \cdot s)$ für alle $r, s \in R$ gilt. Auch hier kann man daher Klammern einsparen und krz $-rs$ schreiben.

Vorsicht: Nicht alle aus dem Ring der ganzen Zahlen vertrauten Rechenregeln gelten in beliebigen Ringen. Zum Beispiel gilt im Ring $\mathbb{Z}_6$ (siehe in den folgenden Beispielen) $2 \cdot_6 3 = 0$, ohne dass $2 = 0$ oder $3 = 0$ gelten würde.

- Die Definition verbietet nicht, dass $0 = 1$ ist. In diesem Fall folgt aber $r = r \cdot 1 = r \cdot 0 = 0$ für alle $r \in R$, und es liegt der sogenannte triviale Ring vor, der nur aus einem einzigen Element besteht.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind – jeweils mit der üblichen Addition und Multiplikation – kommutative Ringe.
- Die Gruppe $\mathbb{Z}_m$ (siehe Beispiele zu 3.3) kann durch eine analog definierte Multiplikation $\cdot_m$ zu einem kommutativen Ring gemacht werden: $x \cdot_m y$ rechnet man dadurch aus, dass man von dem normalen Produkt in $\mathbb{Z}$ den Rest bei der Division durch m nimmt, also solange m abzieht, bis man im Bereich $\{0, \dots, m-1\}$ landet.
- Die Polynome mit Koeffizienten in einem Ring R und der Unbekannten X bilden mit der bekannten Polynomaddition und -multiplikation den Polynomring $R[X]$.
  Also z. B. $\mathbb{R}[X]$: Polynome mit einer Unbekannten X und Koeffizienten in $\mathbb{R}$,
  oder $\mathbb{Z}[X]$: Polynome mit einer Unbekannten X und Koeffizienten in $\mathbb{Z}$.

  Nimmt man mit einer neuen Unbekannten Y z. B. den Polynomring $\mathbb{R}[X]$ als Koeffizientenbereich, erhält man den Polynomring mit zwei Unbekannten X und Y mit Koeffizienten in $\mathbb{R}$, also $\mathbb{R}[X][Y] = \mathbb{R}[X, Y]$.

3.5 Körper

Definition 3.7 *Ein Körper ist ein nicht-trivialer, kommutativer Ring, in dem jedes Element* $\neq 0$ *multiplikativ invertierbar ist. Das heißt, ein Körper besteht aus einer nicht-leeren Menge* K*, zwei zweistelligen Verknüpfungen* $+$ *und* $\cdot$ *auf* K *(Addition und Multiplikation) und Elementen* 0 *und* 1 *(Null und Eins), für die gilt:* Körper

- $0 \neq 1$
- $(K, +, 0)$ *und* $(K \setminus \{0\}, \cdot, 1)$ *sind kommutative Gruppen*[3]
- *die Multiplikation ist distributiv über der Addition*

Die in der Definition ab „das heißt“ beschriebenen Eigenschaften sind äquivalent zur Definition: Mit der gleichen Rechnung wie bei Ringen zeigt man, dass $0 \cdot k = 0$ für alle $k \in K$ ist. Damit sieht man, dass die Multiplikation auf ganz K assoziativ ist und 1 als neutrales Element hat, d. h. dass $(K, \cdot, 1)$ ein kommutatives Monoid ist.

- $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit der üblichen Addition und Multiplikation sind Körper.

[3] Es gibt auch das allgemeineres Konzept eines *Schiefkörper*, bei dem die Multiplikation nicht kommutativ zu sein braucht.

- Für Primzahlen p ist $\mathbb{Z}_p$ mit den definierten Operationen $+_m$ und $\cdot_m$ ein Körper und wird dann oft mit $\mathbb{F}_p$ bezeichnet.
- $\mathbb{R}(x)$ ist der Körper der rationalen Funktionen über $\mathbb{R}$,

$$\mathbb{R}(x) = \left\{ \frac{P(x)}{Q(x)} \,\middle|\, P, Q \in \mathbb{R}[x], Q \neq 0 \right\}.$$

Besonders interessant für die Informatik ist der Körper $\mathbb{F}_2$, der aus den beiden Elementen 0 und 1 besteht mit folgenden Verknüpfungen:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Kapitel I: Lineare Algebra

4 Vektorräume

4.1 Definition

Sei K ein Körper, also z. B. $K = \mathbb{R}$ oder $K = \mathbb{F}_2$ (dies werden die hauptsächlichen Beispiele in dieser Vorlesung sein).

Definition 4.1 *Ein K-Vektorraum V besteht aus einer nicht-leeren Menge V zusammen mit einer zweistelligen inneren Verknüpfung $+ : V \times V \to V$ (der Addition) und einer äußeren Verknüpfung $\cdot : K \times V \to V$ (der Skalarmultiplikation), für die gilt:* Vektorraum

- *$(V, +, 0)$ ist eine kommutative Gruppe mit neutralem Element 0*
- *und es gelten folgende Regeln für die Skalarmultiplikation:*[4]

(K1)	$(k_1 +_K k_2) \cdot v = (k_1 \cdot v) +_V (k_2 \cdot v)$	(V1)	$k \cdot (v_1 +_V v_2) = (k \cdot v_1) +_V (k \cdot v_2)$
(K2)	$0_K \cdot v = 0_V$	(V2)	$k \cdot 0_V = 0_V$
(K3)	$(-_K k) \cdot v = -_V (k \cdot v)$	(V3)	$k \cdot (-_V v) = -_V (k \cdot v)$
(K4)	$(k_1 \cdot_K k_2) \cdot v = k_1 \cdot (k_2 \cdot v)$		
(K5)	$1_K \cdot v = v$		

für alle $k, k_1, k_2 \in K$ und $v, v_1, v_2 \in V$.

Elemente von V heißen Vektoren, Elemente von K Skalare. Falls der Körper K aus dem Kontext bekannt ist, spricht man auch kurz von „Vektorraum“ statt von „K-Vektorraum“.

Für jede Operation und Konstante im Körper bzw. Vektorraum gibt es in der Definition eine Regel für die Skalarmultiplikation, die etwas über Vertauschbarkeit von den Operationen aussagt (in gewisser Weise also aussagt, wie ein verschachtelter Term „auszurechnen“ ist). Lediglich eine Regel für $(k^{-1}) \cdot v$ fehlt, weil es auf V keine multiplikative Struktur gibt.

Lemma 4.2 *Die Regeln* (K2), (K3), (V2), (V3) *in der Definition einer k-Vektorraums folgen bereits aus den restlichen Teilen der Definition.*

Beweis: Es gilt $0 \cdot v = (0 + 0) \cdot v = (0 \cdot v) + (0 \cdot v)$. Da $(V, +)$ eine Gruppe ist, folgt daraus $0 = 0 \cdot v$, denn man kann $-(0 \cdot v)$ auf beiden Seiten addieren. Mit der gleichen Begründung folgt aus $k \cdot 0 = k \cdot (0 + 0) = (k \cdot 0) + (k \cdot 0)$ auch $0 = k \cdot 0$.
Weiter gilt nun $((-k) \cdot v) + (k \cdot v) = ((-k) + k) \cdot v = 0 \cdot v = 0$. Aus der Eindeutigkeit von Inversen in Gruppen folgt daraus $(-k) \cdot v = -(k \cdot v)$. Mit der gleichen Begründung folgt aus $(k \cdot (-v) + k \cdot v = k \cdot (v + (-v)) = k \cdot 0 = 0$ auch $k \cdot (-v) = -(k \cdot v)$. □

[4] Zur Verdeutlichung sind vorübergehend die Operationen und die Konstanten 0 und 1 im Körper K mit einem Index K gekennzeichnet, also $+_K, -_K, \cdot_K, 0_K, 1_K$, und die Operationen und die Konstante 0 in der Gruppe $(V, +)$ mit einem Index V, also $+_V, -_V, 0_V$.

In Vektorräumen benutzt man die gleichen notationellen Kurzformen wie bei Ringen: *Punkt vor Strich* als Klammersparregeln und Weglassen des Multiplikationspunktes.

Multiplikationen sind entweder Multiplikationen zwischen Skalaren (und ergeben ein Skalar) oder die Skalarmultiplikation zwischen einem Skalar auf der linken Seite des Produkts und einem Vektor auf der rechten Seite (und ergeben einen Vektor). In einem allgemeinen Vektorraum gibt es keine Multiplikation zwischen Vektoren. [5]

Bis auf das Symbol 0, was alleine stehend für die Null im Körper und für die Null im Vektorraum (den *Nullvektor*) stehen kann, ist bei allen anderen Ausdrücken auch ohne die Indizes K und V klar, welche Operationen und welche Art von Objekt – Skalar oder Vektor – beschrieben ist.

Insbesondere sind die folgenden Ausdrücke zwischen Skalaren k und Vektoren v, v_1, v_2 *nicht* definiert: $k + v$, $v + k$, $v_1 \cdot v_2$, $v \cdot k$, 1_V, v^{-1}.

- $\mathbb{R}^n$, also die Menge der n-Tupel reeller Zahlen, ist ein $\mathbb{R}$-Vektorraum mit komponentenweiser Addition und Skalarmultiplikation. Dann ist also

$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$$
$$r \cdot (r_1, \ldots, r_n) = (r \cdot r_1, \ldots, r \cdot r_n)$$

  Für Vektoren $r \in \mathbb{R}^n$ gibt es zwei Standardschreibweisen:

  – als Zeilenvektor $(r_1, r_2, \ldots, r_n)$ oder $(r_1\ r_2\ \ldots\ r_n)$
  (Die Kommata dienen nur der Lesbarkeit und haben keine Bedeutung.)

  – als Spaltenvektor $\begin{pmatrix} r_1 \\ r_2 \\ \ldots \\ r_n \end{pmatrix}$

  Beides sind nur verschiedene Schreibweisen desselben Objekts. In den kommenden Abschnitten wird es aber, abhängig von der Situation, günstiger sein, die eine oder die andere Variante zu wählen.

  Außerdem ist es üblich, die Komponenten (auch Einträge oder Kooordinaten) eines Vektors r mit $r_1, \ldots, r_n$ zu bezeichnen, also dem gleichen Buchstaben mit den Indizes $1, \ldots, n$. Dies wird oft implizit angenommen.

- Spezialfälle hiervon:

  Für $n = 2$ erhält man die *koordinatisierte reelle Ebene*: Wenn man zwei verschiedene Koordinatenachsen in der Ebene wählt, kann man jeden Punkt der Ebene mit dem Paar (x, y) seiner Koordinaten identifizieren.

  Für $n = 3$ erhält man analog den *koordinatisierten reellen Raum*: Die Wahl dreier nicht in einer Ebene liegender Koordinatenachsen erlaubt es, jeden Punkt des Raumes mit dem Tripel (x, y, z) seiner Koordinaten identifizieren.

  Für $n = 1$ erhält man die *koordinatisierte reelle Gerade*: Die Wahl des Koordinatensystems reduziert sich in diesem Fall auf die Wahl des Ursprungs und des Maßstabes.

[5] In speziellen Fällen gibt es allerdings auch Vektorprodukte.

Ein Element von $\mathbb{R}^1$, also ein 1-Tupel (r) mit $r \in \mathbb{R}$, kann man mit der reellen Zahl r identifizieren.[6] In diesem Fall sind also Vektorraum und Skalarenkörper gleich.

Für $n = 0$ erhält man den einelementigen Vektorraum $\mathbb{R}^0 = \{0\}$.

- Allgemeiner kann man Folgen reeller Zahlen betrachten, also den $\mathbb{R}$-Vektorraum $\mathbb{R}^\infty := \{(r_0, r_1, r_2, \dots) \mid r_i \in \mathbb{R}\}$, ebenfalls mit komponentenweisen Operationen, also

$$(r_0, r_1, r_2, \dots) + (s_0, s_1, s_2, \dots) = (r_0 + s_0, r_1 + s_1, r_2 + s_2, \dots)$$
$$r \cdot (r_0, r_1, r_2, \dots) = (r \cdot r_0, r \cdot r_1, r \cdot r_2, \dots)$$

- Die Polynome mit Koeffizienten aus $\mathbb{R}$ bilden ebenfalls einen $\mathbb{R}$-Vektorraum mit der üblichen Addition und der Skalarmultiplikation $r \cdot \sum_{i=1}^n r_i X^i = \sum_{i=1}^n (r \cdot r_i) X^i$. Wenn man Skalare mit konstanten Polynomen identifiziert, ist dies gewissermaßen ein Teil der Ringstruktur auf $\mathbb{R}[X]$.

- All die bisherigen Beispiele funktionieren für beliebige Körper, d. h. für jeden Körper K erhält man K-Vektorräume K^n, K^∞, $K[X]$ mit den gleichen Konventionen an Notationen.

- Da $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$ ist, kann man jeden $\mathbb{C}$-Vektorraum auch als $\mathbb{R}$-Vektorraum betrachten, indem man die Skalarmultiplikation auf reelle Skalare einschränkt. Insbesondere ist $\mathbb{C}$ selbst sowohl $\mathbb{C}$-Vektorraum als auch $\mathbb{R}$-Vektorraum. Als $\mathbb{R}$-Vektorraum kann man ihn mit $\mathbb{R}^2$ identifizieren („Gaußsche Zahlenebene“).

- $\mathbb{R}$ ist dagegen *kein* $\mathbb{F}_2$-Vektorraum. $\mathbb{R}$ enthält zwar ebenfalls Elemente 0 und 1 wie $\mathbb{F}_2$; diese verhalten sich aber in $\mathbb{F}_2$ anders als in $\mathbb{R}$ (d. h. $\mathbb{F}_2$ ist kein Teil- oder Unterkörper von $\mathbb{R}$), denn $1_{\mathbb{F}_2} +_{\mathbb{F}_2} 1_{\mathbb{F}_2} = 0_{\mathbb{F}_2}$, aber $1_{\mathbb{R}} +_{\mathbb{R}} 1_{\mathbb{R}} \neq 0_{\mathbb{R}}$.

  So gilt z. B. $2\sqrt{2} = (1 \cdot \sqrt{2}) +_{\mathbb{R}} (1 \cdot \sqrt{2}) \neq (1 +_{\mathbb{F}_2} 1) \cdot \sqrt{2} = 0 \cdot \sqrt{2} = 0$.

4.2 Untervektorräume

In diesem Abschnitt sei V stets ein K-Vektorraum.

Definition 4.3 *$U \subseteq V$ heißt K-Untervektorraum von V, falls U unter den eingeschränkten Operationen selbst ein K-Vektorraum ist. Man schreibt dafür $U \leqslant V$.*

Untervektorraum

Wenn der Körper K durch den Kontext bekannt ist, sagt man auch kurz „Untervektorraum“ statt „K-Untervektorraum“. Außerdem verkürzt man bisweilen „Untervektorraum“ zu „Unterraum“.

Nach Definition ist also U ein K-Untervektorraum von V, falls $0 \in U$ und für alle $u, u_1, u_2 \in U$ und $k \in K$ die Elemente $u_1 + u_2$, $-u$ und $k \cdot u$ in U liegen und falls alle Vektorraum-Axiome erfüllt sind.

Lemma 4.4 *U ist genau dann ein Untervektorraum von V, wenn U eine nicht-leere, bezüglich Addition und Skalarmultiplikation abgeschlossene Teilmengen von V ist.*

Beweis: Man kann sich leicht davon überzeugen, dass sich Regeln wie Assoziativität, Kommutativität und Distributivität auf Teilmengen übertragen, ebenso die Neutralität von 0, falls 0

in der Teilmenge liegt. Die Abgeschlossenheit einer Teilmenge bezüglich Negation folgt aus der Abgeschlossenheit bezüglich der Skalarmultiplikation, da $-u = (-1) \cdot u$. Wenn $U \neq \emptyset$, etwa $u \in U$, folgt auch $0_V = 0_K \cdot u \in U$. □

Sei $K = \mathbb{R}$ und $V = \mathbb{R}^2$. Die $\mathbb{R}$-Untervektorräume von V sind dann:

- der triviale Untervektorraum $\{0_V\}$;
- alle Teilmengen der Form $\{(x, y) \in \mathbb{R}^2 \mid ax + by = 0\}$ für feste $a, b \in \mathbb{R}$ – dies sind die Geraden durch den Ursprung $(0, 0)$;
- der ganze Vektorraum $\mathbb{R}^2$.

Keine Untervektorräume sind:

- Die Punkte eines Kreises bilden keinen Untervektorraum des $\mathbb{R}^2$ (weder abgeschlossen unter Addition, noch unter Skalarmultiplikation).
- Die Fläche zwischen zwei sich schneidenden Geraden ist kein Untervektorraum des $\mathbb{R}^2$ (abgeschlossen unter Skalarmultiplikation, aber nicht unter Addition).
- Die Punkte mit ganzzahligen Koordinaten, also das „Gitter“ $\mathbb{Z}^2$ (abgeschlossen unter Addition, aber nicht unter Skalarmultiplikation).

Satz 4.5 *Der Schnitt von beliebig vielen K-Untervektorräumen von V ist wieder ein K-Untervektorraum von V.*

Beweis: Man prüft leicht anhand der Definition nach, dass dies gilt. Falls zum Beispiel $u, v \in \bigcap_{i \in I} U_i$ für Untervektorräume U_i, so sind $u, v \in U_i$ für alle $i \in I$, also ist auch $u + v \in U_i$ für alle $i \in I$ und mithin $u + v \in \bigcap_{i \in I} U_i$. Analog für die anderen Eigenschaften. □

Definition 4.6 *Sei $X \subseteq V$. Der von X in V erzeugte Untervektorraum $\langle X \rangle$ (oder kurz: das Erzeugnis von X) ist der Schnitt aller Untervektorräume von V, die X enthalten. Wegen dem vorangehenden Satz ist dies der bezüglich Inklusion kleinste Untervektorraum von V, der X enthält.* Erzeugnis

Notationen und Sprechweisen Für $\langle \{v_i \mid i \in I\} \rangle$ schreibt man auch kurz $\langle v_i \mid i \in I \rangle$ und für $\langle \{v_1, \ldots, v_n\} \rangle$ kurz $\langle v_1, \ldots, v_n \rangle$. Ist $V = \langle v_i \mid i \in I \rangle$, so sagt man

- die v_i $(i \in I)$ „erzeugen V“ oder
- die v_i $(i \in I)$ „sind Erzeuger oder Erzeugende von V“ oder
- $\{v_i \mid i \in I\}$ „ist ein Erzeugendensystem von V“

oder Varianten hiervon. V heißt endlich erzeugt, falls es ein endliches Erzeugendensystem gibt.

Definition 4.7 *Sei $X \subseteq V$. Eine Linearkombination von X ist ein Ausdruck der Form* Linear-kombination

$$k_1 x_1 + \cdots + k_n x_n$$

mit $n \in \mathbb{N}$, $k_i \in K$ und $x_i \in X$. Die Linearkombination heißt nicht trivial, *wenn mindestens ein k_i nicht null ist.*

Konvention: Falls X unendlich ist, soll für Ausdrücke $\sum_{x\in X} k_x x$ gelten, dass alle k_x bis auf endlich viele null sind und die Summe nur über die endlich vielen $k_x x$ gebildet wird, für die $k_x \neq 0$ ist. Damit bezeichnet $\sum_{x\in X} k_x x$ also eine Linearkombination von X.

Eine unendliche Summe ergibt in einem beliebigen Vektorraum keinen Sinn, da es aus der Definition heraus keine Möglichkeit gibt, eine solche Summe zu bilden. Falls es sich um einen $\mathbb{R}$- oder $\mathbb{C}$-Vektorraum handelt, könnte man zwar versuchen, eine unendliche Summe als den Grenzwert einer Reihe zu verstehen, das soll hier aber nicht betrachtet werden.

Satz 4.8 *Der von $X \subseteq V$ erzeugte Untervektorraum besteht aus allen durch Linearkombinationen von X beschriebenen Elemente von V. Insbesondere ist*

$$\langle v_1, \dots, v_n\rangle = \{k_1 v_1 + \dots + k_n v_n \mid k_1, \dots, k_n \in K\}$$

Beweis: Da jeder Untervektorraum unter Summen und Skalarmultiplikation abgeschlossen ist, enthält er mit $v_1, \dots, v_n$ auch jedes durch eine Linearkombination von $v_1, \dots, v_n$ gegebene Element. Dies gilt also insbesondere für das Erzeugnis einer $v_1, \dots, v_n$ enthaltenden Menge. Also gilt die Inklusion „$\supseteq$“ im Satz.

Für die umgekehrte Inklusion „$\subseteq$“ reicht es zu sehen, dass die Menge der durch Linearkombinationen von X beschriebenen Elemente unter Addition und Skalarmultiplikation abgeschlossen ist und alle Elemente von X enthält. Letzteres gilt, da $x = 1 \cdot x$, die Abgeschlossenheit, da

$$\sum_{x\in X} k_x x + \sum_{x\in X} k'_x x = \sum_{x\in X} (k_x + k'_x)x$$
$$k \cdot \sum_{x\in X} k_x x = \sum_{x\in X} (k \cdot k_x)x$$

□

Falls $X = \emptyset$ ist nach Definition $\langle\emptyset\rangle = \{0\}$. Der Satz stimmt auch in diesem Fall, da der Wert der „leeren Summe“ $\sum_{x\in\emptyset} k_x x$ als 0 definiert wird.

- $(1,0,0), (0,1,0), (0,0,1)$ erzeugen $\mathbb{R}^3$, da sich jedes Element $(x,y,z) \in \mathbb{R}^3$ schreiben lässt als $x \cdot (1,0,0) + y \cdot (0,1,0) + z \cdot (0,0,1)$.
- Ebenso ist $(-1,0,0), (0,2,0), (0,0,1), (1,1,1)$ ein Erzeugendensystem von $\mathbb{R}^3$.
- $(0,1,0), (0,0,2), (0,3,-2)$ dagegen erzeugen einen echten Untervektorraum von $\mathbb{R}^3$, nämlich $\{(0,r,s) \mid r,s \in \mathbb{R}\}$.
- Die Folgen $(1,0,0,0,\dots), (0,1,0,0,\dots), (0,0,1,0,\dots), \dots$ erzeugen einen echten Untervektorraum von $\mathbb{R}^\infty$, nämlich den Untervektorraum der Folgen von endlichem Träger. Das sind Folgen $(r_0, r_1, r_2, \dots)$, bei denen alle r_i bis auf endlich viele null sind.

4.3 Lineare Unbhängigkeit

Sei wieder stets V ein K-Vektorraum, und sei $X \subseteq V$ eine Menge von Vektoren.

Definition 4.9 *Ein Vektor $v \in V$ ist linear abhängig von X, falls $v \in \langle X\rangle$, d. h. falls es $x_1, \dots, x_n \in X$ und $k_1, \dots, k_n \in K$ gibt mit $v = k_1 x_1 + \dots + k_n x_n$.* linear unabhängig

X ist linear unabhängig, falls kein $x \in X$ linear abhängig von $X \setminus \{x\}$ ist.

Satz 4.10 *Eine Menge von unendlich vielen Vektoren ist genau dann linear unabhängig, wenn jede endliche Teilmenge linear unabhängig ist.*

Beweis: Folgt unmittelbar aus der Definition. □

Vorsicht vor den Tücken der Mengenschreibweise bei Doppelnennungen:
Angenommen die Menge $\{v_1, v_2\}$ ist linear unabhängig und $v_2 = v_3$. Dann ist $\{v_1, v_2, v_3\} = \{v_1, v_2\}$ linear unabhängig, aber v_3 ist linear abhängig von $\{v_1, v_2\}$. Dies liegt daran, dass hier $\{v_1\} = \{v_1, v_2, v_3\} \setminus \{v_3\} \neq \{v_1, v_2\}$. Diese Schwierigkeit wird mit der folgenden Definition umgangen.

Menge ohne Doppelnennungen

Definition 4.11 $\{v_i \mid i \in I\}$ *heißt* Beschreibung einer Menge ohne Doppelnennungen*, falls* $v_i \neq v_j$ *für* $i \neq j$*, also falls die Elemente* v_i *für* $i \in I$ *paarweise verschieden sind.*

Anders ausgedrückt: die Abbildung $I \to V$*,* $i \mapsto v_i$ *ist injektiv, oder, noch einmal anders ausgedrückt,* $v_j \notin \{v_i \mid i \in I \setminus \{j\}\}$ *für alle* $j \in I$*.*

Der Kürze halber spreche ich von „Menge ohne Doppelnennungen“, obwohl es sich nicht um eine Eigenschaft der Menge, sondern ihrer Beschreibung handelt.

Im endlichen Fall ist also genau dann $\{v_1, \ldots, v_n\}$ eine Menge ohne Doppelnennungen, wenn sie n Elemente enthält.

Satz 4.12 $\{v_1, \ldots, v_n\}$ *ist genau dann linear unabhängig und ohne Doppelnennungen, wenn nur die triviale Linearkombination von* $v_1, \ldots, v_n$ *Null ergibt, d. h. wenn* $k_1 v_1 + \cdots + k_n v_n = 0$ *nur für* $k_1 = 0, \ldots, k_n = 0$ *gilt.*

Beweis: Wenn die Menge linear abhängig ist oder Doppelnennungen vorliegen, gilt etwa $v_1 \in \langle v_2, \ldots, v_n \rangle$ (sonst Umindizieren!), also $(-1) \cdot v_1 + k_2 v_2 + \cdots + k_n v_n = 0$.

Wenn es umgekehrt eine Darstellung $k_1 v_1 + \cdots + k_n v_n = 0$ gibt, bei der etwa $k_1 \neq 0$, so folgt $v_1 = -\frac{k_2}{k_1} v_2 + \cdots + (-\frac{k_n}{k_1}) v_n$, also ist entweder $v_1 \in \{v_2, \ldots, v_n\}$ und es gibt Doppelnennungen oder die Menge $\{v_1, \ldots, v_n\}$ ist linear abhängig. □

Aus diesem Satz folgt unmittelbar eine allgemeine Version auch für unendliche Mengen:

Satz 4.13 *Eine Menge* $\{v_i \mid i \in I\}$ *ist genau dann linear unabhängig und ohne Doppelnennungen, wenn aus* $\sum_{i \in I} k_i v_i = 0$ *folgt, dass alle* $k_i = 0$ *sind, wenn also in diesem Sinne keine nicht-triviale Linearkombination Null ergibt.*

Definition 4.14 *Eine Basis eines Vektorraums* V *ist ein linear unabhängiges Erzeugendensystem.*

Satz 4.15 $\{v_i \mid i \in I\}$ *ist eine Basis von* V
$\iff$ $\{v_i \mid i \in I\}$ *ist eine maximale linear unabhängige Teilmenge von* V
$\iff$ $\{v_i \mid i \in I\}$ *ist ein minimales Erzeugendensystem von* V

(„maximal“ und „minimal“ sind bezüglich der Teilmengenbeziehung)

Beweis: Sei zunächst $B = \{v_i \mid i \in I\}$ eine Basis. Da B linear unabhängig ist, gilt für jedes $b \in B$, dass $b \notin B \setminus \{b\}$, also ist keine echte Teilmenge von B ein Erzeugendensystem

von V. Da umgekehrt B Erzeugendensystem von V ist, gilt für beliebiges $v \in V \setminus B$, dass $v \in \langle B \rangle = \langle (B \cup \{v\}) \setminus \{v\} \rangle$, also ist keine echte Obermenge $B \cup \{v\}$ von B linear unabhängig.

Sei nun B maximal linear unabhängig und $v \in V \setminus B$. Dann ist $B \cup \{v\}$ linear abhängig, also existiert eine nicht-triviale Linearkombination $k_1 v_1 + \cdots + k_n v_n + kv = 0$ mit paarweise verschiedenen $v_i \in B$. Es kann nicht $k = 0$ sein, da sonst eine nicht-triviale Linearkombination von Elementen von B null wäre, im Widerspruch zur linearen Unabhängigkeit von B, also ist $v = -\frac{k_1}{k} v_1 + \cdots + -\frac{k_n}{k} v_n \in \langle B \rangle$ und B ist Erzeugendensystem.

Sei nun B minimales Erzeugendensystem und $b \in B$. Dann it $b \notin \langle B \setminus \{b\} \rangle$, mithin ist B linear unabhängig. □

Satz 4.16 *Jeder endlich erzeugte Vektorraum besitzt Basen; jedes endliche Erzeugendensystem enthält eine Basis und jede linear unabhängige Teilmenge lässt sich zu einer Basis vergrößern.*

Beweis: Die erste und die zweite Aussage folgen unmittelbar aus dem vorigen Satz, da sich ein endliches Erzeugendensystem zu einem minimalen Erzeugendensystem verkleinern lässt. Ist eine linear unabhängige Teilmenge X gegeben und ein endliches Erzeugendensystem E, so ist auch $X \cup E$ ein Erzeugendensystem. Nun kann keine echte Teilmenge X' von X ein Erzeugendensystem sein, weil X' sonst als linear unabhängiges Erzeugendensystem zwar eine Basis wäre, aber nicht maximal linear unabhängig. Also muss es unter den Teilmengen Y mit $X \subseteq Y \subseteq X \cup E$ ein minimales Erzeugendensystem geben, das also eine Erweiterung von X zu einer Basis darstellt. □

Dieser Satz gilt auch für unendlich dimensionale Vektorräume, ist aber langwieriger zu beweisen und beruht auf einem etwas komplizierteren mengentheoretischen Axiom.

Satz und Definition 4.17 *Je zwei Basen eines Vektorraums haben die gleiche Anzahl von Elementen (im unendlichen Fall: die gleiche Mächtigkeit, d. h. es gibt eine Bijektion zwischen zwei Basen).* Dimension

Die Anzahl der Elemente der Basen eines K-Vektorraums V heißt Dimension von V (über K). Man schreibt dafür $\dim_K V$ oder kurz $\dim V$, wenn K im Kontext festgeschrieben ist.

Beweis: Dieser Satz bleibt vorerst ohne Beweis. Für endlich erzeugte Vektorräume folgt der Beweis später aus dem Gauß-Verfahren (man muss sich aber davon überzeugen, dass der Satz für das Gauß-Verfahren nicht gebraucht wird). Für Vektorräume mit unendlichen Basen wird der Satz nicht bewiesen. □

Bemerkung 4.18 Für den endlich-dimensionalen Fall ist die Aussage „$\{v_1, \ldots, v_n\}$ *ist eine Basis von V ohne Doppelnennungen*“ nun äquivalent zu „$\{v_1, \ldots, v_n\}$ *ist eine Basis von V mit* $n = \dim V$“.

- $\mathbb{R}^n$ hat eine Basis $\{e_1, \ldots, e_n\}$ mit $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, etc. Diese Basis heißt Standardbasis des $\mathbb{R}^n$. Man sieht, dass $\dim_{\mathbb{R}} \mathbb{R}^n = n$.
- Im Fall $n = 1$ besteht die Standardbasis also aus 1; im Fall $n = 0$ ist die Standardbasis (wie jede andere Basis) die leere Menge.

- $\{(1,2,3),(4,5,6),(7,8,0)\}$ ist eine Basis des $\mathbb{R}^3$. Ein Verfahren zum Überprüfen, ob gegebene Elemente des $\mathbb{R}^n$ eine Basis bilden, wird das Gauß-Verfahren liefern.
- $\mathbb{R}[X]$ besitzt (gewissermaßen per Definition) die Basis $\{1, X, X^2, X^3, \dots\} = \{X^i \mid i \in \mathbb{N}\}$. Auch diese Basis heißt Standardbasis von $\mathbb{R}[X]$. Man sieht, dass $\mathbb{R}[X]$ unendliche Dimension hat.
- $\mathbb{R}^\infty$ hat ebenfall unendliche Dimension; es ist aber keine explizite Basis des Vektorraums bekannt. Die Folgen $(1,0,0,0,\dots),(0,1,0,0,\dots),(0,0,1,0,\dots),\dots$ sind zwar linear unabhängig, bilden aber kein Erzeugendensystem.
- Alle voranstehenden Beispiele gelten entsprechend für andere Körper wie $\mathbb{F}_2$ oder $\mathbb{C}$. Insbesondere hat $\mathbb{F}_2^n$ die Dimension n.
- $\mathbb{C}$ hat als $\mathbb{C}-$Vektorraum die Dimension 1 (mit Standardbasis 1), als $\mathbb{R}-$Vektorraum die Dimension 2, z. B. mit der Basis $\{1, \mathrm{i}\}$. Allgemeiner ist $\dim_{\mathbb{C}} \mathbb{C}^n = n$ und $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$. Eine $\mathbb{R}$-Basis von $\mathbb{C}^n$ ist

$$\{(1,0,0,\dots,0),(\mathrm{i},0,0,\dots,0),(0,1,0,\dots,0),$$
$$(0,\mathrm{i},0,\dots,0),\dots,(0,0,\dots,0,1),(0,0,\dots,0,\mathrm{i})\}$$

Satz 4.19 *Seien $v_1,\dots,v_n$ paarweise verschiedene Elemente. Dann ist $\{v_1,\dots,v_n\}$ genau dann eine Basis von V, wenn es für jedes $v \in V$ eine eindeutige Darstellung $v = k_1v_1 + \dots + k_nv_n$ gibt, d. h. wenn aus $v = k_1v_1 + \dots + k_nv_n = k_1'v_1 + \dots + k_n'v_n$ folgt, dass $k_1 = k_1', \dots, k_n = k_n'$.*

Beweis: Zunächst ist klar, dass genau dann für jedes $v \in V$ solch eine Darstellung existiert, wenn $\{v_1,\dots,v_n\}$ ein Erzeugendensystem ist. Angenommen nun $v = k_1v_1 + \dots + k_nv_n = k_1'v_1 + \dots + k_n'v_n$. Dann gilt $0 = (k_1 - k_1')v_1 + \dots + (k_n - k_n')v_n$, d. h. es gibt genau dann zwei verschiedene Darstellungen für einen Vektor, falls es eine nicht-triviale Linearkombination der Null gibt, was nach Satz 4.12 genau dann der Fall ist, wenn $\{v_1,\dots,v_n\}$ nicht linear unabhängig ist. □

Auch für diesen Satz kann man eine „unendliche Version“ angeben, die unmittelbar aus Satz 4.19 folgt:

Satz 4.20 *Eine Teilmenge $\{v_i \mid i \in I\}$ von V ohne Doppelnennungen ist genau dann eine Basis von V, wenn es für jedes $v \in V$ eine eindeutige Darstellung $v = \sum_{i\in I} k_iv_i$ mit $k_i \in K$ gibt.*

Definition 4.21 *Ist $\{v_1,\dots,v_n\}$ eine Basis ohne Doppelnennungen, so werden die eindeutig bestimmten Skalare $k_1,\dots,k_n$ mit $v = k_1v_1 + \dots + k_nv_n$ die Koordinaten von v bezüglich der Basis genannt.* Koordinaten

5 Lineare Abbildungen

5.1 Definition

Seien V und W K-Vektorräume.

Lineare Abbildung

Definition 5.1 *Eine Abbildung $\varphi : V \to W$ ist eine K-lineare Abbildung oder ein K-Vektorraumhomomorphismus, falls φ mit der Gruppenstruktur und der Skalarmultiplikation verträglich ist, d. h. falls für alle $v, v_1, v_2 \in V$ und $k \in K$ gilt*[7]*:*

- $\varphi(v_1 +_V v_2) = \varphi(v_1) +_W \varphi(v_2)$, $\varphi(0_V) = 0_W$ *und* $\varphi(-_V v) = -_W \varphi(v)$
- $\varphi(k \cdot_V v) = k \cdot_W \varphi(v)$.

Falls aus dem Kontext klar ist, um welchen Körper K es sich handelt, spricht man auch kurz von „linearen Abbildungen“ bzw. „Vektorraumhomomorphismen“.

Lemma 5.2 *Die beiden Bedingungen $\varphi(0) = 0$ und $\varphi(-v) = -\varphi(v)$ folgen sowohl bereits aus der Additivität $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ oder auch aus der Verträglichkeit mit der Skalarmultiplikation.*

Beweis: Es ist $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$, also folgt $0 = \varphi(0)$, da $(V, +)$ eine Gruppe ist. Weiter gilt $0 = \varphi(0) = \varphi(v + (-v)) = \varphi(v) + \varphi(-v)$, also ist $\varphi(-v) = -\varphi(v)$.

Alternativ: $\varphi(0) = \varphi(0 \cdot v) = 0 \cdot \varphi(v) = 0$ und $\varphi(-v) = \varphi((-1) \cdot v) = (-1) \cdot \varphi(v) = -\varphi(v)$. □

Isomorphismus
Isomorphie

Definition 5.3 *Eine Abbildung $\varphi : V \to W$ ist ein K-Vektorraumisomorphismus, falls φ eine bijektive Abbildung ist und sowohl φ als auch die Umkehrabbildung φ^{-1} K-linear sind.*

V und W heißen isomorph (als K-Vektorräume), falls ein K-Vektorraumisomorphismus $\varphi : V \to W$ existiert. Man schreibt dafür $V \cong W$.

Bemerkung 5.4 Man kann zeigen, dass die Umkehrabbildung einer bijektiven K-linearen Abbildung automatisch K-linear ist.

Der Begriff „isomorph“ und die Notation $V \cong W$ werden auch bei anderen Strukturen eingesetzt (z. B. Gruppen, Ringe). Wenn sie ohne nähere Spezifikation verwendet werden, setzen sie voraus, dass aus dem Kontext klar ist, welche Art von Strukturen betrachtet werden, hier also K-Vektorräume. Ebenso verkürzt man dann auch „Vektorraumisomorphismus“ und „Vektorraumhomomorphismus“ zu „Isomorphismus“ bzw. „Homomorphismus“.

Bemerkung 5.5 Isomorphie ist eine Äquivalenzrelation auf jeder Menge von K-Vektorräumen. (Reflexivität ist klar, da die Identität offenbar ein Isomorphismus ist. Symmetrie ist in die Definition eingebaut. Transitivität von Linearität wird in Satz 5.13 bewiesen; die Transitivität der Bijektivität ist aus Mathe I bekannt (und leicht).

Satz 5.6 *Sei $\{v_i \mid i \in I\}$ eine Basis von V ohne Doppelnennungen, und seien w_i beliebige Elemente von W. Dann gibt es genau eine lineare Abbildung $\varphi : V \to W$ mit $\varphi(v_i) = w_i$ für*

[7] Der Deutlichkeit halber sind wieder vorübergehend bei den Operationen Indizes V und W angebracht, je nachdem, in welcher Struktur gerechnet wird.

alle $i \in I$.
Außerdem ist φ ist genau dann ein Isomorphismus, wenn $\{w_i \mid i \in I\}$ eine Basis von W ohne Doppelnennungen ist.

BEWEIS: (nur für den Fall von endlichem I) Nach Satz 4.19 schreibt sich jeder Vektor $v \in V$ auf eindeutige Weise als Linearkombination der Basis $v = k_1v_1 + \cdots + k_nv_n$. Wenn es überhaupt eine lineare Abbildung φ wie gewünscht gibt, muss $\varphi(k_1v_1 + \cdots + k_nv_n) = k_1\varphi(v_1) + \cdots + k_n\varphi(v_n) = k_1w_{i_1} + \cdots + k_nw_{i_n}$ gelten. Es gibt also bestenfalls eine Möglichkeit.

Wir definieren nun $\varphi : V \to W$ auf diese Weise. Wegen der Eindeutigkeit der Darstellung ist φ damit wohldefiniert. Ist φ nun tatsächlich linear?

Dazu überprüft man, dass

$$\varphi(k \cdot v) = \varphi\big(k \cdot \sum_{i=1}^{n} k_i \cdot v_i\big) = \varphi\big(\sum_{i=1}^{n} (k \cdot k_i) \cdot v_i\big) = \sum_{i=1}^{n} (k \cdot k_i) \cdot w_i$$
$$k \cdot \varphi(v) = k \cdot \varphi\big(\sum_{i=1}^{n} k_i \cdot v_i\big) = k \cdot \sum_{i=1}^{n} k_i \cdot w_i = \sum_{i=1}^{n} (k \cdot k_i) \cdot w_i$$

und analog für die Additivität.

Schließlich sieht man:

φ ist surjektiv
$\iff$ für jedes $w \in W$ gibt es einen Vektor $v = \sum_{i=1}^{n} k_iv_i$ mit $\varphi(v) = w$, also $\sum_{i=1}^{n} k_iw_i = w$
$\iff$ $\{w_1, \ldots, w_n\}$ ist ein Erzeugendensystem.

φ ist injektiv
$\iff$ falls $\sum_{i=1}^{n} k_iw_i = \sum_{i=1}^{n} k'_iw_i$, so gilt $\sum_{i=1}^{n} k_iv_i = \sum_{i=1}^{n} k'_iv_i$
$\iff$ die Darstellung eines Vektors als Linearkombination von $\{w_1, \ldots, w_n\}$ ist eindeutig.

Zusammen ergibt sich damit nach Satz 4.19, dass $\{w_1, \ldots, w_n\}$ genau dann eine Basis ohne Doppelnennungen ist, wenn φ bijektiv (also ein Isomorphismus) ist. □

Ein Isomorphismus ist soviel wie eine Umbenennung der Elemente des Vektorraums und überträgt alle aus der Vektorraumsstruktur definierbaren Eigenschaften. Insbesondere bildet er ein Erzeugendensystem auf ein Erzeugendensystem, eine linear unabhängige Menge auf eine linear unabhängige Menge und eine Basis auf eine Basis ab, und kann also nur zwischen Vektorräumen gleicher Dimension bestehen!

Folgerung 5.7 *Eine lineare Abbildung $\varphi : V \to W$ ist durch die Bilder einer Basis festgelegt.*

Satz 5.8 *Genau dann gibt es einen K-Vektorraumisomorphismus $\varphi : V \to W$, wenn $\dim_K V = \dim_K W$.*

BEWEIS: Wenn $\varphi : V \to W$ ein Isomorphismus ist und B eine Basis von V, dann ist $\{\varphi(b) \mid b \in B\}$ eine Basis von W der gleichen Mächtigkeit.

Wenn B und B' Basen gleicher Mächtigkeit von V bzw. W sind, angezeigt durch eine Bijektion $\beta : B \to B'$, dann setzt sich β zu einer bijektiven linearen Abbildung $V \to W$, also einem Isomorphismus, fort. □

Definition 5.9 *Eine angeordnete Basis $(v_1, \ldots, v_n)$ ist eine Basis $\{v_1, \ldots, v_n\}$ ohne Doppelnennungen zusammen mit einer festen Reihenfolge der Elemente (nämlich der Anordnung, in der die Elemente als Komponenten des n-Tupels auftreten).* angeordnete Basis

Wenn man die Basiselemente durch Variablen $v_1, \ldots, v_n$ bezeichnet, scheint eine Reihenfolge bereits durch die Anordnung der Indizes gegeben zu sein; daher wirkt die Definition auf den ersten Blick vielleicht überflüssig. In einer konkreten Situation steht aber $\{v_1, \ldots, v_n\}$ z. B. für die Menge $\{(1,1,2), (-2,3,3), (2,-2,0)\}$, auf der keine vorgegebene Reihenfolge erkennbar ist.

Sei nun stets $K = \mathbb{R}$ (wobei die Überlegungen, abgesehen von der geometrischen Anschauung, ebenso für jeden anderen Körper K gelten) und $\varphi : V \to W$ eine $\mathbb{R}$-lineare Abbildung zwischen endlich-dimensionalen $\mathbb{R}$-Vektorräumen $V = \mathbb{R}^n$ und $W = \mathbb{R}^m$. Dann ist φ festgelegt durch die Bilder der Standardbasis $\{e_1, \ldots, e_n\}$. Es ist nun üblich und günstig, die Elemente von V und W als Spaltenvektoren zu schreiben. Wir betrachten zunächst drei Spezialfälle:

- Sei zunächst $n = m = 1$. Dann ist $e_1 = 1$. Mit $\lambda := \varphi(e_1) = \varphi(1) \in \mathbb{R}$ gilt dann:

  $$\varphi(r) = \varphi(r \cdot 1) = r \cdot \varphi(1) = \lambda \cdot r.$$

  Die linearen Abbildungen $\mathbb{R} \to \mathbb{R}$ sind also genau die Multiplikationen mit einer festen reellen Zahl.

- Sei nun n beliebig und $m = 1$. Mit $\lambda_1 := \varphi(e_1)$, …, $\lambda_n := \varphi(e_n)$ gilt dann:

  $$\varphi\Big(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\Big) = \varphi\Big(\sum_{i=1}^{n} r_i \cdot e_i\Big) = \sum_{i=1}^{n} r_i \cdot \varphi(e_i) = \lambda_1 \cdot r_1 + \cdots + \lambda_n \cdot r_n$$

  Die Urbilder der Elemente der Bildraums $\mathbb{R}$ bilden parallele, zu $(\lambda_1, \ldots, \lambda_n)$ senkrechte Hyperebenen im $\mathbb{R}^n$. Man kann die Abbildung geometrisch verstehen als die Projektion auf die Gerade durch den Ursprung in Richtung $(\lambda_1, \ldots, \lambda_n)$, die noch um die Länge von $(\lambda_1, \ldots, \lambda_n)$, also um den Faktor $\sqrt{\lambda_1^2 + \cdots + \lambda_n^2}$, skaliert (d. h. gestreckt oder gestaucht) wird.

- Sei nun $n = 1$ und m beliebig. Mit $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix} := \varphi(e_1) = \varphi(1)$ gilt dann:

  $$\varphi(r) = \varphi(r \cdot 1) = r \cdot \varphi(1) = r \cdot \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix} = \begin{pmatrix} \mu_1 \cdot r \\ \vdots \\ \mu_m \cdot r \end{pmatrix}$$

  Das Bild von φ ist also die Gerade durch den Punkt $\varphi(1)$; die Abbildung φ bildet $\mathbb{R}$ unter Streckung bzw. Stauchung (Skalierung um die Länge von $\varphi(1)$) auf diese Gerade ab.

- Seien schließlich im allgemeinen Fall n und m beliebig. Mit

  $$\begin{pmatrix} \mu_{11} \\ \mu_{21} \\ \vdots \\ \mu_{m1} \end{pmatrix} := \varphi(e_1)\ , \begin{pmatrix} \mu_{12} \\ \mu_{22} \\ \vdots \\ \mu_{m2} \end{pmatrix} := \varphi(e_2)\ , \ldots , \begin{pmatrix} \mu_{1n} \\ \mu_{2n} \\ \vdots \\ \mu_{mn} \end{pmatrix} := \varphi(e_n)$$

gilt dann:

$$\varphi\left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\right) = \varphi\left(\sum_{i=1}^{n} r_i \cdot e_i\right) = \sum_{i=1}^{n} r_i \cdot \varphi(e_i) =$$

$$= r_1 \cdot \begin{pmatrix} \mu_{11} \\ \vdots \\ \mu_{m1} \end{pmatrix} + \cdots + r_n \cdot \begin{pmatrix} \mu_{1n} \\ \vdots \\ \mu_{mn} \end{pmatrix} = \begin{pmatrix} \mu_{11} \cdot r_1 + \cdots + \mu_{1n} \cdot r_n \\ \vdots \\ \mu_{m1} \cdot r_1 + \cdots + \mu_{mn} \cdot r_n \end{pmatrix}$$

Um lineare Abbildungen wie im letzten Beispiel besser beschreiben zu können, führt man Matrizen ein:

Definition 5.10 *Eine* $(m \times n)$-Matrix *über eine Körper* K *ist eine rechteckige Anordnung von* mn *Körperelementen* a_{ij} *für* $i = 1, \ldots, m$ (Zeilenindex) *und* $j = 1, \ldots, n$ (Spaltenindex) *in* m *Zeilen und* n *Spalten:* Matrix

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

Die Menge aller $(m \times n)$*-Matrizen mit Einträgen aus* K *wird mit* $\mathrm{Mat}_{m\times n}(K)$ *bezeichnet.*

Wenn nicht explizit anders angegeben, werden die Einträge einer mit einem Großbuchstaben bezeichneten Matrix durch die entsprechenden Kleinbuchstaben beschrieben. Zum Beispiel werden also die Einträge der Matrix C in der Regel mit c_{ij} bezeichnet, d. h. $C = (c_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$.

Eine $(m \times n)$-Matrix A besteht aus

- m Zeilenvektoren $z_1 = (a_{11}\ a_{12}\ \ldots\ a_{1n})\ , \ldots ,\ z_m = (a_{m1}\ a_{m2}\ \ldots\ a_{mn})$
- und aus n Spaktenvektoren $s_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}\ , \ \ldots\ ,\ s_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$.

Dies deute ich bei Bedarf durch die Schreibweisen $A = \left(\begin{array}{c} z_1 \\ \hline \vdots \\ \hline z_m \end{array}\right)$ bzw. $A = (s_1 | \ldots | s_n)$ an.

Definition 5.11 *Man definiert die* Multiplikation einer $(m \times n)$-Matrix mit einem Spaltenvektor *aus* K^n *durch die Formel:* Matrix · Vektor

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} a_{11}r_1 + a_{12}r_2 + \cdots + a_{1n}r_n \\ a_{21}r_1 + a_{22}r_2 + \cdots + a_{2n}r_n \\ \vdots \\ a_{m1}r_1 + a_{m2}r_2 + \cdots + a_{mn}r_n \end{pmatrix}$$

Satz 5.12 *Durch diese Definition ergibt sich, dass die linearen Abbildungen $K^n \to K^m$ genau die Multiplikationen von links mit $(m \times n)$-Matrizen sind. Zur linearen Abbildung $\varphi : K^n \to K^m$ gehört dabei die $(m \times n)$-Matrix*

$$\big(\, \varphi(e_1) \,\big|\, \cdots \,\big|\, \varphi(e_n) \,\big).$$

Man sagt dafür auch, dass die lineare Abbildung durch die Matrix *dargestellt* wird.

In Zukunft werde ich oft die $(m \times n)$-Matrix A mit der linearen Abbildung $K^n \to K^m$, $v \mapsto A \cdot v$ identifizieren und zum Beispiel von der „Abbildung A“ sprechen.

5.2 Matrixmultiplikation

Satz 5.13 *Seien $\varphi : K^n \to K^m$ und $\psi : K^m \to K^l$ beides K-lineare Abbildungen. Dann ist $\psi \circ \varphi : K^n \to K^l$ ebenfalls K-linear.*

Beweis: Man rechnet nach, dass $(\psi \circ \varphi)(v_1 + v_2) = \psi(\varphi(v_1 + v_2)) = \psi(\varphi(v_1) + \varphi(v_2)) = \psi(\varphi(v_1)) + \psi(\varphi(v_2)) = (\psi \circ \varphi)(v_1) + (\psi \circ \varphi)(v_2)$ und $(\psi \circ \varphi)(k \cdot v) = \psi(\varphi(k \cdot v)) = \psi(k \cdot \varphi(v)) = k \cdot \psi(\varphi(v)) = k \cdot (\psi \circ \varphi)(v)$. □

Die Abbildungen φ, ψ und $\psi \circ \varphi$ aus dem Satz werden durch eine $(m \times n)$-Matrix A, eine $(l \times m)$-Matrix B und eine $(l \times n)$-Matrix C dargestellt. Wie hängt nun C mit A und B zusammen? Wie kann man C aus A und B ausrechnen?

$$C \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \psi\big(\varphi\big(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}\big)\big) = B \cdot \big(A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}\big) =$$

$$= B \cdot \begin{pmatrix} \sum_{i=1}^{n} a_{1i} v_i \\ \vdots \\ \sum_{i=1}^{n} a_{mi} v_i \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{m} b_{1j} \sum_{i=1}^{n} a_{ji} v_i \\ \vdots \\ \sum_{j=1}^{m} b_{lj} \sum_{i=1}^{n} a_{ji} v_i \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{m} \sum_{i=1}^{n} b_{1j} a_{ji} v_i \\ \vdots \\ \sum_{j=1}^{m} \sum_{i=1}^{n} b_{lj} a_{ji} v_i \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} (\sum_{j=1}^{m} b_{1j} a_{ji}) v_i \\ \vdots \\ \sum_{i=1}^{n} (\sum_{j=1}^{m} b_{lj} a_{ji}) v_i \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{j=1}^{m} b_{1j} a_{j1} & \dots & \sum_{j=1}^{m} b_{1j} a_{jn} \\ \vdots & & \vdots \\ \sum_{j=1}^{m} b_{lj} a_{j1} & \dots & \sum_{j=1}^{m} b_{lj} a_{jn} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Abbildung 1: Matrizenmultiplikation

Dazu rechnet man $C \cdot v = (B \cdot A) \cdot v$ aus (siehe Formelkasten in Abbildung 1) und stellt fest, dass der (i, j)-Eintrag der Matrix C sich berechnet als

$$c_{ij} = \sum_{x=1}^{m} b_{ix} a_{xj} = \begin{pmatrix} b_{i1} & \dots & b_{im} \end{pmatrix} \cdot \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = i\text{-te Zeile} \begin{pmatrix} \cdots & \cdots & \cdots \\ b_{i1} & \dots & b_{im} \\ \cdots & \cdots & \cdots \end{pmatrix} \cdot \overset{j\text{-te Spalte}}{\begin{pmatrix} \vdots & a_{1k} & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & a_{mk} & \vdots \end{pmatrix}}$$

wobei hierfür die i-te Zeile von B mit der k-ten Spalte von A so multipliziert wird, wie im letzten Abschnitt definiert (dies heißt auch *Skalarprodukt* des i-ten Zeilenvektors von B mit dem k-ten Spaltenvektor von A, siehe Defintion 6.5).

Definition 5.14 *Das Matrixprodukt $B \cdot A$ einer $(l \times m)$-Matrix B mit einer $(m \times n)$-Matrix A ist die $(l \times n)$-Matrix C mit Einträgen $c_{ik} = \sum_{j=1}^{m} b_{ij} a_{jk}$.* Matrix · Matrix

Das Matrixprodukt $B \cdot A$ ist also dann und nur dann definiert, wenn die Anzahl der Spalten von B gleich der Anzahl der Zeilen von A ist. Als Merkregel für die Dimensionen der Matrizen kann man sich „$(l \times m) \cdot (m \times n) = (l \times n)$“ einprägen; der gemeinsame mittlere Term verschwindet also.

Das Matrixprodukt wurde genau so definert, dass folgendes gilt:

Satz 5.15 *Wenn A eine $(m \times n)$-Matrix über K ist und B eine $(l \times m)$-Matrix über K und $v \in K^n$, so gilt*

$$(B \cdot A) \cdot v = B \cdot (A \cdot v).$$

Im letzten Abschnitt wurde das Produkt $B \cdot v$ einer $(l \times m)$-Matrix B mit einem Spaltenvektor $v \in K^m$ definiert. Nun ist solch ein Spaltenvektor v nichts anderes als eine $(m \times 1)$-Matrix A. Somit ist also das Produkt $B \cdot v$ eigentlich doppelt definiert, aber man kann sich leicht anhand der Formeln davon überzeugen, dass beide Definitionen übereinstimmen.

Dass dies kein Zufall ist, sieht man folgendermaßen ein: Man kann einen Vektor $v \in K^m$ mit der linearen Abbildung $K^1 \to K^m$, $1 \mapsto v$ identifizieren, deren Matrix gerade der Spaltenvektor v ist. (Die Abbildung ist also die Multiplikation eines Skalars mit v.) Die Verküpfung dieser Abbildung mit der durch B beschriebenen linearen Abbildung ist dann die lineare Abbildung $K^1 \to K^l$, welche 1 auf $B \cdot v$ abbildet. Die Matrix dieser Abbildung berechnet sich als das Matrixprodukt von B und v, ist aber andererseits der Spaltenvektor $B \cdot v$.

Man hätte sich aber auch umgekehrt die Matrixmultiplikation aus der Multiplikation einer Matrix mit einem Vektor herleiten können. Wenn A die lineare Abbildung $\varphi : K^n \to K^m$ darstellt und B die Abbildung $\psi : K^m \to K^l$, so gilt $(\psi \circ \varphi)(e_i) = \psi(\varphi(e_i)) = \psi(A \cdot e_i) = B \cdot (A \cdot e_i)$, d. h. der i-te Spaltenvektor der Matrix zu $\psi \circ \varphi$ ist $B \cdot s_i$, wobei s_i der i-te Spaltenvektor von A ist. Wenn A nur aus einer Spalte besteht, ist dies also die schon bekannte Multiplikation der Matrix B mit dem Spaltenvektor.

Man sieht also, dass das Matrixprodukt $B \cdot A$ „spaltenweise in A“ funktioniert, d. h. wenn $A = (s_1 | \dots | s_n)$, so ist $B \cdot A = (B \cdot s_1 | \dots | B \cdot s_n)$. Umgekehrt funktioniert es „zeilenweise in B“, d. h. wenn $B = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix}$, so ist $B \cdot A = \begin{pmatrix} z_1 \cdot A \\ \vdots \\ z_m \cdot A \end{pmatrix}$, wobei hier in den Zeilen also das Matrixprodukt der Zeilenvektoren von B, aufgefasst als $(1 \times m)$-Matrixzen, mit der $(m \times n)$-Matrix A steht.

- Ein Beispiel für eine (willkürlich gewählte) Matrixmultiplikation:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 \cdot (-1) + 2 \cdot 0 + 3 \cdot 1 & 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 3 \\ 4 \cdot (-1) + 5 \cdot 0 + 6 \cdot 1 & 4 \cdot 0 + 5 \cdot 2 + 6 \cdot 3 \end{pmatrix} = \begin{pmatrix} 2 & 13 \\ 2 & 28 \end{pmatrix}$$

- Die Verküpfung „Spiegelung an der y-Achse ∘ Spiegelung an der x-Achse“ wird beschrieben durch
$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
ergibt also die Matrix der Punktspiegelung am Ursprung.

- Eine Drehung um den Winkel α mit anschließender Drehung um den Winkel β ergibt insgesamt eine Drehung um $\alpha+\beta$. Aus der Berechnung des Matrixprodukts ergeben sich dadurch die Additionstheoreme für Sinus und Cosinus:
$$\begin{aligned} &\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \\ &\qquad = \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\ &\qquad = \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\sin\alpha\cos\beta - \cos\alpha\sin\beta \\ \cos\alpha\sin\beta + \sin\alpha\cos\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix} \end{aligned}$$

Definition 5.16 *Die zur Identitätsabbildung* $\mathrm{id} : K^n \to K^n$ *gehörige Matrix ist die Einheitsmatrix genannte* $(n\times n)$*-Matrix* I_n*, deren Spalten (bzw. Zeilen) gerade die Standardbasisvektoren sind.* Einheitsmatrix

Die zur konstanten Nullabbildungen $K^n \to K^m$, $v \mapsto 0$, *gehörige Matrix ist die Nullmatrix, deren Einträge alle* 0 *sind. Sie wird meist ebenfalls mit* 0 *bezeichnet.*

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \qquad 0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Exkurs zur Komplexität der Matrizenmultiplikation:

Matrizenmultiplikationen spielen in vielen algorithmischen Anwendungen eine große Rolle; es ist daher interessant und nützlich, möglichst schnelle Verfahren zu finden. Das Verfahren, das der Definition folgt, läuft für zwei $(n \times n)$-Matrizen in $O(n^3)$: pro Eintrag n Multiplikationen und $n-1$ Additionen. Für große Matrizen gibt es aber schnellere Verfahren: Das erste solche wurd 1969 von Volker Strassen [8] entwickelt und läuft in $O(n^{2,807})$. Er wurde nach und nach verbessert; den letzten großen Schritt lieferte 1990 der Coppersmith-Winograd-Algorithmus [9] mit $O(n^{2,3737})$. Etwas überraschend kam 2010 nochmals eine Verbesserung durch Andrew Stothers; der derzeit letzte Stand ist ein Algorithmus von Virginia Vassilevska Williams aus dem Jahre 2011 mit einer Laufzeit von $O(n^{2,3727})$. Als untere Schranke hat man sicher $O(n^2)$, da n^2 Einträge auszurechnen sind; einige Forscher vermuten, dass diese untere Schranke optimal ist, also dass es Algorithmen in $O(n^2)$ gibt.

(Zu bedenken ist dabei, dass kleinere Exponenten wegen der in der O-Notation versteckten Konstanten evtl. nur für sehr große Matrizen Verbesserungen bringen; außerdem sagt die Laufzeit nichst über die Güte des Algorithmus hinsichtlich Stabilität (Fehleranfälligkeit) aus. Die Verbesserung des Exponenten in der dritten Nachkommastelle scheint zunächst vernachlässigbar, es ist aber bereits $1000^{2,3737}$ –

[8] Volker Strassen (∗ 1936), ehemaliger Student der Universität Freiburg, zuletzt Professor in Konstanz.
[9] nach Don Coppersmith (∗ ca. 1950) und Shmuel Winograd (∗ 1936), damals IBM.

$1000^{2,3727} \approx 10^5$; bei vielen Multiplikationen großer Matrizen kann sich also ein spürbarer Effekt ergeben.)

Satz 5.17 *Die Matrizenmulitplikation ist assoziativ, aber i. a. nicht kommutativ, auch bei* $(n \times n)$*-Matrizen untereinander. Die Einheitsmatrizen sind neutrale Elemente in dem Sinn, dass* $I_m \cdot A = A$ *und* $A \cdot I_n = A$ *für jede* $(m \times n)$*-Matrix* A *gelten. Nullmatrizen sind* absorbierende Elemente*, d. h. es gilt* $0 \cdot A = 0$ *und* $A \cdot 0 = 0$ *(für die Nullmatrix passender Größe, so dass also die Multiplikationen definiert sind).*

Beweis: Alle Eigenschaften folgen daraus, dass sie auf Seite der zugehörigen Abbildungen gelten. Die nicht vorhandene Kommutativität sieht man z. B. an

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}.$$

□

Bemerkung 5.18 Eine (1×1)-Matriz (a_{11}) kann man mit der Zahl a_{11} identifizieren. Die Multiplikation von (1×1)-Matrizen ist also kommutativ.

Abgesehen von der fehlenden Kommutativität gibt es noch andere Eigenschaften, welche die Matrizenmultiplikation von der Multiplikation z. B. reeller Zahlen unterscheidet. So gibt es sogenannte „nilpotente“ Elemente, das sind Matrizen $A \neq 0$ mit $A^n = 0$ für ein $n > 0$. Zum Beispiel gilt:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Insbesondere folgt für Matrizen aus $A \cdot B = 0$ nicht $A = 0$ oder $B = 0$!

Definition 5.19 *Abbildungen* $\varphi, \psi : K^n \to K^m$ *kann man addieren durch* $(\varphi + \psi)(v) := \varphi(v) + \psi(v)$ *und skalar multiplizieren durch* $(k \cdot \varphi)(v) := k \cdot \varphi(v)$*. Die Menge der Abbildungen wird dadurch zu einem* K*-Vektorraum* $\mathrm{Abb}(K^n, K^m)$*. Die Teilmenge der linearen Abbildungen* $K^n \to K^m$ *bildet darin einen Untervektorraum* $\mathrm{Lin}(K^n, K^m)$*.*

$\mathrm{Abb}(K^n, K^m)$
$\mathrm{Lin}(K^n, K^m)$

Man kann nun die Addition und Skalarmultiplikation mittels der Identifikation von linearen Abbildungen und Matrizen in Satz 5.12 auf Matrizen ausdehnen, so dass die Menge $\mathrm{Mat}_{m\times n}(K)$ zu einem zu $\mathrm{Lin}(K^n, K^m)$ isomorphen K-Vektorraum wird. Man kann nun leicht nachrechnen, dass die folgende Definition die Matrizenaddition und die Skalarmultiplikation von Matrizen beschreibt:

Definition 5.20 *Seien* A *und* B $(m \times n)$*-Matrizen über* K *und* $k \in K$*. Dann ist*

$\mathrm{Mat}_{m\times n}(K)$

$$A + B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} := \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \vdots & & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

$$k \cdot A = k \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} := \begin{pmatrix} ka_{11} & \dots & ka_{1n} \\ \vdots & & \vdots \\ ka_{m1} & \dots & ka_{mn} \end{pmatrix}$$

Satz 5.21 **(a)** *Die $(m \times n)$-Matrizen über K bilden einen mn-dimensionalen, zu $\mathrm{Lin}(K^n, K^m)$ isomorphen K-Vektorraum $\mathrm{Mat}_{m\times n}(K)$. Das neutrale Element der Addition ist die $(m \times n)$-Nullmatrix.*
Die Matrizen E_{ij}, deren (i, j)-Eintrag jeweils 1 ist und alle anderen Einträge 0, bilden eine Basis, die Standardbasis von $\mathrm{Mat}_{m\times n}(K)$ genannt wird. Jede Aufzählung der Standardbasis liefert einen Vektorraum-Isomorphismus $\mathrm{Mat}_{m\times n}(K) \to K^{mn}$, der die Standardbasis von $\mathrm{Mat}_{m\times n}(K)$ in der gewählten Reihenfolge auf die Standardbasis von K^{mn} in der natürlichen Reihenfolge abbildet.

(b) *Es gelten die Distributivgesetze, d. h. immer dann, wenn die Operationen definiert sind, gelten $A \cdot (B_1 + B_2) = (A \cdot B_1) + (A \cdot B_2)$ und $(B_1 + B_2) \cdot A = (B_1 \cdot A) + (B_2 \cdot A)$.*

(c) *Die quadratischen $(n \times n)$-Matrizen $\mathrm{Mat}_{n\times n}(K)$ bilden mit Matrizenaddition und -multiplikation einen (für $n \geq 2$ nicht-kommutativen) Ring mit Eins I_n.*

(d) *$k \cdot I_n$ ist die „$(n \times n)$-Diagonalmatrix“ mit Einträgen k auf der Hauptdiagonale von links oben nach rechts unten und Einträgen 0 an allen anderen Stellen. Es gilt dann $k \cdot A = (k \cdot I_n) \cdot A = A \cdot (k \cdot I_n)$. Es folgt daraus, dass die Skalarmultiplikation mit der Matrizenmultiplikation vertauscht, d. h. es gilt $k \cdot (A \cdot B) = (k \cdot A) \cdot B = A \cdot (k \cdot B)$, sofern das Produkt $A \cdot B$ definiert ist.*

Beweis: Die Matrizen E_{ij} bilden eine Basis, da sich jede Matrix eindeutig schreiben lässt als $A = \sum_{i,j} a_{ij} E_{ij}$. Die Distributivgesetze und Teil (d) gelten, weil sie auf der Seite der linearen Abbildungen gelten. Alles andere folgt aus der bisher entwickelten Theorie. □

5.3 Basiswechsel

Ziel dieses Abschnitts ist es nun, lineare Abbildungen zwischen beliebigen endlich dimensionalen Vektorräumen durch Matrizen zu beschreiben. Da beliebige Vektorräume keine ausgezeicheten Basen haben, wird es – abhängig von gewählten Basen – verschiedene darstellenden Matrizen geben. Eine Hauptfrage wird darin bestehen zu verstehen, wie diese Matrizen miteinander zusammenhängen. Als Spezialfall erhält man dann auch die Darstellung linearer Abbildungen $K^n \to K^m$ bezüglich anderer Basen als den Standardbasen.

Satz 5.22 *Sei V ein n-dimensionaler K-Vektorraum. Dann wird durch jede angeordnete Basis $B = (v_1, \ldots, v_n)$ ein Vektorraumisomorphismus $i_B : V \to K^n$, $v_i \mapsto e_i$ festgelegt. Dabei wird $v = k_1 v_1 + \cdots + k_n v_n$ auf seine Koordinaten $(k_1, \ldots, k_n)$ bezüglich der Basis B abgebildet.*

Umgekehrt bestimmt jeder Vektorraumisomorphismus $i : V \to K^n$ eine angeordnete Basis B von V, nämlich $(i^{-1}(e_1), \ldots, i^{-1}(e_n))$, und es ist $i = i_B$.

$U := \{(v_1, v_2, v_3, v_4) \in \mathbb{R}^4 \mid v_1 - v_2 + v_3 - v_4 = 0\}$ ist ein 3-dimensionaler Untervektorraum des $\mathbb{R}^4$. Eine angeordnete Basis $B = (u, v, w)$ von U besteht zum Beispiel aus den Vektoren $u = (1, 1, 0, 0,), v = (0, 0, 1, 1,), w = (1, 0, 0, 1)$. Sie legt den Isomorphismus $i_B : U \to \mathbb{R}^3$ fest durch $u \mapsto e_1, v \mapsto e_2, w \mapsto e_3$.

Es wird dabei z. B. der Vektor $(1, 2, 3, 2) = 2 \cdot u + 3 \cdot v - 1 \cdot w \in U$ abgebildet auf den Vektor seiner Koordinaten bzgl. B, also auf $(2, 3, -1) \in \mathbb{R}^3$.

Umgekehrt gehört z. B. zu dem Vektor $(1,2,3) \in \mathbb{R}^3$ das Urbild $i_B^{-1}(1,2,3) = u + 2 \cdot v + 3 \cdot w = (4,1,2,5) \in U$.

darstellende Matrix bzgl. Basen

Definition 5.23 *Sei V ein n-dimensionaler und W ein m-dimensionaler K-Vektorraum und $\varphi : V \to W$ eine K-lineare Abbildung. Sei außerdem $(v_1, \ldots, v_n)$ eine angeordnete Basis B von V und $(w_1, \ldots, w_m)$ eine angeordnete Basis B' von W. Nach Satz 5.22 legen B und B' Isomorphismen $i_B : V \to K^n$ und $i_{B'} : W \to K^m$ fest, so dass sich folgendes Diagramm ergibt:*

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ i_B \downarrow & & \downarrow i_{B'} \\ K^n & & K^m \end{array}$$

Die Matrix von φ bezüglich der Basen B und B' wird nun definiert als die Matrix der Abbildung $i_{B'} \circ \varphi \circ i_B^{-1} : K^n \to K^m$ und wird mit ${}_{B'}\varphi_B$ bezeichnet.

Im Spezialfall $V = W$ und $B = B'$ schreibt man kurz φ_B für ${}_B\varphi_B$.

Die Spaltenvektoren der Matrix ${}_{B'}\varphi_B$ sind also die Koordinaten von $\varphi(v_1), \ldots, \varphi(v_n)$ bezüglich der angeordneten Basis B'.

Satz 5.24 *Seien V, W und X endlich-dimensionale K-Vektorräume mit angeordneten Basen B, B' bzw. B'' und seien $\varphi : V \to W$ und $\psi : W \to X$ lineare Abbildungen. Dann gilt*

$$ {}_{B''}(\psi \circ \varphi)_B \;=\; ({}_{B''}\psi_{B'}) \cdot ({}_{B'}\varphi_B)$$

BEWEIS: ${}_{B''}(\psi \circ \varphi)_B$ ist nach Definition die Matrix von

$$i_{B''} \circ (\psi \circ \varphi) \circ i_B^{-1} = i_{B''} \circ \psi \circ i_{B'}^{-1} \circ i_{B'} \circ \varphi \circ i_B^{-1}$$

was gerade das Produkt der Matrix von $i_{B''} \circ \psi \circ i_{B'}^{-1}$ mit der Matrix von $i_{B'} \circ \varphi \circ i_B^{-1}$ ist, also $({}_{B''}\psi_{B'}) \cdot ({}_{B'}\varphi_B)$. □

Basiswechsel

Satz und Definition 5.25 *Sei $\varphi : V \to W$ linear, seien B_1, B_2 angeordnete Basen von V und B_1', B_2' angeordnete Basen von W. Dann gilt:*

$${}_{B_2'}\varphi_{B_2} = ({}_{B_2'}\mathrm{id}_{W\,B_1'}) \cdot ({}_{B_1'}\varphi_{B_1}) \cdot ({}_{B_1}\mathrm{id}_{V\,B_2})$$

Die Matrizen ${}_{B_2'}\mathrm{id}_{W\,B_1'}$ und ${}_{B_1}\mathrm{id}_{V\,B_2}$ heißen Basiswechselmatrizen.

Im Spezialfall $V = W$ und $B_i' = B_i$ gilt:

$$\varphi_{B_2} = ({}_{B_2}\mathrm{id}_{V\,B_1}) \cdot \varphi_{B_1} \cdot ({}_{B_1}\mathrm{id}_{V\,B_2}) = ({}_{B_1}\mathrm{id}_{V\,B_2})^{-1} \cdot \varphi_{B_1} \cdot ({}_{B_1}\mathrm{id}_{V\,B_2}).$$

Insbesondere sind Basiswechselmatrizen stets invertierbar (siehe folgende Definition) mit

$$({}_{B_1}\mathrm{id}_{V\,B_2})^{-1} = {}_{B_2}\mathrm{id}_{V\,B_1}$$

BEWEIS: Der erste Teil folgt direkt aus dem Satz, da $\varphi = \mathrm{id}_W \circ \varphi \circ \mathrm{id}_V$. Wegen $({}_{B_2}\mathrm{id}_{V\,B_1}) \cdot ({}_{B_1}\mathrm{id}_{V\,B_2}) = {}_{B_2}(\mathrm{id}_V \circ \mathrm{id}_V)_{B_2} = {}_{B_2}\mathrm{id}_{V\,B_2} = I_{\dim V}$ folgt auch die rechte Seite der Gleichung im Spezialfall. □

Definition 5.26 *Eine $(n\times n)$-Matrix A über K heißt invertierbar, wenn die zugehörige lineare Abbildung $K^n \to K^n$ invertierbar ist, d. h. wenn eine $(n\times n)$-Matrix A^{-1} existiert (nämlich die Matrix zur Umkehrabbildung) mit*

invertierbare Matrix

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n.$$

Wegen der Eindeutigkeit der Umkehrabbildung (alternativ durch die gleiche Überlegung wie in Gruppen) sieht man, dass die Matrix A^{-1} durch die Eigenschaft $A\cdot A^{-1} = I_n$ oder $A^{-1}\cdot A = I_n$ bereits eindeutig bestimmt ist.

Satz 5.27 *A ist genau dann invertierbar, wenn die Spaltenvektoren $A\cdot e_1, \ldots, A\cdot e_n$ von A eine Basis von K^n bilden. Die Umkehrabbildung ist dann durch die Zuordnung $A\cdot e_i \mapsto e_i$ festgelegt.*

A^{-1} ist invertierbar und es gilt $(A^{-1})^{-1} = A$. Falls A und B invertierbare $(n\times n)$-Matrizen sind, so ist auch $B\cdot A$ invertierbar und es gilt $(B\cdot A)^{-1} = A^{-1}\cdot B^{-1}$.

Beweis: Der erste Teil folgt direkt aus Satz 5.6. Die anderen Teile gelten in beliebigen Monoiden, siehe Lemma 3.4. □

Wie rechnet man die Basiswechselmatrizen aus?

Ist die Basis $B_1 = (v_1, \ldots, v_n)$ von V gegeben und ist v'_j der j-te Vektor in B_2, so muss man also die Koeffizienten a_{ij} mit $v'_j = a_{1j}v_1 + \cdots + a_{nj}v_n$ berechnen; diese stehen als j-te Spalte in der Basiswechselmatrix ${}_{B_1}\mathrm{id}_{V\,B_2}$. Wenn die Basiselemente als Vektoren in K^n gegeben sind (also mit ihren Koordinaten bezüglich der Standardbasis), dann ergibt die Gleichung ein lineares Gleichungssystem, das z. B. nach dem Gauß-Verfahren (siehe folgender Abschnitt) gelöst werden kann. Auch das Invertieren von Matrizen geschieht am besten mit dem Gauß-Verfahren.

Besonders einfach ist es, wenn $V = K^n$ und B_1 die Standardbasis ist: Dann sind die Spaltenvektoren der Basiswechselmatrix ${}_{B_1}\mathrm{id}_{V\,B_2}$ gerade die Vektoren von B_2.

- Sei $V = \mathbb{R}^3$ mit der Basis $B_1 = (e_1, e_2, e_3)$, also der Standardbasis und der Basis $B_2 = (v_1, v_2, v_3)$ mit $v_1 = (0,0,1)$, $v_2 = (0,1,2)$ und $v_3 = (1,1,1)$.

  Sei $W = \mathbb{R}^2$ mit den Basen $B'_1 = (w_1, w_2)$, wobei $w_1 = (1,1)$ und $w_2 = (1,-1)$, und $B'_2 = (w'_1, w'_2)$, wobei $w'_1 = (1,0)$ und $w'_2 = (1,1)$.

  Die eine Basiswechselmatrix von V ergibt sich aus den Vektoren von B_2 als Spalten der Matrix, da B_1 die Standardbasis ist:

$$ {}_{B_1}\mathrm{id}_{B_2} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} $$

  Die andere Basiswechselmatrix erhält man als Inverse:

$$ {}_{B_2}\mathrm{id}_{B_1} = ({}_{B_1}\mathrm{id}_{B_2})^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} $$

  Man kann zum einen durch Ausmultiplizieren nachprüfen, dass die angegebene Matrix tatsächlich die Inverse ist, also dass ${}_{B_1}\mathrm{id}_{B_2} \cdot {}_{B_2}\mathrm{id}_{B_1} = I_3$. Zum andern kann man nachrpüfen, dass ${}_{B_2}id_{B_1}$ tatsächlich die Koeffizienten der Standardbasis bezüglich B_2 beinhaltet,

also dass gilt:

$$\begin{aligned} e_1 &= 1 \cdot v_1 - 1 \cdot v_2 + 1 \cdot v_3 \\ e_2 &= -2 \cdot v_1 + 1 \cdot v_2 + 0 \cdot v_3 \\ e_3 &= 1 \cdot v_1 + 0 \cdot v_2 + 0 \cdot v_3 \end{aligned}$$

Analog sieht man für die Basiswechselmatrizen von W, dass

$$\begin{aligned} w_1 &= 0 \cdot w_1' + 1 \cdot w_2' & \qquad w_1' &= \frac{1}{2} \cdot w_1 + \frac{1}{2} \cdot w_2 \\ w_2 &= 2 \cdot w_1' - 1 \cdot w_2' & \qquad w_2' &= 1 \cdot w_1 + 0 \cdot w_2 \end{aligned}$$

und folglich

$${}_{B_{2'}}\mathrm{id}_{B_1'} = \begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix} \quad \text{und} \quad {}_{B_{1'}}\mathrm{id}_{B_2'} = ({}_{B_{2'}}\mathrm{id}_{B_1'})^{-1} = \begin{pmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{pmatrix}$$

Sei nun die lineare Abbildung $\varphi : V \to W$ bezüglich der Basen B_1, B_1' beschrieben durch die Matrix

$${}_{B_1'}\varphi_{B_1} = \begin{pmatrix} 3 & 1 & 2 \\ 0 & 5 & 4 \end{pmatrix}.$$

Dies bedeutet also, dass $\varphi(e_1) = 3w_1$, $\varphi(e_2) = w_1 + 5w_2$ und $\varphi(e_3) = 2w_1 + 4w_2$. Die Matrix von φ bezüglich der Basen B_2, B_2' errechnet sich dann als

$$\begin{aligned} {}_{B_{2'}}\varphi_{B_2} &= ({}_{B_2'}\mathrm{id}_{B_1'}) \cdot ({}_{B_1'}\varphi_{B_1}) \cdot ({}_{B_1}\mathrm{id}_{B_2}) \\ &= \begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 \\ 0 & 5 & 4 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 10 & 8 \\ 3 & -4 & -2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 8 & 26 & 18 \\ -2 & -8 & -3 \end{pmatrix} \end{aligned}$$

Dies bedeutet nun, dass $\varphi(v_1) = 8w_1' - 2w_2'$, $\varphi(v_2) = 26w_1' - 8w_2'$ und $\varphi(v_3) = 18w_1' - 3w_2'$. Exemplarisch kann man dies nachrechnen; so gilt z. B.

$$\begin{aligned} \varphi(v_2) = \varphi(e_2 + 2e_3) = \varphi(e_2) + 2\varphi(e_3) &= w_1 + 5w_2 + 2 \cdot (2w_1 + 4w_2) \\ = 5w_1 + 13w_2 = 5w_2' + 13(2w_1' - w_2') &= 26w_1' - 8w_2' \end{aligned}$$

- Ein weiteres Beispiel für die Berechnung eines Basiswechsels findet sich bei der Diagonalisierung einer Drehung über den komplexen Zahlen auf Seite 38.

- Ein Spezialfall eines Basiswechsels liegt vor, wenn es sich um die gleichen Basiselemente in anderer Anordnung handelt, wenn der Basiswechsel also in einer Umordnung der Basis besteht:

  Wenn B die Basis $(v_1, \ldots, v_n)$ ist, wird eine Umordnung beschrieben durch eine *Permutation* der Indizes, also eine Bijektion $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, wobei die neu angeordnete Basis B^σ dann $(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$ ist.[10]

Definition 5.28 *Die Basiswechselmatrix* $M(\sigma) := {}_{B^\sigma}\mathrm{id}_B$ *hat Einträge* 1 *an den Stellen* $(i, \sigma(i))$ *und* 0 *an allen anderen Stellen. Solche Matrizen heißen Permutationsmatrix: Sie sind quadratische Matrizen, die in jeder Zeile und in jeder Spalte genau eine* 1 *haben und sonst überall* 0.

Permutationsmatrix

Die Inverse zu $M(\sigma)$ ist $M(\sigma^{-1})$, also die Permutationsmatrix mit Einträgen 1 an den Stellen $(i, \sigma^{-1}(i))$. Da jedes i von der Form $\sigma(j)$ ist, ist dann $(i, \sigma^{-1}(i)) = (\sigma(j), j)$, d. h. $M(\sigma^{-1})$ entsteht, indem man $M(\sigma)$ an der Hauptdiagonalen spiegelt. Dies heißt auch die Transponierte $M(\sigma)^{\mathrm{T}}$ von $M(\sigma)$.

Beispiel: Sei $n = 3$ und $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$. Dann ist

$$M(\sigma) = {}_{B^\sigma}\mathrm{id}_B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ und } M(\sigma^{-1}) = {}_{B}\mathrm{id}_{B_\sigma} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

(Kleiner Vorgriff auf Abschnitt 8: Die Abbildung $\sigma \mapsto M(\sigma^{-1})$ ist ein Gruppenhomomorphismus von der Symmetrischen Gruppe $\mathrm{Sym}(n)$ der Permutationen von $\{1, \ldots, n\}$ in die multiplikative Gruppe $\mathrm{GL}(n, K)$ der invertierbaren $(n \times n)$-Matrizen.)

Spezialfall: Transpositionen sind spezielle Permutatione, die nur zwei Elemente vertauschen (und damit selbst-invers sind). Die Transposition τ, welche die Elemente i und j vertauscht, schreibt man auch (ij). Der Lesbarkeit halber schreibe ich $M_{(ij)}$ für $M((ij))$. Es gilt dann (alle nicht aufgeführten Einträge sind gleich 0 und o. B. d. A. ist $i < j$):

$$M_{(ij)} = M_{(ij)}^{-1} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ i\text{-te Zeile} \\ \\ j\text{-te Zeile} \\ \\ \end{matrix}$$

Es ist also etwa (zweite und dritte Zeile und Spalte jeweils vertauschen!)

$$M_{(23)} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 0 & 1 & 2 \\ 3 & 4 & 5 & 6 \end{pmatrix} \cdot M_{(32)} = \begin{pmatrix} 1 & 3 & 2 & 4 \\ 9 & 1 & 0 & 2 \\ 5 & 7 & 6 & 8 \\ 3 & 5 & 4 & 6 \end{pmatrix}.$$

Ein Ziel der linearen Algebra besteht darin, zu einer gegebenen linearen Abbildung $\varphi : V \to V$ eine Basis B zu finden, so dass die Matrix φ_B möglichst „schön“ ist. Hierzu gibt es eine ganze Reihe von Ergebnissen über sogenannte Normalformen von Matrizen. „Besonders schön“ ist

eine Matrix in Diagonalgestalt, also von der Form

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

(alles außerhalb der von λ_1 bis λ_n gebildeten Diagonalen hat den Eintrag 0).

Für die Basisvektoren $v_1, \ldots, v_n$ gilt dann $\varphi(v_i) = \lambda v_i$ und für beliebige Vektoren $\varphi(a_1 v_1 + \cdots + a_n v_n) = \lambda a_1 v_1 + \cdots + \lambda a_n v_n$.

Definition 5.29 *Ein Vektor $v \neq 0$ heißt Eigenvektor der linearen Abbildung $\varphi : V \to V$ zum Eigenwert $\lambda \in K$, falls $\varphi(v) = \lambda v$.* Eigenvektor

Der Idealfall besteht also darin, dass man zu einer linearen Abbildung eine Basis aus Eigenvektoren findet. (Wenn man weiß, dass λ ein Eigenwert ist und φ durch die Matrix A beschrieben ist, kann man die Eigenvektoren durch Lösen des linearen Gleichungssystemes $A \cdot x = \lambda x$ mit unbekannten Koeffizienten für x finden. Jedes skalare Vielfache eines Eigenvektors ($\neq 0$) ist wieder ein Eigenvektor. Die Eigenwerte wiederum kann man als Nullstellen des sogenannten *charakteristischen Polynoms* bestimmen.)

Im Allgemeinen findet man aber keine Basis aus Eigenvektoren. Es gibt zwei Hinderungsgründe:

(1) *Drehungen im $\mathbb{R}^2$ haben i. a. keine Eigenvektoren.* Dies ist geometrisch sofort ersichtlich. Nur wenn der Drehwinkel ein ganzzahliges Vielfaches von 180° ist, gibt es Eigenvektoren in $\mathbb{R}^2$.

Diese Problem lässt sich dadurch beheben, dass man den Körper erweitert, hier zu den komplexen Zahlen $\mathbb{C}$. So hat z. B. die Drehung um 90° bezüglich der Standardbasis die Matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ – ohne Eigenvektoren in $\mathbb{R}^2$ – aber als Matrix über den komplexen Zahlen sind $\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 \\ -i \end{smallmatrix}\right)$ zwei linear unabhängige Eigenvektoren zu den Eigenwerten $-i$ und i, d. h. bezüglich der aus diesen beiden Vektoren gebildeten Basis ergibt sich die Diagonalform $\left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right)$.

Man kann an diesem Beispiel noch einmal schön den Basiswechsel nachvollziehen: Da eine der Basen die Standardbasis ist, besteht eine der beiden Basiswechselmatrizen aus den Vektoren der anderen Basis als Spalten und die andere Basiswechselmatrix ist deren Inverse:

$$\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix};$$

man kann auch nachrechnen, dass diese Matrix tatsächlich die Koeffizienten der Standardbasis bezüglich der neuen Basis enthält, da

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ i \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 \\ -i \end{pmatrix} \text{ und } \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{2i}\begin{pmatrix} 1 \\ i \end{pmatrix} - \frac{1}{2i}\begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

Auch den Basiswechsel lässt sich nachrechnen; es gilt:

$$\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\text{und} \quad \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

(2) *Scherungen im $\mathbb{R}^2$ haben i. a. nur einen Eigenvektor (bis auf skalare Vielfache) .*

Diese Problem kann nicht durch Vergrößerung des Körpers behoben werden; eine Scherung wie z. B. $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ bildet einen Vektor $v = ae_1 + be_2$ auf $ae_1 + b(e_2 + e_1)$ ab. Man kann leicht nachrechnen, dass nur die skalaren Vielfachen von e_1 Eigenvektoren sind, also wenn $b = 0$.

Man kann nun zeigen, dass dies über $\mathbb{C}$ der einzige Hinderungsgrund ist: Durch geeignete Basiswahl erreicht man die sogenannte Jordan'sche [11]Normalform, bei der die Matrix aus Teilmatrizen der folgenden Form ausgebaut ist, die gewissermaßen höherdimensionale Scherungen beschreiben:

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}$$

[11]nach Camille Jordan (1838–1922)

5.4 Lineare Gleichungssysteme

Definition 5.30 *Ein lineares Gleichungssystem (mit m Gleichungen und n Unbekannten) über einem Körper K besteht aus Gleichungen* Lineares Gleichungssystem

$$\begin{array}{ccccccc} a_{11}\cdot x_1 & + & a_{12}\cdot x_2 & +\cdots+ & a_{1n}\cdot x_n & = & b_1 \\ & & & \vdots & & \vdots & \\ a_{m1}\cdot x_1 & + & a_{m2}\cdot x_2 & +\cdots+ & a_{mn}\cdot x_n & = & b_m \end{array}$$

mit $a_{ij}, b_i \in K$ und Unbekannten $x_1, \ldots, x_n$. Eine Lösung *des Gleichungssystems besteht aus Werten $k_1, \ldots, k_n \in K$, welche gleichzeitig alle m Gleichungen erfüllen.*

Das zugehörige homogene (lineare) Gleichungssystem ist

$$\begin{array}{ccccccc} a_{11}\cdot x_1 & + & a_{12}\cdot x_2 & +\cdots+ & a_{1n}\cdot x_n & = & 0 \\ & & & \vdots & & \vdots & \\ a_{m1}\cdot x_1 & + & a_{m2}\cdot x_2 & +\cdots+ & a_{mn}\cdot x_n & = & 0 \end{array}$$

Offenbar kann man das lineare Gleichungssystem in einer Matrix zusammenfassen als

$$A \cdot x = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = b$$

Das lineare Gleichungssystem entspricht also einer linearen Abbildung $A : K^n \to K^m$, als seine Lösungen sucht man die Vektoren im Urbild $A^{-1}[b] = \{v \in K^n \mid A \cdot v = b\}$ des zusätzlich gegebenen Vektors b. Dies motiviert die folgenden Definitionen und Untersuchungen:

Satz und Definition 5.31 *Sei $\varphi : V \to W$ eine K-lineare Abbildung zwischen K-Vektorräumen V und W.* Kern Bild

(a) *Das Bild von φ, also $\mathrm{Bild}(\varphi) = \{\varphi(v) \mid v \in V\}$, ist ein Untervektorraum von W.*
Der Kern von φ, definiert als $\mathrm{Kern}(\varphi) := \{v \in V \mid \varphi(v) = 0\}$, ist ein Untervektorraum von V.

(b) *Es gilt*

$$v \sim_\varphi v' :\iff \varphi(v) = \varphi(v') \iff v - v' \in \mathrm{Kern}(\varphi)$$

Die Äquivalenzklassen dieser Äquivalenzrelation sind die Nebenklassen von $\mathrm{Kern}(\varphi)$ von der Form $v_0 + \mathrm{Kern}(\varphi) := \{v_0 + v \mid v \in \mathrm{Kern}(\varphi)\}$.

Beweis: (a) Da $\varphi(0_V) = 0_W$ ist $0_V \in \mathrm{Kern}(\varphi)$ und $0_W \in \mathrm{Bild}(\varphi)$.

Seien $w_1 = \varphi(v_1)$ und $w_2 = \varphi(v_2)$ in $\mathrm{Bild}(\varphi)$. Dann sind $w_1 + w_2 = \varphi(v_1 + v_2)$ und $k \cdot w_1 = \varphi(k \cdot v_1)$ ebenfalls in $\mathrm{Bild}(\varphi)$, also ist $\mathrm{Bild}(\varphi)$ ein Untervektorraum.

Seien $v_1, v_2 \in \mathrm{Kern}(\varphi)$. Dann ist $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) = 0 + 0 = 0$ und $\varphi(k \cdot v_1) = k \cdot \varphi(v_1) = k \cdot 0 = 0$. Also ist auch $\mathrm{Kern}(\varphi)$ ein Untervektorraum.

(b) Es ist $\varphi(v) = \varphi(v') \iff \varphi(v - v') = \varphi(v) - \varphi(v') = 0 \iff v - v' \in \mathrm{Kern}(\varphi)$. □

Für ein $w \in W$ gibt es also zwei mögliche Fälle:

- entweder $w \notin \mathrm{Bild}(\varphi)$ und $\varphi^{-1}[w] = \emptyset$

- oder $w \in \text{Bild}(\varphi)$ und $\varphi^{-1}[w]$ ist die Nebenklasse $v + \text{Kern}(\varphi)$ von $\text{Kern}(\varphi)$ mit für ein v mit $\varphi(v) = w$.

Wenn $\varphi : V \to W$ eine K-lineare Abbildung ist, kann man auf $V/_{\sim_\varphi}$ (was man üblicherweise $V/\text{Kern}(\varphi)$ schreibt) so eine K-Vektorraum-Struktur definieren, dass $V \to V/\text{Kern}(\varphi), v \mapsto v/_{\sim_\varphi}$ eine K-lineare Abbildung wird. Die Zerlegung auf Seite 5 ergibt im Falle einer linearen Abbildung dann eine Folge von *linearen* Abbildungen:

$$\begin{array}{ccccccc} & \text{surjektiv} & & & \text{bijektiv} & & \text{injektiv} & \\ V & \longrightarrow & V/\text{Kern}(\varphi) & \longrightarrow & \text{Bild}(\varphi) & \longrightarrow & W \\ v & \mapsto & v/_{\sim_\varphi} & \mapsto & \varphi(v) & \mapsto & \varphi(v) \end{array}$$

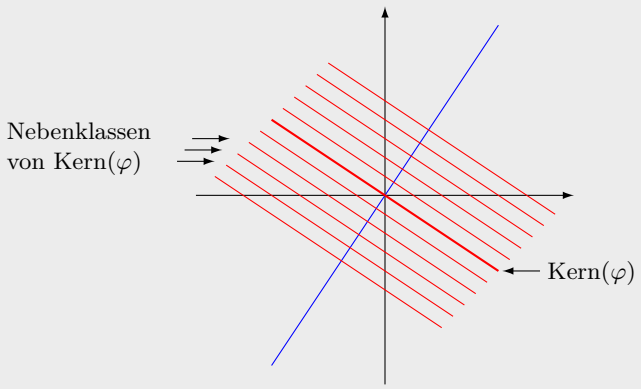
Dieses Ergebnis heißt auch *Homomorphiesatz* (für Vektorräume).

Folgerung 5.32 *φ ist injektiv* $\iff \text{Kern}(\varphi) = \{0\} \iff \dim \text{Kern}(\varphi) = 0.$

φ ist surjektiv $\iff \text{Bild}(\varphi) = \{W\} \overset{\text{falls } W \text{ endlich-dimensional}}{\iff} \dim \text{Bild}(\varphi) = \dim W.$

Beweis: Der erste Teil folgt direkt aus Satz 5.31. Beim zweiten Teil ist die Äquivalenz die Definition von Surjektivität. Die zweite Äquivalenz folgt, weil ein echter Untervektorraum eines endlich-diemnsionalen Vektorraums kleinere Dimension hat: Eine Basis B des Untervektorraums ist noch keine Basis von W, kann aber zu einer Basis von W ergänzt werden, hat also weniger Elemente. □

Betrachte die lineare Abbilung $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, welche die senkrechte Projektion auf die (blaue) Gerade darstellt. Diese Gerade ist das Bild von φ; die im Ursprung dazu senkrecht stehende (fette rote) Gerade ist der Kern von φ. Die Parallelen dazu sind die Nebenklassen des Kerns, und zwar ist jede dieser Geraden das volle Urbild ihres Schnittpunktes mit der blauen Geraden.



Satz 5.33 (Dimensionssatz) *Sei $\varphi : V \to W$ linear. Dann gilt*

$$\dim V = \dim \text{Kern}(\varphi) + \dim \text{Bild}(\varphi)$$

Beweis: [12] Sei $l = \dim \text{Kern}(\varphi)$ und $n = \dim V$ und wähle eine Basis $\{v_1, \ldots, v_l\}$ von $\text{Kern}(\varphi)$. Diese ist eine lineare unabhängige Teilmenge von V, kann also zu einer maximal linear unabhängigen Teilmenge $\{v_1 \ldots, v_l, v_{l+1}, \ldots, v_n\}$ ergänzt werden, d. h. zu einer Basis von V. Zu

[12] Für endlich-dimensionales V; der Beweis funktioniert mit den entsprechenden Modifikationen aber auch für unendlich-dimensionale Vektorräume.

zeigen ist also $n - l = \dim \text{Bild}(\varphi)$, indem gezeigt wird, dass $\varphi(v_{l+1}), \ldots, \varphi(v_n)$ eine Basis ohne Doppelnennungen von $\text{Bild}(\varphi)$ ist.

Sei $w = \varphi(a_1 v_1 + \cdots + a_n v_n) \in \text{Bild}(\varphi)$. Dann ist $w = a_1\varphi(v_1) + \cdots + a_n\varphi(v_n) = a_{l+1}\varphi(v_{l+1}) + \cdots + a_n\varphi(v_n)$, da $\varphi(v_1) = \cdots = \varphi(v_l) = 0$. Also ist $\varphi(v_{l+1}), \ldots, \varphi(v_n)$ ein Erzeugendensystem von $\text{Bild}(\varphi)$.

Zu zeigen bleibt die lineare Unabhängigkeit, mit Lemma 4.12: Sei also $0 = b_{l+1}\varphi(v_{l+1}) + \cdots + b_n\varphi(v_n) = \varphi(b_{l+1}v_{l+1} + \cdots + b_n v_n) \in \text{Kern}(\varphi)$. Da $v_1, \ldots, v_l$ eine Basis von $\text{Kern}(\varphi)$ ist, gibt es $b_1, \ldots, b_l$ mit $b_{l+1}v_{l+1} + \cdots + b_n v_n = b_1 v_1 + \cdots + b_l v_l$, oder $(-b_1)v_1 + \cdots + (-b_l)v_l + b_{l+1}v_{l+1} + \cdots + b_n v_n = 0$. Aus der linearen Unabhängigkeit der Basis $v_1, \ldots, v_n$ folgt nun aber $b_1 = \cdots = b_n = 0$. □

Satz 5.34 *Sei $\varphi : V \to W$ linear und $\dim V = \dim W$ endlich. Dann ist φ injektiv, genau dann wenn surjektiv (und damit genau dann, wenn bijektiv).*

Beweis: Wenn φ injektiv ist , dann ist $\dim W = \dim V = \dim \text{Kern}(\varphi) + \dim \text{Bild}(\varphi) = 0 + \dim \text{Bild}(\varphi) = \dim \text{Bild}(\varphi)$. Also ist φ nach Corollar 5.32 surjektiv.

Wenn φ surjektiv ist, dann ist $\dim \text{Kern}(\varphi) = \dim V - \dim \text{Bild}(\varphi) = \dim W - \dim \text{Bild}(\varphi) = 0$. Also ist φ nach Corollar 5.32 injektiv. □

Folgerung 5.35 *Insbesondere gilt für $(n \times n)$-Matrizen A und B:*
Wenn $A \cdot B = I_n$ (also die durch B beschriebene lineare Abbildung $K^n \to K^n$ injektiv und die durch A beschriebene Abbilddung surjektiv), dann ist $B = A^{-1}$ und $A = B^{-1}$.

Achtung: Für lineare Abbildungen $\varphi, \psi : V \to V$ eines unendlichen-dimensionalen Vektorraums V folgt aus $\psi \circ \varphi = \text{id}$ nicht, dass φ und ψ invertierbar sind!

Angewandt auf ein lineares Gleichungssystem $A \cdot x = b$ gibt es die beiden bereits besprochenen Möglichkeiten:

- entweder $b \notin \text{Bild}(A)$ und es gibt keine Lösung
- oder $b \in \text{Bild}(A)$ und die Lösungsmenge besteht aus einer Nebenklasse $c + \text{Kern}(A)$, wobei c irgendeine Lösung des Gleichungssystems ist.

Um die Lösungsmenge des Gleichungssytems zu bestimmen, muss man also eine sogenannte *spezielle Lösung* c finden – sofern sie existiert! – und den Kern von A bestimmen. Ist $v_1, \ldots, v_l$ eine Basis des Kerns, so besteht die Lösungsmenge („die *allgemeine Lösung*“) also aus allen Vektoren der Form $c + k_1 v_1 + \cdots + k_l v_l$ mit $k_i \in K$.

Definition 5.36 *Der Rang einer $(m \times n)$-Matrix A, $\text{rg}(A)$, ist die Dimension des Bildes von A als linearer Abbildung $K^n \to K^m$, d. h. die Dimension des von den Spalten $A \cdot e_1, \ldots, A \cdot e_n$ von A erzeugten Unterraums.* Rang einer Matrix

Nach Definition ist $\text{rg}(A) \leqslant m$ und $= m$ genau dann, wenn A surjektiv ist. Außerdem gilt $n = \dim \text{Kern}(A) + \text{rg}(A)$ nach Satz 5.33. Aus all den vorstehenden Überlegungen und Sätzen ergibt sich nun:

Satz 5.37 *Falls A die Matrix eines homogenen linearen Gleichungssystemes mit m Gleichungen und n Unbekannten ist, dann ist die Dimension des Lösungsraums $n - \text{rg}(A)$.*

Das Gauß-Verfahren zum Lösen linearer Gleichungssysteme

Die Idee des Verfahrens besteht darin, das Gleichungssystem bzw. die Matrix durch eine Reihe „elementarer Umformungen“, die die Lösungsmenge nicht oder in einer kontroliierten Weise ändern, in eine „schöne Form“ zu bringen, aus der man die Lösungsmenge leicht errechnen kann.

elementare Umformungen

Definition 5.38 *Wir betrachten hier drei Arten von elementaren Umformungen. Jede entspricht der Multiplikation von links mit einer invertierbaren Matrix M. Dann gilt*

$$A \cdot v = b \iff MA \cdot v = M \cdot b$$

und wegen $M \cdot 0 = 0$ ist insbesondere $\mathrm{Kern}(MA) = \mathrm{Kern}(A)$, d. h. die Lösungsmenge ändert sich nicht, wenn A und b gleichermaßen umgeformt werden.

(1) Vertauschung der i-ten mit der j-ten Gleichung bzw.
Vertauschung der i-ten mit der j-ten Zeile der Matrix A und des Vektors b.

Dies entspricht der Multiplikation von links mit der Matrix $M_{(ij)} = M_{(ij)}^{-1}$ (siehe Seite 37).

(2) Addition des k-fachen der j-ten Gleichung zur i-ten Gleichung ($i \neq j$) bzw.
Addition des k-fachen der j-ten Zeile der Matrix A und des Vektors b zur i-ten Zeile.

Dies entspricht der Multiplikation von links mit der Matrix $E_{ij}(k) = I_m + k \cdot E_{ij}$ (E_{ij} ist die Standardbasenmatrix aus Satz 5.21). Es gilt offenbar $E_{ij}(k)^{-1} = E_{ij}(-k)$.

(3) Multiplikation der i-ten Gleichung mit $k \neq 0$ bzw.
Multiplikation der i-ten Zeile der Matrix A und des Vektors$b$ mit $k \neq 0$.

*Dies entspricht der Multiplikation von links mit der Matrix $E_i(k) = I_m + (k-1) \cdot E_{ii}$.
Es gilt offenbar $E_i(k)^{-1} = E_i(k^{-1})$.*

Ergänzend können auch Operationen auf den Spalten der Matrix vorgenommen werden (z. B. Vertauschungen der Spalten, die dann den entsprechenden Vertauschungen der Unbekannten entsprechen). Diese sind aber nur zur Verbesserung von Algorithmen hinsichtlich Stabilität notwendig.

Zeilenstufenform, Pivot-Spalten und -Elemente

Definition 5.39 *Eine Matrix A ist in Zeilenstufenform, falls es ein $r \in \mathbb{N}$ und $j_1 < \cdots < j_r$ gibt, so dass $a_{1j_1} \neq 0, \ldots, a_{rj_r} \neq 0$ und*

$$a_{ij} = 0, \text{ falls } \begin{cases} j < j_k \text{ und } i \geqslant k \text{ für } k = 1, \ldots, r-1 \\ \text{oder } i > r \end{cases}$$

Die Elemente a_{ij_i} heißen Pivot-Elemente, die Spalten $j_1, \ldots, j_r$ Pivot-Spalten.

Schematisch angedeutet sieht eine Zeilenstufenform (mit $r = 3$) wie folgt aus; $*$ steht für beliebige Elemente:

$$\begin{pmatrix} 0 & a_{1j_1} & * & * & * & * & * \\ 0 & 0 & a_{2j_2} & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & a_{3j_3} & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Satz 5.40 (a) *Jede Matrix kann durch elementare Umformungen der Art (1) und (2) in Zeilenstufenform gebracht werden.* [13]

(b) *Jede invertierbare Matrix kann durch elementare Umformungen der Art (1), (2) und (3) in die Identitätmatrix überführt werden.*

BEWEIS: Für (a) gibt es den folgenden Algorithmus, das sogenannte Gauß-Verfahren [14]:

Input: $(m \times n)$-Matrix A. Setze $i = 1, j = 1$.

Ist $a_{ij} \neq 0$?

- Ja: ersetze Zeile $k = i+1, \ldots, n$ durch „Zeile $k - \frac{a_{kj}}{a_{ij}} \cdot$ Zeile i“ und ersetze i durch $i+1$ und j durch $j+1$
- Nein: Gibt es ein $l > i$ mit $a_{lj} \neq 0$?
  - Ja: vertausche Zeile i mit Zeile l (für das kleinste l)
  - Nein: ersetze j durch $j+1$

Falls $i > m$ oder $j > n$: Ende

Die Matrix wird spaltenweise von links nach rechts und zeilenweise von oben nach unten so abgearbeitet, dass die gewünschten Nullen auftreten. Betrachtet wird immer nur der Teil unterhalb der aktuellen Stelle: Ein eventuell vorhandener Eintrag $\neq 0$ in der Spalte wird ggf. durch Zeilenvertauschung an die betrachtete Stelle gebracht; durch die Addition eines passenden Vielfachens der Zeile werden unterhalb der betrachteten Stelle Nullen erzeugt. (Ein formaler Korrektheitsbeweis unterbleibt hier).

Für (b) gibt es die oft Gauß-Jordan-Verfahren genannte Fortführung des Algorithmus:

Input: $(n \times n)$-Matrix A. Führe zunächst das Gauß-Verfahren durch.

Sind alle $a_{ii} \neq 0$?

- Nein: die Matrix ist nicht invertierbar
- Ja: Setze $j = n$
  ersetze Zeile $k = 1, \ldots, j-1$ durch „Zeile $k - \frac{a_{kj}}{a_{jj}} \cdot$ Zeile j“
  und ersetze Zeile j durch „Zeile $\frac{1}{a_{jj}} \cdot$ Zeile j“
  und ersetze j durch $j-1$

Falls $j < 1$: Ende

[13] Man kann auch auf die elementaren Umformungen der ersten Art verzichten: Statt die Zeilen i und l zu vertauschen, könnte man im Algorithmus auch Zeile l zu Zeile i hinzuaddieren.

[14] nach Carl Friedrich Gauß (1777–1855)

Durch das Gauß-Verfahren bringt man zunächst die Matrix in Zeilenstufenform. Sie ist genau dann invertierbar, wenn jede Spalte Pivot-Spalte ist, d. h. wenn die Pivot-Elemente die Diagonalelemente $a_{11}, \ldots, a_{nn}$ sind. Man kann nun mit einem „punktgespiegelten“ Gauß-Verfahren, also spaltenweise von rechts nach links und zeilenweise von unten nach oben arbeitend, eine Diagonalmatrix errreichen (d. h. außer es gilt $a_{ij} = 0$ für alle $i \neq j$.) Durch Umformungen der Art (3) kann man außerdem die Diagonaleinträge auf 1 bringen. □

Beispiel 5.41 (für das Gauß-Verfahren, in $\mathbb{R}$)

– *die aktuelle Position des Algorithmus ist umrahmt*
– *betrachtete Einträge sind blau, gefundene Pivot-Elemente rot markiert*

1. Schritt, $i = 1, j = 1$

$$\begin{pmatrix} \boxed{0} & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 4 & 2 & -2 & 2 & 6 \\ 0 & -2 & -1 & 1 & 1 & 1 \end{pmatrix}$$

Spalte 1 ist keine Pivot-Spalte

2. Schritt, $i = 1, j = 2$

$$\begin{pmatrix} 0 & \boxed{0} & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 4 & 2 & -2 & 2 & 6 \\ 0 & -2 & -1 & 1 & 1 & 1 \end{pmatrix}$$

Zeile 1 und 2 werden vertauscht

3. Schritt

$$\begin{pmatrix} 0 & \boxed{2} & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & -2 & 2 & 6 \\ 0 & -2 & -1 & 1 & 1 & 1 \end{pmatrix}$$

0 mal Zeile 1 zu Zeile 2
-2 mal Zeile 1 zu Zeile 3
1 mal Zeile 1 zu Zeile 4

4. Schritt, $i = 2, j = 3$

$$\begin{pmatrix} 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 0 & \boxed{0} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Spalte 3 ist keine Pivot-Spalte

5. Schritt, i=2, j=4

$$\begin{pmatrix} 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & \boxed{0} & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Spalte 4 ist keine Pivot-Spalte

6. Schritt, $i = 2, j = 5$

$$\begin{pmatrix} 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \boxed{0} & 0 \\ 0 & 0 & 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Zeile 2 und 3 werden vertauscht

7. Schritt

$$\begin{pmatrix} 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \boxed{2} & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

0 mal Zeile 2 zu Zeile 3
$-\frac{1}{2}$ mal Zeile 2 zu Zeile 4

8. Schritt, $i = 3, j = 6$ $\begin{pmatrix} 0 & 2 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & \boxed{0} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ Spalte 6 ist keine Pivot-Spalte
Ende bei $i = 3, j = 7$

Was kann mit dem Gauß-Verfahren berechnet werden?

Sei nun stets A eine Matrix, die durch die invertierbare Matrix E in Zeilenstufenform gebracht wird, d. h. E ist eine Matrix $E_k \cdot \ldots \cdot E_1$, wobei $E_1, \ldots, E_k$ Matrizen zu elementaren Umformungen sind, welche nach dem Gauß-Verfahren A in eine Matrix $B := E_k \cdot \ldots \cdot E_1 \cdot A$ in Zeilenstufenform umformen.

Den Rang einer Matrix berechnen:

Der Rang der Matrix ist die Anzahl der Pivot-Elemente in der Zeilenstufenform.

Im Beispiel 5.41 ist der Rang der Matrix also 2.

Eine spezielle Lösung eines linearen Gleichungssystems ausrechnen:

Man bringt das Gleichungssystem in Zeilenstufenform $EA \cdot x = E \cdot b$ und löst die Gleichungen von unten nach oben auf („Rückwärtseinsetzen“). Sind Unbekannte durch eine Gleichung und die vorherigen Festsetzungen nicht eindeutig bestimmt, setzt man einen beliebigen Wert (am Besten 0) ein.

Beispiel 5.42 (für das Lösen eines linearen Gleichungssystems)
Angenommen, es liegt folgendes lineares Gleichungssystem über $\mathbb{R}$ vor:

$$\begin{array}{rcrcrcrcrcl} 2x_1 & - & x_2 & + & x_3 & & & + & x_5 & = & a \\ 4x_1 & - & 2x_2 & + & 6x_3 & + & 2x_4 & + & 6x_5 & = & b \\ -2x_1 & + & x_2 & + & x_3 & + & x_4 & + & x_5 & = & c \end{array}$$

Es wird in Matrizenform „übersetzt“

$$\left(\begin{array}{rrrrr|c} 2 & -1 & 1 & 0 & 1 & a \\ 4 & -2 & 6 & 2 & 6 & b \\ -2 & 1 & 1 & 1 & 1 & c \end{array}\right)$$

und durch das Gauß-Verfahren in Zeilnetsufenform umgeformt zu:

$$\left(\begin{array}{rrrrr|c} 2 & -1 & 1 & 0 & 1 & a \\ 0 & 0 & 4 & 2 & 4 & b - 2a \\ 0 & 0 & 0 & 0 & 0 & 4a - b + 2c \end{array}\right)$$

Falls $4a - b + 2c \neq 0$, z. B. für $a = b = c = 1$, gibt es keine Lösung.

Falls $4a - b + 2c = 0$ gibt es Lösungen: Da der Rang der Matrix 2 ist, besteht zwischen den drei Gleichungen nud diese eine lineare Abhängigkeit. Für z. B. $a = 1, b = 3, c = -0,5$ hat man also das Gleichungssystem umgeformt in

$$\left(\begin{array}{rrrrr|c} 2 & -1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 4 & 2 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

bzw.

$$\begin{aligned} 2x_1 - x_2 + x_3 + x_5 &= 1 \\ 4x_3 + 2x_4 + 4x_5 &= 1 \end{aligned}$$

Um eine spezielle Lösung zu findne, beginnt man mit der untersten Gleichung: Sie legt x_3 in Abhängigkeit von x_4 und x_5 fest, die selbst nicht festgelegt sind. Man setzt daher (z. B.) $x_4 = x_5 = 0$ und löst $4x_3 + 2 \cdot 0 + 4 \cdot 0 = 1$ nach $x_3 = \frac{1}{4}$ auf.

Dann geht man zur nächsten Gleichung, setzt die bislang festgelegten bzw. errechneten Werte ein, setzt $x_2 = 0$, da nicht festgelegt, und löst $2x_1 - 0 + \frac{1}{4} + 0 = 1$ nach $x_1 = \frac{3}{8}$ auf.

Als eine spezielle Lösung erhält man also $(\frac{3}{8}, 0, \frac{1}{4}, 0, 0)$ und überprüft leicht durch Einsetzen in das ursprüngliche Gleichungssystem, dass man sich nicht verrechnet hat. Für andere Werte von x_2, x_4, x_5 bekommt man andere Lösungen.

Eine Basis des Kerns bestimmen:

Man bringt das homogene Gleichungssystem in Zeilenstufenform $EA \cdot x = E \cdot 0 = 0$. Ist der Rang der Matrix gleich n (= Anzahl der Unbekannten), so ist $\mathrm{Kern}(A) = \{0\}$, die Basis also die leere Menge. Andernfalls löst man die Gleichungen von unten nach oben durch Rückwärteinsetzen auf. Für jede Unbekannte, die nicht eindeutig festgelegt ist, bekommt man einen Basisvektor des Kerns, indem man diese Unbekannte auf 1 setzt und alle andern dann nicht festgelegten Unbekannten auf 0.

Fortsetzung der vorherigen Beispiels:

Es werden nun alle Lösungen des zugehörigen *homogenen* linearen Gleichungssystems

$$\begin{aligned} 2x_1 - x_2 + x_3 + x_5 &= 0 \\ 4x_1 - 2x_2 + 6x_3 + 2x_4 + 6x_5 &= 0 \\ -2x_1 + x_2 + x_3 + x_4 + x_5 &= 0 \end{aligned}$$

gesucht. Äquivalent: Es soll der Kern der zugehörigen linearen Abbildung bestimmt werden. Die Umformung in Zeilenstufenform ergab

$$\left(\begin{array}{ccccc|c} 2 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Der Rang der Matrix ist 2, die Dimension des Kerns also $5 - 2 = 3$. Von unten nach oben gesehen sind x_5, x_4 und x_2 nicht festgelegt. Diese setzt man der Reihe nach $= 1$ und die anderen beiden $= 0$, und rechnet x_3 und x_1 jeweils aus den Gleichungen $2x_1 - x_2 + x_3 + x_5 = 0$ und $4x_3 + 2x_4 + 4x_5 = 0$ aus.

Für $x_5 = 1$ und $x_4 = x_2 = 0$ erhält man $x_3 = -1$ und $x_1 = 0$, also ist $(0, 0, -1, 0, 1)$ im Kern.
Für $x_4 = 1$ und $x_5 = x_2 = 0$ erhält man $x_3 = -\frac{1}{2}$ und $x_1 = \frac{1}{4}$, also ist $(\frac{1}{4}, 0, -\frac{1}{2}, 1, 0)$ im Kern.
Für $x_2 = 1$ und $x_5 = x_4 = 0$ erhält man $x_3 = 0$ und $x_1 = \frac{1}{2}$, also ist $(\frac{1}{2}, 1, 0, 0, 0)$ im Kern.

Die drei Vektoren $(0, 0, -1, 0, 1), (\frac{1}{4}, 0, -\frac{1}{2}, 1, 0), (\frac{1}{2}, 1, 0, 0, 0)$ bilden nun eine Basis des Kerns, d. h. der Kern (= die Lösungsmenge des homogenen Gleichungssystems) ist

$$\left\{ r_1 \cdot (0, 0, -1, 0, 1) + r_2 \cdot (\tfrac{1}{4}, 0, -\tfrac{1}{2}, 1, 0) + r_3 \cdot (\tfrac{1}{2}, 1, 0, 0, 0) \;\middle|\; r_1, r_2, r_3 \in \mathbb{R} \right\}.$$

Die Lösungsmenge des ursprünglichen Gleichungssystems mit $a = 1, b = 3, c = -0,5$ ist dann

$$\left\{ (\tfrac{3}{8}, 0, \tfrac{1}{4}, 0, 0) + r_1 \cdot (0, 0, -1, 0, 1) + r_2 \cdot (\tfrac{1}{4}, 0, -\tfrac{1}{2}, 1, 0) + r_3 \cdot (\tfrac{1}{2}, 1, 0, 0, 0) \;\middle|\; r_1, r_2, r_3 \in \mathbb{R} \right\}.$$

Eine Basis des Bilds bestimmen:

Spalten $Ae_{i_1}, \ldots, Ae_{i_l}$ von A sind genau dann linear unabhängig, wenn die entsprechenden Spalten $EAe_{i_1}, \ldots, EAe_{i_l}$ der Matrix in Zeilenstufenform linear unabhängig sind. Also bilden die Spalten von A, die Pivot-Spalten von EA sind, eine Basis des Bildes.

Im Beispiel 5.41 bilden also die Vektoren $(0, 2, 4, -2)$ und $(0, 0, 2, 1)$ eine Basis des Bildes der Ausgangsmatrix.

Eine Menge linear unabhängiger Vektoren zu einer Basis ergänzen:

Man fügt die Vektoren als Spalten zu einer $(m \times n)$-Matrix A zusammen und bestimmt eine Basis des Bildes der $(m \times (n+m))$-Matrix $(A \mid I_m)$ wie oben beschrieben.

alternativ: Man fügt die Vektoren als Zeilen zu der $(n \times m)$-Matrix A^{T} zusammen und bringt sie in Zeilenstufenform. Diejenigen Standardbasisvektoren e_i, für die i keine Pivot-Spalte ist, ergänzen die gegebenen Vektoren zu einer Basis.

Testen, ob eine Matrix invertierbar ist:

Eine Matrix ist genau dann invertierbar, wenn sie quadratisch ist und der Rang mit der Anzahl der Spalten (bzw. Zeilen) übereinstimmt. Anders ausgedrückt: die Zeilenstufenform hat Diagonalgestalt, d. h. alle Einträge b_{ii} sind Pivot-Elemente $\neq 0$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{nicht invertierbar!}$$

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & -4 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 9 \end{pmatrix} \quad \text{invertierbar!}$$

Das Inverse einer Matrix berechnen:

Die elementaren Umformungen, welche A nach dem Gauß-Jordan-Verfahren in die Identitätsmatrix umformen, formen gleichzeitig die Identitätsmatrix in die Inverse von A um: falls $E \cdot A = I_n$, so ist $E \cdot I_n = A^{-1}$.

$$\left(\begin{array}{ccc|ccc} 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & -4 & 1 & 0 & -2 & 1 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 9 & 4 & -2 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{4}{9} & -\frac{2}{9} & \frac{1}{9} \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & \frac{1}{9} & \frac{4}{9} & -\frac{2}{9} \\ 0 & 0 & 1 & \frac{4}{9} & -\frac{2}{9} & \frac{1}{9} \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{2}{9} & \frac{1}{9} & \frac{4}{9} \\ 0 & 1 & 0 & \frac{1}{9} & \frac{4}{9} & -\frac{2}{9} \\ 0 & 0 & 1 & \frac{4}{9} & -\frac{2}{9} & \frac{1}{9} \end{array}\right)$$

Es ist daher $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}^{-1} = \frac{1}{9} \cdot \begin{pmatrix} -2 & 1 & 4 \\ 1 & 4 & -2 \\ 4 & -2 & 1 \end{pmatrix}$

Definition 5.43 *Die Transponierte A^{T} einer $(m \times n)$-Matrix $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ ist die „an der Diagonalen gespiegelte“ $(n \times m)$-Matrix $(a_{ji})_{\substack{j=1,\dots,n \\ i=1,\dots,m}}$.*

Transponierte Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \qquad A^{\mathrm{T}} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

Satz 5.44 *Man sieht leicht, dass $(A \cdot B)^{\mathrm{T}} = B^{\mathrm{T}} \cdot A^{\mathrm{T}}$. Insbesondere ist die Transponierte einer invertierbaren Matrix selbst invertierbar mit $(A^{\mathrm{T}})^{-1} = (A^{-1})^{\mathrm{T}}$.*

Satz 5.45 $\operatorname{rg}(A) = \operatorname{rg}(A^{\mathrm{T}})$.

Beweis: Man sieht, dass der Satz für Matrizen in Zeilenstufenform gilt. Da Isomorphismen die Dimension bewahren, ändert die Multiplikation von rechts oder links mit einer invertierbaren Matrix nicht den Rang einer Matrix. Sei also $E \cdot A$ in Zeilenstufenform für ein invertierbares E. Dann gilt: $\operatorname{rg}(A) = \operatorname{rg}(E \cdot A) = \operatorname{rg}((E \cdot A)^{\mathrm{T}}) = \operatorname{rg}(A^{\mathrm{T}} \cdot E^{\mathrm{T}}) = \operatorname{rg}(A^{\mathrm{T}})$. □

Aus dem Gauß-Verfahren gewinnt man auch einen Beweis für Satz 4.17 im endlich-dimensionalen Fall. Allerdings müsste man sich noch davon überzeugen, dass der Satz für das Gauß-Verfahren nicht gebraucht wurde (und man muss aufpassen, dass man keine Begriffe oder Argumente verwendet, welche bereits auf der Dimension beruhen, wie z. B. den Rang).

Satz 5.46 *Wenn ein Vektorraum V eine Basis mit endlich vielen Elementen besitzt, dann haben alle Basen von V die gleiche Anzahl von Elementen.*

Beweis: Angenommen V hat Basen mit m und mit n Elementen, $m < n$. über die eine Basis ist V isomorph zu K^m; man kann also annehmen, dass $V = K^m$. Nun stellt man die $(m \times n)$-Matrix A auf, deren Spalten die Vektoren der Basis mit n Elementen sind. Diese sind nach Annahme linear unabhängig, also müssen auch die Spalten der in Zeilenstufenform gebrachten Matrix linear unabhängig sein. In der Zeilenstufenform sieht man aber, dass maximal m Spalten linear unabhängig sein können: Widerspruch. □

6 Länge, Winkel, Volumen

In diesem Abschnitt werden nur die endlich-dimensionalen $\mathbb{R}$-Vektorräume $\mathbb{R}^n$ betrachtet. Es sollen nun die geometrisch anschaulichen Begriffe der Länge eines Vektors, des Abstandes zweier Vektoren und des Winkels zwischen zwei Vektoren eingeführt werden. Dabei ist das Vorgehen wie folgt: Man findet eine Formel für die Berechnung, die in den Fällen der Dimension 1, 2 und 3 das Richtige tut und die Eigenschaften besitzt, die man von den Begriffen erwartet. In den höherdimensionalen Fällen, wo eine direkte geometrische Anschauung fehlt, definiert man die Begriffe dann durch diese Formel.

6.1 Norm und Metrik

Als Länge eines Vektors (v) im $\mathbb{R}^1$ sieht man natürlich den Betrag $|v| = \sqrt{v^2}$ an. Die Länge eines Vektors $(v_1, v_2) = v_1 \cdot e_1 + v_2 \cdot e_2 \in \mathbb{R}^2$ berechnet sich dann nach dem Satz des Pythagoras als $\sqrt{v_1^2 + v_2^2}$, ebenso die Länge eines Vektors $(v_1, v_2, v_3) \in \mathbb{R}^3$ durch zweimalige Anwendung des Satzes von Pythagoras als

$$\sqrt{(\text{Länge von } v_1 e_1 + v_2 e_2)^2 + v_3^2} = \sqrt{\sqrt{v_1^2 + v_2^2}^2 + v_3^2} = \sqrt{v_1^2 + v_2^2 + v_3^2}$$

Die Länge eines Vektors $v \cdot e_i$ im $\mathbb{R}^n$ sieht man sinnvollerweise ebenfalls als $|v|$ an, auch wenn man keine geometrische Anschauung dieses Raumes hat, und wenn man die Gültigkeit des Satzes des Pythagoras auch für Ebenen im n-dimensionalen Raum annimmt, erhält man durch sukuzessive Anwendung die Definition:

Länge
Abstand

Definition 6.1 *Die Länge oder Norm eines Vektors $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$ ist*

$$\|v\| := \sqrt{v_1^2 + \cdots + v_n^2}.$$

Der Abstand (oder die Distanz) zweier Vektoren ist

$$\mathrm{d}(v,w) := \|v - w\|.$$

Die Abbildung $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ heißt auch eine Metrik.

Es gilt offenbar $\|v\| = d(v, 0)$, man kann also sowohl den Abstand aus der Länge definieren (wie oben) als auch umgekehrt die Länge aus dem Abstand. Im $\mathbb{R}^2$ und $\mathbb{R}^3$ ist dies nach dem Satz des Pythagoras der gewöhnlichen Längen- bzw. Abstandsbegriff. Auch im $\mathbb{R}^1$ gilt $\|v\| = \sqrt{v^2} = |v|$.

Satz 6.2 (Eigenschaften von Länge und Abstand) *Für alle $u, v, w \in \mathbb{R}^n$ und $r \in \mathbb{R}$ gilt:*

Positivität:	$\|v\| \geqslant 0$	$\mathrm{d}(v, w) \geqslant 0$
	$\|v\| = 0 \Leftrightarrow v = 0$	$\mathrm{d}(v, w) = 0 \Leftrightarrow v = w$
Symmetrie:	$\|v\| = \|-v\|$	$\mathrm{d}(v, w) = \mathrm{d}(w, v)$
Dreiecksungleichung:	$\|v + w\| \leqslant \|v\| + \|w\|$	$\mathrm{d}(v, w) \leqslant \mathrm{d}(v, u) + \mathrm{d}(u, w)$
Homogenität:	$\|r \cdot v\| = \|r\| \cdot \|v\|$	$\mathrm{d}(r \cdot v, r \cdot w) = \|r\| \cdot \mathrm{d}(v, w)$

Neben diesem gewöhnlichen Längenbegriff (der auch „euklidische Norm“ [15] oder „2-Norm“ $\|v\|_2$ genannt wird), gibt es im Mehrdimensionalen auch weitere Möglichkeiten, Längen und Anstände zu

[15] nach Euklid von Alexandria (vermutlich 3. Jahrhundert v. Chr.)

messen, etwa durch die „1-Norm“ $\|v\|_1 = |v_1| + \cdots + |v_n|$ oder durch die „Maximumsnorm“ $\|v\|_\infty := \max\{|v_1|, \ldots, |v_n|\}$. Diese Normen und ihre zugehörigen Metriken erfüllen alle oben genannten Eigenschaften. Umgekehrt nennt man jede Abbildung mit diesen Eigenschaften Norm bzw. Metrik [16] und fasst sie als zulässigen Längen- bzw. Abstandsbegriff auf.

6.2 Determinante

Die Ergebnisse in diesem Abschnitt werden nur inhaltlich motiviert, aber nicht bewiesen!

Die Determinante einer linearen Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ soll die Volumenänderung durch die Abbildung φ messen. Dabei ist zum einen das *n-dimensionale Volumen* gemeint: Der n-dimensionale Hyperwürfel $[0,1]^n \subseteq \mathbb{R}^n$ hat das n-dimensionale Volumen 1; eine $(n-1)$-dimensionale Ebene im $\mathbb{R}^n$ hat dagegen das n-dimensionale Volumen 0. Ein *Parallelepiped* ist die n-dimensionale Verallgemeinerung eine Parallelogramms. Sein Volumen berechnet sich sukzessive durch die Formel „Grundfläche × Höhe“.

Die Linearität von φ bewirkt, dass die Volumenänderung durch φ überall gleich ist. Es reicht also, das Volumen des durch $\varphi(e_1), \ldots, \varphi(e_n)$ aufgespannten Parallelepipeds zu berechnen, da diese Volumen auch die Veränderung angibt gegenüber dem von $e_1, \ldots, e_n$ aufgespannten Parallelepiped, also dem Hyperwürfels mit Volumen 1.

Zum andern soll die Volumenänderung (bzw das Volumen) zusätzlich *orientiert*, also mit einem Vorzeichen versehen, sein:

- Im 1-Dimensionalen gibt ein negatives Vorzeichen an, dass sich die Richtung des Vektors $\varphi(e_1)$ im Vergleich zu e_1 umdreht.
- Im 2-Dimensionalen gibt ein negatives Vorzeichen an, dass die kürzeste Drehrichtung von $\varphi(e_1)$ zu $\varphi(e_2)$ im Uhrzeigersinn ist (während die kürzeste Drehrichtung von e_1 zu e_2 gegen den Uhrzeigersinn ist).
- Im 3-Dimensionalen gibt ein negatives Vorzeichen an, dass $(\varphi(e_1), \varphi(e_2), \varphi(e_3))$ ein Linkssystem bildet (während (e_1, e_2, e_3) ein Rechtssystem ist.

Man kann sich nun im 1-, 2- und 3-Dimensionalen überlegen, dass das orientierte Volumen folgende Eigenschaften besitzt:

„Multilinear in den Spalten“: Als Abbildung $\mathbb{R}^n \times \cdots \times \mathbb{R}^n \to \mathbb{R}$ in den n Spaltenvektoren $\varphi(e_1), \ldots, \varphi(e_n)$ der darstellenden Matrix ist sie in jedem Argument linear.

„Alternierend“: Die Vertauschung von zwei Spalten der darstellenden Matrix ändert das Vorzeichen.

„Normiert“: Die Volumenänderung der Identitätsabbildung ist 1.

Auch für den n-dimensionalen Raum sind dies vernünftige Anforderungen an ein n-dimensionales Volumen.

Definition 6.3 *Man kann nun zeigen, dass es für jedes n genau eine Abbildung* Determinante

$$\det : \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_{n \text{ mal}} \to \mathbb{R}$$

mit den genannten Eigenschaften gibt, die Determinante.

[16] Eine allgemeine Metrik braucht allerdings nicht die Homogenitätsanforderung zu erfüllen.

Für die Determinante einer $(n \times n)$-Matrix schreibt man im Fall $n > 1$ auch senkrechte Striche:

$$\det \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Berechnung der Determinante:

(1) Die Determinante einer (oberen oder unteren) Dreiecksmatrix ist das Produkt der Diagonaleinträge:

$$\begin{vmatrix} d_{11} & \dots & d_{1n} \\ 0 & \ddots & \vdots \\ 0 & 0 & d_{nn} \end{vmatrix} = \begin{vmatrix} d_{11} & 0 & 0 \\ \vdots & \ddots & 0 \\ d_{n1} & \dots & d_{nn} \end{vmatrix} = d_{11} \cdot \dots \cdot d_{nn}$$

(Jeder der Vektoren e_i wird um den volumenändernden Faktor d_{ii} gestreckt und in eine Richtung in $\langle e_1, \dots, e_{i-1} \rangle$ bzw. $\langle e_{i+1}, \dots, e_n \rangle$ geschert. Scherungen ändern das Volumen aber nicht.)

(2) Eine beliebige Matrix A bringt man mit dem Gauß-Verfahren in Zeilenstufenform (die eine obere Dreiecksmatrix ist). (*) Zeilenvertauschungen ändern das Vorzeichen der Determinante; (**) Additionen des Vielfachen einer Zeile zu einer anderen ändern die Determinante nicht. Daher gilt:

$$\det(A) = (-1)^{\text{Anzahl der Zeilemvertauschungen}} \cdot \det(D)$$

Man kann das Gauß-Verfahren mit Spalten- statt mit Zeilenoperationen durchführen. Dann ergibt sich (*) aus der Eigenschaft der Determinante, alternierend zu sein, und (**) aus der Linearität in den Spalten. Man kann aber beweisen, dass $\det(A) = \det(A^{\mathrm{T}})$ ist und daher die Determinante auch alternierend und multilinear in den Zeilen ist. Daher kann man das normale Gauß-Verfahren benutzen.

Satz 6.4 (Eigenschaften der Determinante) *Seien A, B $(n \times n)$.Matrizen über $\mathbb{R}$.*

- $\det(A) \neq 0 \iff$ *A ist invertierbar. Dann gilt* $\det(A^{-1}) = \frac{1}{\det(A)}$.
- $\det(\mathrm{id}) = \det(I_n) = 1$
- „Multiplikationssatz“: $\det(A \cdot B) = \det(A) \cdot \det(B)$
- $\det(A) = \det(A^{\mathrm{T}})$. *Die Determinante ist daher auch alternierend und multilinear als Abbildung der Zeilenvektoren.*
- Berechnungsformeln:
  - $\det(a_{11}) = a_{11}$
  - $\left|\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right| = a_{11} \cdot a_{22} - a_{21} \cdot a_{12}$
  - $\left|\begin{smallmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{smallmatrix}\right| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$
  - „Formel von Leibniz“ [17]:

$$\det(A) = \sum_{\sigma \in \mathrm{Sym}(\{1,\dots,n\})} \mathrm{sgn}(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

[17] Gottfried Wilhelm Leibniz (1646–1716). In der Formel ist $\mathrm{Sym}(\{1, \dots, n\})$ die symmetrische Gruppe (siehe Seite 12) und sgn das Signum (siehe Seiten 70 und 83).

- „Laplace'scher Entwicklungssatz[18]“: *Sei A_{ij} die $((n-1)\times(n-1))$-Matrix, die aus A durch Streichen der i-ten Zeile und j-ten Spalte entsteht. Dann gilt:*

$$\begin{aligned}\det(A) &= \sum_{j=1}^{n}(-1)^{i+j}a_{ij}det(A_{ij}) \quad \text{[Entwicklung nach } i\text{-ter Zeile } (i \text{ ist fest})]\\ &= \sum_{i=1}^{n}(-1)^{i+j}a_{ij}det(A_{ij}) \quad \text{[Entwicklung nach } j\text{-ter Spalte } (j \text{ ist fest})]\end{aligned}$$

Die Leibniz-Formel ist für große n für praktische Berechnungen nicht tauglich, da die Summe über $n!$ Summanden läuft. Die angegeben Spezialfälle für $n = 1, 2, 3$ sind dagegen nutzbar.
Der Laplace'sche Entwicklungssatz führt ebenfalls zu langen Berechnungen und taugt nur, falls in einer Zeile oder Spalte viele Nullen stehen. Man kann mit Hilfe von Determinanten auch eine explizite Formel für die Inverse einer invertierbaren Matrix angeben (die aber für praktische Berechnungen ebenfalls nicht nützlich ist).

$$A^{-1} = \frac{1}{\det(A)} \cdot \tilde{A}^{\mathrm{T}}$$

wobei die Einträge von $\tilde{A}$ der Form $\tilde{a}_{ij} = (-1)^{i+j}\det(A_{ij})$ sind. Die Matrix $\tilde{A}^{\mathrm{T}}$ heißt auch *Adjunkte* $\mathrm{adj}(A)$ von A.

6.3 Skalarprodukt

Definition 6.5 *Das (Standard-)Skalarprodukt im Vektorraum $\mathbb{R}^n$ ist die folgende Abbildung $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $(v, w) \mapsto \langle v, w\rangle$[19] mit*

Standard-skalarprodukt

$$\langle v, w\rangle := (v_1, \ldots, v_n) \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_2 \end{pmatrix} = v_1w_1 + v_2w_2 + \cdots + v_nw_n$$

Satz 6.6 (Eigenschaften des Skalarprodukts) *Für alle $v, v', w, w' \in \mathbb{R}^n$ und $r \in \mathbb{R}$ gilt:*

Positivität:	$\langle v, v\rangle = \|v\|^2 \geqslant 0$	*und*	$\langle v, v\rangle = 0 \iff v = 0$
Symmetrie:	$\langle v, w\rangle = \langle w, v\rangle$		
Bilinearität:	$\langle v + v', w\rangle = \langle v, w\rangle + \langle v', w\rangle$		$\langle v, w + w'\rangle = \langle v, w\rangle + \langle v, w'\rangle$
	$\langle r \cdot v, w\rangle = r \cdot \langle v, w\rangle$		$\langle v, r \cdot w\rangle = r \cdot \langle v, w\rangle$

d. h. das Skalarprodukt ist sowohl im ersten als auch im zweiten Argument eine lineare Abbildung.

Beweis: Einfaches Nachrechnen! □

Satz 6.7 (Cauchy-Schwarz[20]) *Seien $v, w \in \mathbb{R}^n$, dann gilt*

$$|\langle v, w\rangle| \quad \leqslant \quad \|v\| \cdot \|w\|$$

[18] Pierre-Simon Laplace (1749–1827)
[19] In diesem Kontext soll nun $\langle v, w\rangle$ immer das Skalarprodukt bezeichnen und nicht etwa der von v und w erzeugten Untervektorraum!

bzw. (quadriert)

$$\left(\sum_{i=1} v_i w_i\right)^2 \leqslant \sum_{i=1} v_1^2 \cdot \sum_{i=1} w_1^2$$

bzw. für $v \neq 0$ und $w \neq 0$:

$$-1 \leqslant \frac{\langle v, w\rangle}{\|v\| \cdot \|w\|} = \left\langle \frac{v}{\|v\|}, \frac{w}{\|w\|} \right\rangle \leqslant 1$$

Beweis: Der Fall $w = 0$ ist klar (beide Seiten ergeben 0); sei also $w \neq 0$. Dann ist

$$\begin{aligned} 0 &\leqslant \left\langle v - \frac{\langle v, w\rangle}{\|w\|^2} \cdot w, v - \frac{\langle v, w\rangle}{\|w\|^2} \cdot w \right\rangle \\ &= \langle v, v\rangle - 2 \cdot \frac{\langle v, w\rangle}{\|w\|^2} \langle v, w\rangle + \frac{\langle v, w\rangle^2}{\|w\|^4} \langle w, w\rangle \\ &= \frac{1}{\|w\|^2}\Big(\langle v, v\rangle \cdot \langle w, w\rangle - 2 \cdot \langle v, w\rangle^2 + \langle v, w\rangle^2\Big) = \frac{1}{\|w\|^2}\Big(\langle v, v\rangle \cdot \langle w, w\rangle - \langle v, w\rangle^2\Big) \end{aligned}$$

Daraus folgt also $0 \leqslant \langle v, v\rangle \cdot \langle w, w\rangle - \langle v, w\rangle^2$ bzw. $\langle v, w\rangle^2 \leqslant \langle v, v\rangle \cdot \langle w, w\rangle = \|v\|^2 \cdot \|w\|^2$, also nach Wurzelziehen das gewünschte Ergebnis. □

Definition 6.8 *Da $\cos : [0, \pi] \to [-1, 1]$ bijektiv ist, existiert für $v \neq 0$ und $w \neq 0$ existiert ein eindeutiges $\alpha \in [0, \pi]$ mit $\langle v, w\rangle = ||v|| \cdot ||w|| \cdot \cos(\alpha)$. Man nennt α den zwischen v und w eingeschlossenen Winkel $\measuredangle(v, w)$.*

Winkel, senkrecht, orthogonal

Es gilt dann $\langle v, w\rangle = 0 \iff \cos(\measuredangle(v, w)) = 0 \iff \measuredangle(v, w) = \frac{\pi}{2}$. In diesem Fall sagt man, dass v und w senkrecht aueinander stehen oder orthogonal zueinander sind.

Der Winkel ist nicht orientiert, d. h. $\measuredangle(v, w) = \measuredangle(w, v)$. In $\mathbb{R}^2$ könnte man einen Winkel $\neq \pi$ auch mit einem Vorzeichen versehen (abhängig davon, ob der Winkel von v nach w im oder entgegen dem Uhrzeigersinn läuft). In höher-dimensionalen Räumen ist dies aber nicht sinnvoll möglich.

In den Dimensionen 2 und 3 stimmt diese Winkeldefinition mit dem anschaulichen geometrischen Begriff überein; in den höheren Dimensionen ist es eine sinnvolle Verallgemeinerung. In abstrakten n-dimensionalen Räumen gibt es dagegen kein Standard-Skalarprodukt, also auch keinen natürlichen Winkelbegriff. Durch die Wahl einer Basis kann man aber das Skalarprodukt des $\mathbb{R}^n$ übertragen. Das Standard-Skalarprodukt geht axiomatisch davon aus, dass die Standardbasis eine sogenannte *Orthonormalbasis* ist, also die Basisvektoren Länge 1 haben und paarweise aufeinander senkrecht stehen. Darauf beruhen alle weiteren Längen- und Winkelbestimmungen. Die Übertragung des Standard-Skalarprodukts des $\mathbb{R}^n$ auf einen abstrakten n-dimensionalen Vektorraum durch Wahl einer Basis bedeutet, dass man diese Basis zur Orthonormalbasis erklärt.

Satz 6.9 *Sei $v \neq 0$, dann ist die orthogonale Projektion w_v von w auf v gegeben durch*

$$w_v = \frac{\langle w, v\rangle}{\langle v, v\rangle} \cdot v = \underbrace{\frac{\langle w, v\rangle}{\|v\|}}_{\text{Länge}} \cdot \underbrace{\frac{v}{\|v\|}}_{\text{Richtung}}$$

[20] Augustin Louis Cauchy (1789–1857), Hermann Amandus Schwarz (1843–1921)

BEWEIS: Orthogonale Projektion bedeutet, dass $w - w_v$ senkrecht auf v steht. Es reicht also zu zeigen, dass mit dieser Formel $\langle v, w - w_v\rangle = 0$ gilt:

$$\langle v, w - \frac{\langle w,v\rangle}{\langle v,v\rangle}\cdot v\rangle = \langle v,w\rangle - \langle v, \frac{\langle w,v\rangle}{\langle v,v\rangle}\cdot v\rangle = \langle v,w\rangle - \frac{\langle w,v\rangle}{\langle v,v\rangle}\cdot\langle v,v\rangle = \langle v,w\rangle - \langle w,v\rangle = 0$$

□

Definition 6.10 *Eine Basis $\{v_1,\ldots,v_n\}$ von $\mathbb{R}^n$ heißt Orthogonalbasis, falls die Vektoren paarweise aufeinander senkrecht stehen, also $\langle v_i, v_j\rangle = 0$ für alle $i \neq j$ gilt, und Orthonormalbasis (ONB), falls die Vektoren zusätzlich Länge 1 haben, also $\langle v_i, v_i\rangle = 1$ für alle i gilt.*

Orthonormalbasis

Satz 6.11 *Wenn $\{v_1,\ldots,v_n\}$ eine Orthonormalbasis ist, dann gilt*

$$w = \sum_{i=1}^{n} \langle w, v_i\rangle \cdot v_i$$

BEWEIS: Wenn man $w = \sum_{i=1}^n r_i v_i$ ansetzt, kann man ausrechnen:

$$\begin{aligned}\langle w, v_i\rangle &= \langle r_1 v_1 + \cdots + r_n v_n, v_i\rangle \\ &= r_1\cdot\langle v_1,v_i\rangle + \cdots + r_n\cdot\langle v_n,v_i\rangle \\ &= r_1\cdot 0 + \ldots r_{i-1}\cdot 0 + r_i\cdot\langle v_i,v_i\rangle + r_{i+1}\cdot 0 + \cdots + r_n\cdot 0 = r_i\end{aligned}$$

□

Satz 6.12 (Verallgemeinerter Satz des Pythagoras[21]; Cosinussatz) *Für $v, w \in \mathbb{R}^n$ gilt:*

$$\|v+w\|^2 = \|v\|^2 + 2\cdot\langle v,w\rangle + \|w\|^2.$$

Insbesondere gilt $\|v+w\|^2 = \|v\|^2 + \|w\|^2$ genau dann, wenn $\langle v,w\rangle = 0$, also wenn v und w senkrecht aufeinander stehen.

BEWEIS: Einfach ausrechnen unter Benutzung der Bilinearität:

$$\|v+w\|^2 = \langle v+w, v+w\rangle = \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle + \langle w,w\rangle = \|v\|^2 + 2\cdot\langle v,w\rangle + \|w\|^2$$

□

6.4 Orthogonale Abbildungen

Definition 6.13 *Eine lineare Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ heißt orthogonal, wenn φ das Skalarprodukt erhält, wenn also $\langle\varphi(v),\varphi(w)\rangle = \langle v,w\rangle$ für alle $v,w\in\mathbb{R}^n$ gilt.*[22]

Eine $(n\times n)$-Matrix A heißt orthogonal, wenn die zugehörige lineare Abbildung orthogonal ist.

orthogonale lineare Abb. / Matrix

Lemma 6.14 *Für alle $v,w\in\mathbb{R}^n$ gilt: $\langle Av, w\rangle = \langle v, A^{\mathrm{T}}w\rangle$ bzw. $\langle v, Aw\rangle = \langle A^{\mathrm{T}}v, w\rangle$.*

[21] Pythagoras (ca. 570–510 v. Chr.)

[22] Achtung: Die orthogonale Projektion aus Satz 6.9 ist keine orthogonale Abbildung.

BEWEIS: Entweder nachrechnen, oder (alle Vektoren als Spaltenvektoren aufgefasst):

$$\langle Av, w\rangle = w^{\mathrm{T}} \cdot A \cdot v = (w^{\mathrm{T}} \cdot A \cdot v)^{\mathrm{TT}} = (v^{\mathrm{T}} \cdot A^{\mathrm{T}} \cdot w)^{\mathrm{T}} = \langle v, A^{\mathrm{T}} w\rangle^{\mathrm{T}} = \langle v, A^{\mathrm{T}} w\rangle$$

Die letzte Gleichung gilt, weil nur ein Skalar, also eine (1×1)-Matrix, transponiert wird. □

Satz 6.15 *Die folgenden Aussagen sind äquivalent für eine $(n \times n)$-Matrix über $\mathbb{R}^n$:*
(a) *A ist orthogonal;*
(b) *A ist invertierbar und $A^{-1} = A^{\mathrm{T}}$;*
(c) *$Ae_1, \ldots, Ae_n$ ist eine Orthonormalbasis.*

BEWEIS: (a)⇒(c): Es ist $\langle Ae_i, Ae_j\rangle = \langle e_i, e_j\rangle = \begin{cases} 1 & \text{für } i{=}j \\ 0 & \text{für } i{\neq}j \end{cases}$

(c)⇒(b): Der (i, j)-Eintrag von $A^{\mathrm{T}} \cdot A$ ist gerade $\langle Ae_i, Ae_j\rangle$, also 1 für die Diagonalelemente $i = j$ und 0 sonst. Das bedeutet aber gerade, dass $A^{\mathrm{T}} \cdot A = \mathrm{Id}$.

(b)⇒(a): $\langle Av, Aw\rangle = \langle v, A^{\mathrm{T}} Aw\rangle = \langle v, A^{-1} Aw\rangle = \langle v, w\rangle$. □

Orthogonale Abbildungen sind längentreu, d. h. $\|Av\| = \|v\|$ für alle v, und winkeltreu, d. h. $\measuredangle(Av, Aw) = \measuredangle(v, w)$ für alle v, w. Aus $A^{-1} = A^{\mathrm{T}}$ folgt $\det(A)^{-1} = \det(A^{\mathrm{T}}) = \det(A)$ und somit $\det A = \pm 1$. Orthogonale Abbildungen sind also zudem volumentreu bis auf die Orientierung, die sich ändern kann, wie es bei Spiegelungen der Fall ist.

Drehungen im $\mathbb{R}^2$ sind orthogonal (mit Determinante 1). Wegen $\sin^2(\alpha) + \cos^2(\alpha) = 1$ kann man für die Drehmatrix leicht nachrechnen, dass

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^{-1} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

gilt bzw. dass die Spalten eine ONB bilden.

Ebenso sind Spiegelungen orthogonal (mit Determinante -1).

Drehungen und Spiegelungen sind die einzigen orthogonalen Abbildungen der Ebene.

Scherungen sind Beispiele von volumenerhaltenden Abbildungen, die weder längen- noch winkeltreu sind. Streckungen (aller Vektoren um den gleichen Faktor) sind Beispiele von winkeltreuen Abbildungen, die weder längen- noch volumentreu sind. Man kann aber zeigen, dass längentreue Abbildungen bereits orthogonal sind, und ebenso Abbildungen, die winkel- und volumentreu sind.

(Ersteres folgt unmittelbar aus dem verallgemeinerten Satz von Pythagoras: Wenn alle Längen erhalten bleiben, muss auch $\langle v, w\rangle$ erhalten bleiben. Für die zweite Aussage muss man ein bisschen mehr überlegen.)

7 Codierungstheorie

In der Codierungstheorie geht es um folgende Problematik: Informationen werden als Folgen von Symbolen aufgeschrieben und festgehalten. (Man sagt dazu auch, dass eine Information durch die sie wiedergebende Folge der Symbole „codiert“ wird.) Zum Beispiel kann dies durch Morse-Zeichen, durch Zahlenfolgen im ASCII-Code oder, wie in diesem Text hier, durch Symbolfolgen des um Satzzeichen angereicherten lateinischen Alphabets geschehen. Bei der Übermittlung – z. B. der Übertragung durch Funk oder Kabel oder der Speicherung der Information über längere Zeiträume hinweg – können Fehler passieren oder Teile der Information verloren gehen. Durch eine in die Codierung eingebaute Redundanz können ggf. Übertragungsfehler erkannt und korrigiert werden. Die einfachste Art solch einer Redundanz besteht darin, die Nachricht mehrfach zu wiederholen. Stimmen die empfangenen Informationen nicht überein, so weiß man, dass Übertragungsfehler eingetreten sein. Indem man gegebenenfalls die am häufigsten empfangene Version als die richtige ansieht, kann man u. U. auch Übertragungsfehler ausgleichen. Codierung, Decodierung und Fehlkerkorrektur sind in diesem Fall zwar einfach; das Verfahren ist aber insofern ineffizient, als sich die Länge der übermittelten Nachricht (und damit Zeit und Kosten) vervielfacht. Die Frage ist nun, ob es bessere Verfahren gibt.

Eine kleine sprachliche Schwierigkeit entsteht dadurch, dass es in der Regel mehrere Codierungsschritte gibt: Eine Information wird zunächst zum Beispiel als Text der deutschen Sprache gefasst (was man bereits als eine erste Codierung ansehen könnte), der dann als Buchstabenfolge codiert wird. Jeder dieser Buchstaben kann dann wiederum als ASCII-Zeichen durch eine $\{0,1\}$-Folge codiert werden. Jeder dieser Folgen wird dann schließlich (in der ursprünlgichen ASCII-Version) ein „Prüfbit“ angehängt, das für eine gewisse Informationsredundanz sorgt. Hier geht es ausschließlich um diesen letzten Codierungsschritt!

Zunächst brauchen wir die in der Codierungstheorie übliche Terminologie.

Hamming-Raum

Definition 7.1 *Sei A ein endliches Alphabet (d. h. eine Symbolmenge) mit $q > 0$ Elementen Man betrachtet Wörter einer festen Länge n über A, d. h. Elemente $(a_1, \ldots, a_n)$ von A^n, um Nachrichten zu codieren. Die Menge A^n dieser n-Tupel wird der Hamming-Raum[23] $H(n, A)$ genannt, bzw. $H(n, q)$, wenn es nur auf die Anzahl der Elemente von A ankommt.*

Oft nimmt man als Alphabet eine endliche Gruppe oder einen endlichen Körper, da die algebraische Struktur hilft, gute Codierungen und Algorithmen zu finden. Für jedes $q > 0$ gibt es die Gruppe $(\mathbb{Z}_q, +)$ mit q Elementen; falls $q = p^n$ eine Prinzahlpotenz ist, gibt es auch den endlichen Körper $\mathbb{F}_q$ mit q Elementen. $H(n, q)$ ist dann ein $\mathbb{F}_q$-Vektorraum der Dimension n. Besonders häufig ist der Fall $q = 2$ mit $\mathbb{F}_2 = \{0, 1\}$. Der Hamming-Raum $H(8, \mathbb{F}_2)$ ist zum Beispiel die Menge der Bytes. Den Hamming-Raum $H(4, \mathbb{F}_2)$ kann man mit den hexadezimalen Ziffern identifizieren.

- Im ASCII-Code wurden Zeichenzunächst durch ein Byte $(a_1, \ldots, a_8)$, also ein 8-Tupel über $\mathbb{F}_2$, codiert. Dabei bildeten die ersten sieben Ziffern $a_1, \ldots, a_7$ die eigentliche Information: als Binärzahl gelesen geben sie die Stelle des codierten Zeichens (Buchstabe, Ziffer, Satz- oder Steuerungszeichen) in der Liste der ASCII-Zeichen an. Die letzte Ziffer a_8 war eine Kontrollziffer, welche den sogenannten *parity check* durchführt: a_8 war so gewählt, dass $a_1 + \cdots + a_8 = 0$ in $\mathbb{F}_2$ gilt. Der Code „erkennt“, wenn an einer Stelle ein Übertragungsfehler

[23] Richard Hamming (1915-1998)

passiert, da dann die Prüfrechnung nicht mehr stimmt. Geht bei der Übertragung eine Stelle verloren, kann man sie errechnen.

- Im alten ISBN-Code war die eigentliche Information einen neunstelligen Dezimalzahl. Um in einem Körper arbeiten zu können, hat man die Ziffern $0, \dots, 9$ als Elemente von $\mathbb{F}_{11}$ aufgefasst. Das 9-Tupel $(b_1, \dots, b_9)$ wurde nun so um eine Prüfziffer $b_{10} \in \mathbb{F}_{11}$ ergänzt, dass $\sum_{i=1}^{10} i \cdot b_i = 0$ in $\mathbb{F}_{11}$ gilt. (Das Element 10 in $\mathbb{F}_{11}$ wurde dann X geschrieben.)

  Dieser Code erkennt eine falsche Ziffer und auch Vertauschungen von zwei Ziffern, d. h. die Prüfrechnung stimmt dann nicht mehr.

- Der aktuelle ISBN-Code ist ein 13-Tupel über $\mathbb{Z}/10\mathbb{Z}$, wobei wieder die letzte Ziffer eine Prüfziffer ist, die so gewählt wird, dass $b_1 + 3b_2 + b_3 + 3b_4 + \dots + b_{13} = 0$ in $\mathbb{Z}/10\mathbb{Z}$ gilt. Dieser Code erkennt ebenfalls eine falsche Ziffer, aber nur noch gewisse Vertauschungen.

- Bei der neuen internationale Bankkontonummer IBAN folgen nach der anfänglichen Länderkennung (zwei Buchstaben) zwei Prüfziffern, die so gewählt sind, dass für eine gewisse, aus der IBAN gebildete Zahl z die Zahl $z - 1$ durch 97 teilbar ist. z entsteht aus der IBAN, indem man zunächst den Ländercode mit den Prüfziffern ans Ende setzt und dann die Buchstaben des Ländercodes durch zweistellige Zahlen ersetzt (A = 10, B = 11, ...).

7.1 Fehler und die Hamming-Metrik

Anschaulich gesprochen ist ein Code gut, wenn er besonders viele Fehler erkennt oder sogar deren Korrektur zulässt. Um dies zu präzisieren, muss man festlegen, was Fehler sind und wie man ihre Anzahl misst. Im üblichen Setting legt man dazu fest, dass es nur um die Anzahl der Stellen geht, die nicht übereinstimmen.

Definition 7.2 *Für $v = (v_1, \dots, v_n)$ und $w = (w_1, \dots, w_n)$ in $H(n, A)$ definiert man den Hamming-Abstand (oder die Hamming-Metrik) als*

Hamming-Metrik

$$\mathrm{d}(v, w) := \left| \{ i \mid v_i \neq w_i \} \right|$$

In $H(8, \{a, b, c, \dots, z\}$ gilt:

$$\mathrm{d}(freiburg, reisberg) = 5$$

Misst man die Anzahl von Fehlern durch die Hamming-Metrik, sollte man sich folgende Unterschiede zu möglichen Alltagsbegriffen klar machen (mit Beispielen in $H(5, \{0, 1, \dots, 9\})$):

- Eine Vertauschung von zwei Ziffern zählt als zwei Fehler: $\mathrm{d}(12345, 12435) = 2$.
- Alle Stellen als gleichwertig gezählt: $\mathrm{d}(11011, 11016) = \mathrm{d}(11011, 61011) = 1$.
  Bei Dezimalzahlen würde man dagegen Fehler in den höheren Stellen als gewichtiger ansehen!
- Alle Elemente des Alphabets werden untereinander als gleichwertig gezählt:
  $\mathrm{d}(00000, 10000) = \mathrm{d}(00000, 90000) = 1$.

Satz 7.3 $\mathrm{d}(\ ,\ )$ *ist eine Metrik auf* $H(n,A)$*, d. h. für alle* $u,v,w \in H(n,A)$ *gilt:*

- Positivität: $\mathrm{d}(v,w) \geqslant 0$ *und* $\mathrm{d}(v,w) = 0 \iff v = w$
- Symmetrie: $\mathrm{d}(v,w) = \mathrm{d}(w,v)$
- Dreiecksungleichung: $\mathrm{d}(u,w) \leqslant \mathrm{d}(u,v) + \mathrm{d}(v,w)$

Falls $(A,+)$ *eine Gruppe ist, ist* $H(n,q)$ *eine Gruppe unter der komponentenweisen Addition und es gilt:*

- Translationsinvarianz: $\mathrm{d}(v,w) = \mathrm{d}(v+u, w+u)$,
  insbesondere $\mathrm{d}(v,w) = \mathrm{d}(v-w,0) = \mathrm{d}(-w,-v) = \mathrm{d}(-v,-w)$

Falls $A = K$ *ein Körper ist, ist* $H(n,A)$ *ein* K*-Vektorraum und es gilt:*

- Invarianz unter Skalarmultiplikation: $\mathrm{d}(v,w) = \mathrm{d}(kv,kw)$ *für alle* $k \in K \setminus \{0\}$

Beweis: Die ersten beiden Eigenschaften folgen unmittelbar aus der Definition. Die Dreiecksungleichung sieht man aus der Transitivität der Gleichheit: Wenn $u_i \neq w_i$, dann gilt $u_i \neq v_i$ oder $v_i \neq w_i$. Offensichtlich gilt $\mathrm{d}(v,w) \geqslant \mathrm{d}(f(v),f(w))$ für eine beliebige komponentenweise definierte Abbildung $f : H(n,A) \to H(n,A)$. Daraus folgt für bijektive solche f:

$$\mathrm{d}(v,w) \geqslant \mathrm{d}(f(v),f(w)) \geqslant \mathrm{d}(f^{-1}(f(v)), f^{-1}(f(w))) = \mathrm{d}(v,w)$$

Dies impliziert die Invarianz unter Translationen und unter Skalarmultiplikation, da die Abbildungen $v \mapsto v+u$ und $v \mapsto k \cdot v$ für $k \neq 0$ bijektiv sind (Umkehrabbildungen sind $v \mapsto v-u$ und $v \mapsto k^{-1} \cdot v$). □

Während die übliche euklidische Metrik $\|v-w\|$ im $\mathbb{R}^n$ ebenfalls translationsinvariant ist, gilt dort $\|rv - rw\| = |r| \cdot \|v-w\|$. Die Invarianz der Hamming-Metrik unter Skalarmultiplikation ist also eine „ungeometrische“ Eigenschaft.

Codes und ihre Eigenschaften

Definition 7.4 **(a)** *Ein q-ärer Code der Länge n (über A) ist eine nicht-leere Teilmenge von* $H(n,A)$ *bzw.* $H(n,q)$*. Der Minimalabstand des Codes ist* $\min\{\mathrm{d}(v,w) \mid v,w \in C, v \neq w\}$.[24]

Ein Code C *erkennt e Fehler, falls der Minimalabstand größer als e ist, und korrigiert e Fehler, falls es zu jedem* $v \in H(n,A)$ *höchstens ein* $c \in C$ *gibt mit* $\mathrm{d}(v,c) \leqslant e$*.*

(b) *Ein linearer q-ärer* $[n,k,d]$*-Code (oder auch* $[n,k]$*-Code) ist ein Untervektorraum von* $H(n,q) = \mathbb{F}_q^n$ *der Dimension k vom Minimalabstand d.*

Das Gewicht von $v \in C$ *ist* $\mathrm{d}(v,0)$*, das Minimalgewicht von* C *ist* $\min\{\mathrm{d}(v,0) \mid v \in C, v \neq 0\}$.

Für einen $[n,k]$-Code C gilt $|C| = q^k$ bzw. $k = \log_q |C|$. Manche Autoren bevorzugen, statt der Dimension eines Codes C an zweiter Stelle die Anzahl der Elemente von C anzugeben.

Wegen $\mathrm{d}(v,w) = \mathrm{d}(v-w,0)$ ist das Minimalgewicht eines linearen Codes gleich seinem Minimalabstand. Typischerweise nennt man im Zusammenhang mit linearen Codes den Parameter d eher das Minimalgewicht.

Die Terminologie ist leider etwas missverständlich. Wenn ein Code e Fehler erkennt, bedeutet dies nur Folgendes: Wenn ein Codewort „gesendet“ wurde und bei der Übertragung höchstens e Fehler (im Sinne des Hamming-Abstands) passiert sind, kann man anhand des empfangenen

[24] Für den Fall $|C| = 1$ kann man den Minimalanbstand als ∞ setzen.

Wortes erkennen, dass die Übertragung fehlerhaft war. Man kann aber weder erkennen, weiviele Fehler passiert sind, noch das ursprüngliche Wort rekonstruieren.

Wenn ein Code e Fehler korrigiert, bedeutet es Folgendes: Wenn ein Codewort „gesendet“ wurde, kann man ursprüngliche Wort rekonstruieren, falls höchstens e Fehler passiert sind. Sind in Wirklichkeit mehr Fehler passiert, kann die Rekonstruktion falsch sein.

Erkennung und Korrektur von e Fehlern ist immer im Sinne von „mindestens e“ gemeint. Ein Code, der 5 Fehler erkennt, erkennt also auch 4 Fehler, und es ist nicht ausgeschlossen, dass er auch 6 Fehler erkennt. Falls einCode e Fehler erkennt oder korrigiert und nicht mehr, sagt man auch, dass er *genau* e Fehler erkennt bzw. korrigiert.

Unmittelbar aus der Definition sieht man:

Satz 7.5

(a) *Ein Code mit Minimalabstand d erkennt $d-1$ Fehler und korrigiert $\lfloor \frac{d-1}{2} \rfloor$ Fehler.*

(b) *Ein Code, der e Fehler korrigiert, erkennt $2e$ Fehler und hat Minimalabstand $\geqslant 2e+1$.*

- Der alte ISBN-Code ist ein 11-ärer Code der Länge 10, der genau einen Fehler erkennt und keinen korrigiert.
- Der ASCII-Code ist ein binärer linearer $[8,7,2]$-Code, der also genau einen Fehler erkennt und keinen korrigiert.
- Der Wiederholungscode $\{(x,x,x) \mid x \in \mathbb{F}_q\} \subseteq H(3,q)$ ist ein q-ärer linearer $[3,1,3]$-Code, der also genau zwei Fehler erkennt und genau einen korrigiert.

Definition 7.6 *Der Ball vom Radius e um v ist*[25] Ball

$$B_e(v) := \big\{ w \in H(n,A) \;\big|\; \mathrm{d}(v,w) \leqslant e \big\}.$$

Es gilt offensichtlich:

- C erkennt genau dann e Fehler, wenn $c' \notin B_e(c)$ für alle $c, c' \in C$, $c \neq c'$.
- C korrigiert genau dann e Fehler, wenn die Bälle $B_e(c)$ für $c \in C$ paarweise disjunkt sind.

Satz 7.7 *Die Anzahl der Elemente eines Balls ist (unabhängig von v) gegeben durch*

$$\big|B_e(v)\big| = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$

Für $q = 2$ gilt insbesondere

$$\big|B_e(c)\big| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{e}$$

Beweis: i durchläuft die möglichen Abstände zu v; der Binomialkoeffizient gibt die Anzahl der Möglichkeiten für die i Stellen, an denen die Abweichungen auftreten; $q-1$ ist für jede Stelle die Anzahl der alternativen Elemente des Alphabets. □

[25] In der Analysis sind Bälle üblicherweise als offene Bälle definiert, d. h. man fordert „$< e$“ statt „$\leqslant e$“. Dies ist in der diskreten Situation hier nicht besonders sinnvoll.

Bemerkung 7.8 In einer kommutativen Gruppe $(A, +)$ definiert man für $a \in A$ und $m \in \mathbb{N}$:

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

Falls p eine Primzahl ist und A ein $\mathbb{F}_p$-Vektorraum, gilt $p \cdot a = 0$. Umgekehrt ist $(A, +)$ mit der oben definierten Multiplikation für $m = 0, \ldots, p-1$ schon ein $\mathbb{F}_p$-Vektorraum, wenn $p \cdot a = 0$ für alle a gilt. (Im Fall $p = 2$ muss also $a + a = 0$ für alle a gelten).

Insbesondere folgt daraus, dass jede unter Addition abgeschlossene Teilmengen $C \subseteq \mathbb{F}_p^n$ bereits ein Untervektorraum ist.

(Beweis siehe Teil II der Vorlesung).

Wörter der Länge 4 über $\mathbb{F}_2$ (also etwa die Binärdarstellung von hexadezimalen Zahlen) sollen durch einen Code mit Minimalabstand 3 codiert werden, also so, dass zwei Fehler erkannt und ein Fehler korrigiert wird.

Erster Code: Die „naive“ Methode besteht darin, das Ausgangswort dreifach zu senden. Wörter aus $H(4, \mathbb{F}_2)$ werden also codiert als Wörter in $H(12, \mathbb{F}_2)$, nämlich $v = (v_1, v_2, v_3, v_4)$ als $v^\frown v^\frown v := (v_1, v_2, v_3, v_4, v_1, v_2, v_3, v_4, v_1, v_2, v_3, v_4)$.

$C_1 = \left\{ v^\frown v^\frown v \;\middle|\; v \in H(4, \mathbb{F}_2) \right\}$ ist ein binärer $[12, 4, 3]$-Code, d. h. der Code erkennt zwei Fehler und korrigiert einen.

Dieser Code ist aber nicht besonders effizient: Die Raumgröße ist $|H(12, \mathbb{F}_2)| = 2^{12} = 4.096$. Es gibt 16 Codewörter, die mit ihren „Korrekturbereichen“ einen Platz von $16 \cdot |B_1(c)| = 16 \cdot 13 = 208$ einnehmen. Der „verschwendete Platz“ besteht also aus $4.096 - 208 = 3.888$ Wörtern.

Zweiter Code: C_2 besteht aus folgenden Wörtern in $H(7, \mathbb{F}_2)$:

$(0,0,0,0,0,0,0)$	$(0,1,0,0,1,0,1)$	$(1,0,0,0,0,1,1)$	$(1,1,0,0,1,1,0)$
$(0,0,0,1,1,1,1)$	$(0,1,0,1,0,1,0)$	$(1,0,0,1,1,0,0)$	$(1,1,0,1,0,0,1)$
$(0,0,1,0,1,1,0)$	$(0,1,1,0,0,1,1)$	$(1,0,1,0,1,0,1)$	$(1,1,1,0,0,0,0)$
$(0,0,1,1,0,0,1)$	$(0,1,1,1,1,0,0)$	$(1,0,1,1,0,1,0)$	$(1,1,1,1,1,1,1)$

Ein Wort v aus $H(4, \mathbb{F}_2)$ wird codiert durch dasjenige Wort aus $H(7, \mathbb{F}_2)$ in der Liste, dessen Anfangsstück gerade v ist. Man kann nun überprüfen, dass C_2 ein binärer $[7, 4, 3]$-Code ist. Der Code erkennt also ebenfalls zwei Fehler und korrigiert einen, bei gleicher Anzahl von Codewörtern (d. h. bei gleicher Dimension 4).

Die Raumgröße ist hier $|H(7, \mathbb{F}_2)| = 2^7 = 128$. Die 16 Codewörter nehmen mit ihren „Korrekturbereichen“ einen Platz von $16 \cdot |B_1(c)| = 16 \cdot 8 = 128$ ein, d. h. es gibt keinen verschwendeten Platz. Solche Codes heißen *perfekte Codes*.

C_2 ist ein Beispiel für einen sogenannten *Hamming-Code*. Im nächsten Abschnitt wird erklärt, wie man C_2 systematisch konstruieren kann und wie Codierung und Decodierung funktionieren. Auch für C_2 gibt es dank linearer Algebra gute Codierungs- und Decodierungsalgorithmen.

Ein „guter“ Code sollte

- möglichst viele Fehler erkennen und korrigieren, d. h. großen Minimalabstand haben,
- möglichst viele Codewörter im Verhältnis zur Wortlänge n haben

- und dabei eine effiziente Codierung, Decodierung und ggf. Fehlerkorrektur gestatten.

Für Codierung und Decodierung gibt es immer die Möglichkeit, eine Codierungstafel aufzustellen. Für die Korrektur eines fehlerhaft übertragenen Worts muss dann in der Tafel nach dem Wort im Code gesucht werden, das den kleinsten Hamming-Abstand zum übertragenen Wort hat (wenn man davon ausgeht, dass höchstens so viele Fehler aufgetreten sind, wie der Code korrigieren kann). Bei einem großen Code ist dies aber ein eher umständlicher Algorithmus. Schnelle Algorithmen setzen voraus, dass der Code eine interne Struktur besitzt. Daher sind lineare Codes interessant.

Die ersten beiden Anforderungen laufen einander zuwider: Redundanzen (Prüfziffern) erhöhen die Wortlänge. Für einen gegebenen Hamming-Raum gibt es daher Schranken für das Verhältnis von Codegröße und Minimalabstand:

Satz 7.9 (Die Hamming-Schranke) *Die Anzahl der Codewörter eines q-ären Codes der Länge n mit Mindestabstand $\geqslant d$ ist höchstens*

$$\frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} \cdot (q-1)^i}$$

Beweis: Die Schranke folgt aus Satz 7.5 und Satz 7.7, da $q^n = |H(n,q)| \geqslant |C| \cdot |B_e(c)|$ für $e = \lfloor \frac{d-1}{2} \rfloor$. □

Definition 7.10 *Ein Code heißt perfekt, wenn er die Hamming-Schranke erreicht.*

perfekter Code

- $q = 2, n = 7, d = 3$: Hier ergibt die Hamming-Schranke $2^7/(1+7) = 16$. Der Hamming-Code C_2 im Beispiel oben erreicht als perfekter Code diese Schranke.
- $q = 2, n = 6$: Die Folge der Binomialkoeffizienten $\binom{6}{i}$ ist 1, 6, 15, 20, 15, 6, 1. Keine der Summen $\binom{6}{0}+\ldots\binom{6}{e}$ ist ein Teiler von $2^6 = 64$ außer für $e = 0$ und $e = 6$. Diese entsprechen den sogenannten trivialen Codes: Es gibt im ersten Fall überhaupt nur ein Codewort (bei Minimalabstand ∞); im zweiten sind alle Wörter Codewörter (bei Minimalabstand 1). Beide Codes sind perfekt, aber für die Belange der Codierungstheorie uninteressant. Für Wörter der Länge 6 gibt es also keine nicht-trivialen perfekten binären Codes.

triviale Codes

Satz 7.11 (Die Gilbert-Schranke[26]) *Gegeben q, n, d, so gibt es einen q-ären Code der Länge n und vom Minimalabstand mindestens d mit mindestens*

$$\frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} \cdot (q-1)^i}$$

Codewörtern. Ist q eine Primzahlpotenz, so kann man den Code linear über $\mathbb{F}_q$ wählen.

Beweis: Sei C ein Code vom Minimalabstand $\geqslant d$, so dass $|C|$ kleiner als die Gilbert-Schranke ist. Nach Annahme gilt $|C| \cdot |B_{d-1}(c)| < q^n = |H(n,q)|$, d. h. $\bigcup_{c \in C} B_{d-1}(c) \neq H(n,q)$. Also

[26] Edgar Gilbert (1923–2013)

gibt es ein $x \in H(n,q)$, welches zu allen $c \in C$ mindestens Abstand d hat. Dann ist $C \cup \{x\}$ ein größerer Code vom Minimalabstand $\geqslant d$. Durch sukzessives Vergrößern erhält man also einen Code, der die Gilbert-Schranke erfüllt.

Für den linearen Fall nimmt man an, dass $C \subseteq H(n,\mathbb{F}_q)$ bereits ein linearer Code ist (z. B. der triviale Code $\{0\}$) und wählt x wie oben. Statt $C \cup \{x\}$ betrachtet man nun den erzeugten linearen Code $\langle C \cup \{x\}\rangle$, muss aber noch zeigen, dass dieser weiterhin Mindestgewicht $\geqslant d$ hat.

Ein typisches Element darin hat die Form $kx + c$ mit $k \in \mathbb{F}_q$ und $c \in C$.
– Falls $k = 0$, so ist $\mathrm{d}(kx + c, 0) = \mathrm{d}(c, 0) \geqslant d$ nach Annahme an C.
– Falls $k \neq 0$, so ist $\mathrm{d}(kx + c, 0) = \mathrm{d}(kx, -c) = \mathrm{d}(x, -\frac{1}{k}c) \geqslant d$ nach Wahl von x, da $\frac{1}{k}c \in C$. □

Für $q = 2, n = 7, d = 3$ ergibt die Gilbert-Schranke $2^7/(1+7+21) \approx 4,41$. Die Gilbert-Schranke stellt also die Existenz eines Codes C vom Minimalabstand 3 mit mindestens 5 Codewörtern sicher. Im linearen Fall weiß man, dass die Anzahl der Element von C als Untervektorraum von $\mathbb{F}_2^7$ eine Zweierpotenz sein muss, also erhält man $|C| \geqslant 8$. Aus dem obigen Beispiel wissen wir aber, dass es sogar den Hamming-Code mit 16 Wörtern gibt.

7.2 Lineare Codes

Sei C nun ein q-ärer $[n,k]$-Code, also ein k-dimensionaler Unterraum von $H(n,q) = \mathbb{F}_q^n$.

Definition 7.12 *Eine Erzeugermatrix G für einen linearen $[n,k]$-Code C ist eine $(k \times n)$-Matrix, deren Zeilen eine Basis von C bilden.* Erzeugermatrix

Eine Erzeugermatrix eines Codes ist nicht eindeutig bestimmt. Man kann sie aber durch elementare Umformungen auf die Form

$$\left(\begin{array}{c|c} \mathrm{Id}_k & A \end{array}\right)$$

bringen, wobei A eine $(k \times (n-k))$-Matrix ist. Im Allgemeinen wird der Code durch solche Umformungen verändert und durch einen *äquivalenten* Code ersetzt (d. h. man betrachtet das Bild des Codes unter einem Automorphismus des Vektorraums $H(n,q)$). Äquivalente Codes haben zwar u. U. andere Codewörter, aber dieselben Parameter n, k, d.

Eine Erzeugermatrix in dieser spezielle Form entspricht, wie noch gezeigt wird, einer Codierung durch Anhängen von Prüfziffern an die eigentliche Information.

Der im vorherigen Abschnitt angegebene $[7,4,3]$-Hamming-Code hat mit

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

eine Erzeugermatrix in der Form $(\mathrm{Id}_k \mid A)$.

Man sieht hier leicht, dass die Basisvektoren ein Gewicht und paarweise einen Abstand von mindestens 3 haben. Dies ist natürlich eine notwendige Bedingung für einen Minimalabstand von mindestens 3, aber keine hinreichende.

Die Vektoren $(1,1,1,0,0,0)$, $(0,0,0,1,1,1)$ und $(1,1,0,1,1,0)$ haben Gewicht $\geqslant 3$ und paarweisen Abstand $\geqslant 3$, der von ihnen erzeugte Code hat aber nur Minimalgewicht 2: Die Summe der ersten beiden Vektoren ist $(1,1,1,1,1,1)$ und hat Abstand 2 zum dritten Vektor.

Man kann lediglich, wie im Beweis der Gilbert-Schranke, von einem Vektor v, der zu einem Untervektorraum U einen Minimalabstand hat, auf den Minimalabstand des von v und U erzeugten Untervektorraums schließen.

Codierung durch die Erzeugermatrix

Die Codierung eines (Zeilen-)Vektors $v \in H(k,q)$ erfolgt nun durch

$$v \cdot G = (G^{\mathrm{T}} \cdot v^{\mathrm{T}})^{\mathrm{T}} \in H(n,q).$$

Hat G die besondere Form $(\mathrm{Id}_k \mid A)$, so entsteht der Codevektor also durch das Anhängen der $n-k$ Prüfziffern $v \cdot A$, da $v \cdot G$ die Form $(v \cdot \mathrm{Id}_k)^\frown(v \cdot A) = v^\frown w$ für einen Vektor w der Länge $n-k$ hat. Die Prüfziffern erhält man als Linearkombination der Prüfziffern der Basiselemente.

Im angegebenen Beispiel des $[7,4,3]$-Hamming-Codes wird etwa der Vektor $v = (1,0,1,1)$ durch $(1,0,1,1) \cdot G = (1,0,1,1,0,1,0)$ codiert. Der Vektor schreibt sich als $e_1 + e_3 + e_4$, demgemäß ergeben sich die Prüfziffern für v als die analoge Linearkombination $(0,1,1) + (1,1,0) + (1,1,1)$ der Prüfziffern der Standardbasisvektoren.

Satz 7.13 *Die Codierungsabbildung $\mathbb{F}_q^k \to \mathbb{F}_q^n, v \mapsto v \cdot G$ ist injektiv.*

Beweis: Im Falle des Anhängens von Prüfziffern ist dies trivialerweise gegeben; da jeder Code zu einem solchen äquivalent ist, also durch Isomorphie dazu übergeht, gilt es auch allgemein.

Alternativer Beweis: Die Zeilen von G sind linear unabhängig, also gilt

$$\mathrm{rg}(G) = \mathrm{rg}(G^{\mathrm{T}}) = \dim \mathrm{Bild}(G^{\mathrm{T}}) = k$$

und somit $\dim \mathrm{Kern}(G^{\mathrm{T}}) = \dim \mathbb{F}_q^k - \dim \mathrm{Bild}(G^{\mathrm{T}}) = k - k = 0$. □

Definition 7.14 *Eine Prüfmatrix oder Kontrollmatrix H für einen $[n,k]$-Code C ist eine $((n-k) \times n)$-Matrix, für die $C = \mathrm{Kern}(H)$ gilt.* Prüfmatrix

Mit der Prüfmatrix kann man also die Kontrollrechnung für einen Code ausführen: Gilt $H \cdot v = 0$, so liegt v im Code, andernfalls nicht.

Satz 7.15 *Die folgenden Aussagen über einen linearen $[n,k]$-Code C und eine $((n-k) \times n)$-Matrix H sind äquivalent:*

(1) *H ist eine Prüfmatrix von C.*
(2) *Es gilt $H \cdot c^{\mathrm{T}} = 0$ für alle $c \in C$, und die Zeilen von H sind linear unabhängig.*
(3) *Es gilt $G \cdot H^{\mathrm{T}} = 0$, und die Zeilen von H sind linear unabhängig.*

Beweis: $G \cdot H^{\mathrm{T}} = 0$ ist äquivalent zu $H \cdot G^{\mathrm{T}} = 0$ und impliziert $H \cdot c^{\mathrm{T}} = 0$ für alle $c \in C$, da jedes $c \in C$ Linearkombination von Zeilen von G ist. Beides bedeutet also, dass C im Kern von H liegt.

Die lineare Unabhängigkeit der Zeilen von H ist gleichbedeutend mit $n-k = \operatorname{rg}(H) = \dim \operatorname{Bild}(H)$ und damit gleichbedeutend mit $\dim \operatorname{Kern}(H) = n - \dim \operatorname{Bild}(H) = n-(n-k) = k = \dim C$.

Zusammen sind beide Bedingungen äquivalent zu $C = \operatorname{Kern}(H)$. □

Folgerung 7.16 *Genau dann sind G und H Erzeuger- und Prüfmatrix eines $[n,k]$-Codes, wenn G eine $(k \times n)$-Matrix vom Rang k und H eine $((n-k)\times n)$-Matrix vom Rang $(n-k)$ ist, für die $G \cdot H^{\mathrm{T}} = 0$ ist.*

Beweis: Erzeuger- und Prüfmatrix haben nach Definition und Satz 7.15 diese Eigenschaften. Umgekehrt hat eine $(k\times n)$-Matrix G vom Rang k linear unabhängige Zeilen und ist damit per Definition Erzeugermatrix des von ihren zeilen erzeugten Codes, also von $\operatorname{Bild}(G^{\mathrm{T}})$. H ist dann wieder nach Satz 7.15 eine zugehörige Prüfmatrix. □

Folgerung 7.17 *Wenn eine Erzeugermatrix G die Form $(\mathrm{Id}_k \mid A)$ hat, so ist*

$$H = \left(\begin{array}{c|c} -A^{\mathrm{T}} & \mathrm{Id}_{n-k} \end{array} \right)$$

eine zugehörige Prüfmatrix.

Beweis: Wenn

$$G = \begin{pmatrix} 1 & 0 & \dots\dots & 0 & a_{11} & \dots & a_{1\,n-k} \\ 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \dots\dots & 0 & 1 & a_{k1} & \dots & a_{k\,n-k} \end{pmatrix},$$

und

$$H = \begin{pmatrix} -a_{11} & \dots & -a_{k1} & 1 & 0 & \dots & \dots & 0 \\ \vdots & & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \vdots & \vdots & & \ddots & \ddots & 0 \\ -a_{1\,n-k} & \dots & -a_{k\,n-k} & 0 & \dots & \dots & 0 & 1 \end{pmatrix},$$

dann ist der (i,j)-Eintrag von $G \cdot H^{\mathrm{T}}$ gerade $(e_i \frown (a_{i1},\dots,a_{in-k})) \cdot ((-a_{1j},\dots,-a_{kj}) \frown e_j)^{\mathrm{T}} = -a_{ij} + a_{ij} = 0$.

Außerdem ist $k \geqslant \operatorname{rg}(G) \geqslant \operatorname{rg}(I_k) = k$ und $n-k \geqslant \operatorname{rg}(H) \geqslant \operatorname{rg}(I_{n-k}) = n-k$. □

Ein linearer Code C ist durch eine seiner Erzeugermatrizen G und auch durch eine seiner Prüfmatrizen H festgelegt. G und H sind aber nicht eindeutig durch C bestimmt (nur in der speziellen Form).

Im Falle des $[7,4,3]$-Hamming-Codes und der Erzeugermatrix G von oben ist

$$H = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$$

die passende Prüfmatrix.

Fehlerkorrektur mit Hilfe der Prüfmatrix

Sei $C \subseteq H(n,q)$ ein $[n,k,d]$-Code und $w \in H(n,q)$ wird empfangen. Wir nehmen an, dass höchstens e Übertragungsfehler vorgekommen sind mit $e = \lfloor \frac{d-1}{2} \rfloor$. Nun wird dasjenige $c \in C$ gesucht mit $\mathrm{d}(w,c) \leqslant e$. Aufgrund der Annahmen lässt sich w als $w = c+f$ schreiben mit $c \in C$ und einem Fehler f mit $\mathrm{d}(f,0) \leqslant e$.

Man berechnet nun zunächst das sogenannte Syndrom von w, das ist $H \cdot w^{\mathrm{T}}$. Dafür gilt

$$H \cdot w^{\mathrm{T}} = H \cdot (c+f)^{\mathrm{T}} = H \cdot c^{\mathrm{T}} + H \cdot f^{\mathrm{T}} = 0 + H \cdot f^{\mathrm{T}} = H \cdot f^{\mathrm{T}},$$

d. h. das Syndrom von w ist gleich dem Syndrom des Fehlers f.

Für zwei mögliche Fehler f, f' gilt zudem

$$\mathrm{d}(f-f',0) = \mathrm{d}(f,f') \leqslant \mathrm{d}(f,0) + \mathrm{d}(0,f') \leqslant e + e < d,$$

also ist $f - f' \notin C$ und somit $H \cdot f^{\mathrm{T}} - H \cdot f'^{\mathrm{T}} = H \cdot (f-f')^{\mathrm{T}} \neq 0$. Verschiedene Fehler haben also verschiedene Syndrome.

Man erstellt nun einmal eine Liste aller Syndrome (dies sind $|B_e(0)|$ viele, also relativ wenige), schaut darin nach, welchem Fehgler f das berechnete Syndrom $H \cdot w^{\mathrm{T}}$ entspricht, und korriguiert w zu $c = w - f$. (Im Falle der binären Hamming-Codes wird dieses Verfahren noch deutlich einfacher: siehe unten.)

Syndrom

Man kann das Minimalgewicht eines Codes zwar nicht unmittelbar einer Basis ablesen, also nicht unmittelbar von der Erzeugermatrix, dafür aber von der Prüfmatrix:

Satz 7.18 *Ein linearer Code C hat genau dann Minimalgewicht mindestens d, wenn je $d-1$ Spalten der Prüfmatrix linear unabhängig sind.*

Beweis: Eine Linearkombination $\sum_{i=0}^{n} a_i S_i$ der Spalten S_i von H entspricht gerade einem Produkt $H \cdot a = 0$ mit dem Vektor $a = (a_1, \ldots, a_n)$. Eine lineare Abhängigkeit der Spalten kommt also von einem Vektor $a \in \mathrm{Kern}(H) = C$; die Anzahl der tatsächlich vorkommenden Spalten in dieser nicht-trivialen Linearkombination der Null ist die Anzahl der Komponenten $a_i \neq 0$ in a, also gerade das Gewicht von a. □

Folgerung 7.19 *Ein linearer Code hat Minimalgewicht mindestens 3, wenn je zwei Spalten der Prüfmatrix linear unabhängig sind, d. h. wenn keine null ist und keine das skalare Vielfache einer anderen ist.*

Definition 7.20 *Ein Hamming-Code ist ein linearer Code C vom Minimalgewicht 3, dessen Prüfmatrix zu gegebener Zeilenanzahl die maximale Anzahl von Spalten hat.*

Hamming-Code

Die zu einem gegebenen Vektor v linear abhängigen Vektoren sind gerade die Elemente des von v erzeugten Untervektorraums. Ist m die Anzahl der Zeilen der Prüfmatrix H eines Hamming-Codes, so bilden die Spalten von H ein Repräsentantensystem der eindimensionalen Untervektorräume von $\mathbb{F}_q^m$, d. h. keine Spalte von H ist die Nullspalte und für jeden Vektor $v \in \mathbb{F}_q^m, v \neq 0$ gibt es genau einen Spaltenvektor von H, der ein skalares Vielfaches von v ist. Möchte man H in der speziellen Form $(\ldots | I_m)$ haben, muss man unter den Repräsentanten der eindimensionalen

Untervektorräume inbesondere die Standardbasisvektoren $e_1, \ldots, e_m$ wählen und den letzten m Spalten zuordnen.

Die Anzahl der Vektoren $\neq 0$ in $\mathbb{F}_q^m$ ist $q^m - 1$. Da es $q-1$ Skalarfaktoren $\neq 0$ gibt, gibt es also $\frac{q^m-1}{q-1}$ eindimensionale Untervektorräume von $\mathbb{F}_q^m$, d. h. der zugehörige Hamming-Code besteht aus Wörtern der Länge $n = \frac{q^m-1}{q-1}$. Die Dimension des Hamming-Codes ist dann $k = \frac{q^m-1}{q-1} - m$.

Satz 7.21 *Hamming-Codes sind perfekt.*

Beweis: Für gegebene m ist $n = \frac{q^m-1}{q-1}$ und $k = \frac{q^m-1}{q-1} - m$. Man rechnet nach, dass

$$|C| \cdot |B_1(c)| = q^{\frac{q^m-1}{q-1}-m} \cdot \left(1 + \tfrac{q^m-1}{q-1} \cdot (q-1)\right) = q^{\frac{q^m-1}{q-1}-m} \cdot q^m = q^{\frac{q^m-1}{q-1}} = |H(n, \mathbb{F}_q)|.$$

□

Spezialfall $q = 2$: Hier ist die Situation besonders einfach, da die eindimensionalen Untervektorräume jeweils aus zwei Vektoren bestehen – dem Nullvektor und einem anderen Vektor. Somit kommen sämtliche Vektoren in $\mathbb{F}_q^m \setminus \{0\}$ als Spaltenvektoren von H vor. Ihre Anzahl n ist $2^m - 1$, die Dimension des Codes ist also $2^m - (m+1)$. (Alle binären Hamming-Codes gleicher Länge sind außerdem äquivalent.)

Auch die Fehlerkorrektur ist im Falle $q = 2$ besonders einfach: Die möglichen Fehler sind gerade die Standardbasisvektoren $e_1, \ldots, e_n$ in $\mathbb{F}_2^n$. Das Syndrom $H \cdot e_i^{\mathrm{T}}$ von e_i ist gerade die i-te Spalte von H. Zur Fehlerkorrektur berechnet man also das Syndrom $H \cdot w^{\mathrm{T}}$. Ist das Syndrom 0, so ist kein Fehler aufgetreten. Andernfalls schaut man nach, in welcher Spalte i von H das Syndrom auftritt und ändert das i-te Bit von w.

Liste der perfekten Codes

Ist q eine Primzahlpotenz, so gibt es die folgenden perfekten q-ären Codes (wobei e die Anzahl der korrigierbaren Fehler bezeichnet):

- Triviale Codes, die nur aus einem Wort bestehen. Nimmt man dafür den Nullvektor, so ist es ein $[n, 0, \infty]$-Code mit $e = n$.
- Der triviale $[n, n, 1]$-Code mit $e = 0$. (Alle Wörter sind im Code.)
- Die q-ären Hamming-Codes: $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3]$-Codes mit $e = 1$.
  Außerdem einige nicht-lineare Codes mit gleichen Parametern wie Hamming-Codes.
- Die binären Wiederholungscodes ungerader Länge: Zu jedem $e \in \mathbb{N}$ der $[2e+1, 1, 2e+1]$-Code, der nur die beiden Wörter $(0, 0, \ldots, 0)$ und $(1, 1, \ldots, 1)$ enthält.
- Der binäre Golay-Code [27]: ein $[23, 12, 7]$-Code mit $e = 3$.
- Der ternäre Golay-Code: ein $[11, 6, 5]$-Code mit $e = 2$.

Der binäre Wiederholungscode stimmt für $e = 0$ mit dem trivialen $[1, 1, 1]$-Code und für $e = 1$ mit dem $[3, 1, 3]$-Hamming-Code überein.

[27] Marcel Golay (1902–1989)

Falls q keine Primzahlpotenz ist, so weiß man nicht, ob es perfekte nicht-triviale q-äre Codes gibt. Nur für einige wenige Werte weiß man, dass keine perfekten q-ären Codes existieren außer den trivialen. Im Allgemeinen weiß man auch wenig darüber, welches abseits der perfekten Codes die hinsichtlich der „Packungsdichte“ besten Codes sind.

Kapitel II: Algebra

8 Gruppen

8.1 Homomorphismen und Untergruppen

Zur Erinnerung an Abschnitt 3.3

Definition 8.1 *Eine Gruppe besteht aus einer nicht-leeren Menge G und einer zweistelligen Operation $\circ : G \times G \to G$ auf G, die assoziativ ist, ein neutrales Element e hat, und in der jedes Element $g \in G$ ein inverses Element g^{-1} besitzt.* Gruppe

G heißt kommutative Gruppe, wenn $\circ$ zusätzlich kommutativ ist.

Das neutrale Elemente und die jeweiligen Inversen sind eindeutig bestimmt; insbesondere gilt $(g^{-1})^{-1} = g$ und $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$. Verschiedene notationelle Konventionen sind auf den Seiten 12 f. beschrieben.

Einige wichtige Beispiele:

- die kommutative Gruppe $\mathbb{Z} = (\mathbb{Z}, +, 0)$
- die kommutative Gruppe $\mathbb{Z}_m = \big(\{0, \dots, m-1\}, +_m, 0\big)$, wobei

$$x +_m y = \text{„}\textit{Rest von } x + y \textit{ bei Division durch } m\text{“} = \begin{cases} x + y & \text{falls } x + y < m \\ x + y - m & \text{falls } x + y \geqslant m \end{cases}$$

- die Gruppen $\mathrm{Sym}(M) = (\mathrm{Sym}(M), \circ, \mathrm{id})$ der Permutationen von M, d. h. der Bijektionen $M \to M$ (Diese Gruppen sind für $|M| \geqslant 3$ nicht mehr kommutativ.)
- für einen Vektorraum V die Gruppe $\mathrm{Aut}(V)$ der Vektorraumisomorphismen $V \to V$ mit der Hintereinanderausführung von Abbildungen als Operation;
- die Gruppe $\mathrm{GL}(n, K)$ der invertierbaren $(n \times n)$-Matrizen über einem Körper K, d. h. der $(n \times n)$-Matrizen mit Determinante $\neq 0$ (diese Gruppen sind für $n \geqslant 2$ nicht mehr kommutativ).
- die Gruppe $\mathrm{O}(n, \mathbb{R})$ der orthogonalen $(n \times n)$-Matrizen über $\mathbb{R}$

Definition 8.2 *Eine Abbildung $\varphi : G \to H$ zwischen zwei Gruppen $(G, \circ_G, e_G)$ und $(H, \circ_H, e_H)$ heißt Gruppenhomomorphismus, falls* Gruppenhomomorphismus

- $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$ *für alle $g_1, g_2 \in G$;*
- $\varphi(e_G) = e_H$*;*
- $\varphi(g^{-1}) = \varphi(g)^{-1}$ *für alle $g \in G$.*

Bemerkung 8.3 $\varphi : G \to H$ ist bereits dann ein Gruppenhomomorphismus, wenn die erste Bedingung $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$ für alle $g_1, g_2 \in G$ gilt (Beweis wie im ersten Teil des Beweises von Lemma 5.2).

Beispiele für Gruppenhomomorphismen:

- die „Rest-Abbildung“ $\mathbb{Z} \to \mathbb{Z}_m$, die den Rest bei der Division durch m angibt, also eine Zahl $n = qm + r$ mit $0 \leqslant r < m$ auf r abbildet
- die Determinante $\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$
- die Abbildung $M^{\mathrm{T}} : \mathrm{Sym}(\{1, \ldots, n\}) \to \mathrm{GL}(n, \mathbb{R})$, die einer Permutation σ die Permutationsmatrix $M(\sigma^{-1}) = M(\sigma)^{\mathrm{T}}$ zuordnet (siehe Definition 5.28)
- das Signum (oder Vorzeichen) $\mathrm{sgn} : S_n \to (\{\pm 1\}, \cdot)$ mit $\mathrm{sgn} = \det \circ M^{\mathrm{T}}$

Wenn aus dem Kontext klar ist, dass es um Gruppen geht, spricht man auch kurz von „Homomorphismus“. Es folgen nun eine ganze Reihe von Konzepten und zugehörigen Notationen, die es bereits im Kontext von Vektorräumen gibt (und auch z. B. für Ringe noch eingeführt werden). Falls nicht klar ist, auf welche Art von Struktur man sich bezieht, muss man dies spezifizieren. Falls also zum Beispiel eine Abbildung zwischen Vektorräumen $\varphi : V \to W$ betrachtet wird, die ja auch Gruppen sind, und φ als Homomorphismus bezeichnet wird, dann muss entweder aus dem Kontext klar sein, ob ein Vektorraumhomomorphismus (= lineare Abbildung) oder ein Gruppenhomomorphismus gemeint ist, oder man muss es benennen.

Gruppenisomorphismus

Definition 8.4 *Ein Gruppenhomomorphismus $\varphi : G \to H$ heißt (Gruppen-)Isomorphismus, falls φ bijektiv ist und die Umkehrabbildung φ^{-1} ebenfalls ein Gruppenhomomorphismus ist.*

Zwei Gruppen G und H heißen isomorph zueinander, $G \cong H$, falls es einen Gruppenisomorphismus $G \to H$ gibt.

Bemerkung 8.5 Ein bijektiver Gruppenhomomorphismus ist bereits stets ein Gruppenisomorphismus (Beweis wie bei den linearen Abbildungen).

- Die Gruppe der Vektorraumisomorphismen $K^n \to K^n$ ist isomorph zu der Matrixgruppe $\mathrm{GL}(n, K)$: jede Basiswahl liefert einen Isomorphismus.
- Sind M und N zwei gleichmächtige Mengen, so liefert jede Bijektion $\beta : M \to N$ einen Gruppenisomorphismus $\hat{\beta} : \mathrm{Sym}(M) \to \mathrm{Sym}(N)$, $\sigma \mapsto \beta \circ \sigma \circ \beta^{-1}$.

  Bis auf Isomorphie ist $\mathrm{Sym}(M)$ also durch die Anzahl der Elemente von M festgelegt; für $|M| = n$ schreibt man dann auch S_n für eine zu $\mathrm{Sym}(M)$ isomorphe Gruppe.
- $\mathbb{Z}_1 \cong S_1 \cong \mathrm{GL}(0, \mathbb{R})$ sind drei Realisierungen der trivialen Gruppe, die nur aus einem Element besteht.
- Bis auf Isomorphie gibt es auch nur eine zweielementige Gruppe; sie tritt z. B. als $\mathbb{Z}_2$, S_2 oder als die Gruppe $(\{+1, -1\}, \cdot)$ auf.
  (Erst für vier Elemente gibt es nicht-isomoprhe Gruppen, nämlich $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$.)
- Für jedes $b > 1$ ist die Exponentation zur Basis b ein Gruppenisomorphismus $(\mathbb{R}, +, 0) \to (\mathbb{R}^{>0}, \cdot, 1)$, $r \mapsto b^r$. Der Umkehrisomorphismus ist der Logarithmus $\log_b$ zur Basis b.

- Es gibt auch „zufällige“ Isomorphien, so kann man etwa zeigen, dass die beiden Gruppen S_3 und $\mathrm{GL}(2, \mathbb{F}_2)$ isomorph zueinander sind.
  Dagegen sind $\mathbb{Z}_6$ und S_3 zwei nicht-isomorphe Gruppen mit je 6 Elemente, denn $\mathbb{Z}_6$ ist kommutativ, S_3 aber nicht.

Definition 8.6 *Eine Untergruppe U von G, $U \leqslant G$, ist eine Teilmenge U von G, die bzgl. der auf U eingeschränkten Operationen selbst wieder eine Gruppe ist. U ist also eine Teilmenge, die das neutrale Element enthält, abgeschlossen bzgl. der Gruppenoperation ist und zu jedem seiner Element auch dessen Inverses enthält.* Untergruppe

- Die Gruppe G selbst und die triviale Gruppe $\{e\}$ sind stets Untergruppen von G.
- Jeder Untervektorraum eines Vektorraums ist insbesondere auch eine Untergruppe. (Untervektorräume sind die unter Skalarmultiplikation abgeschlossenen Untergruppen.)
- Die geraden Zahlen bilden eine Untergruppe $2\mathbb{Z}$ von $\mathbb{Z}$.
- Falls G eine (nicht-kommutative) Gruppe ist, so bildet das Zentrum

  $$\mathrm{Z}(G) := \{g \in G \mid g \circ h = h \circ g \text{ für alle } h \in G\}$$

  eine Untergruppe von G.

  Es ist z. B. $\mathrm{Z}(S_3) = \{e\}$ und $\mathrm{Z}\big(\mathrm{GL}(n, \mathbb{R})\big) = \left\{ \begin{pmatrix} r & & 0 \\ & \ddots & \\ 0 & & r \end{pmatrix} \;\middle|\; r \in \mathbb{R}\backslash\{0\} \right\}$.
- Die Gruppe $\mathrm{O}(n, \mathbb{R})$ ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{R})$.
- Die Gruppe der Vektorraumisomorphismen $V \to V$ ist eine Untergruppe von Sym_V.
- $\mathbb{N} \subseteq \mathbb{Z}$ ist ein Beispiel einer unter der Gruppenoperation abgeschlossenen Teilmenge der Gruppe $(\mathbb{Z}, +)$, die das neutrale Element enthält, aber keine Untergruppe ist, da sie nicht unter (additiven) Inversen abgeschlossen ist.
  (Dies im Gegensatz zu Vektorräumen, bei denen der Abschluss einer nicht-leeren Teilmenge unter Addition und Skalarmultiplikation bereits ausreicht für einen Untervektorraum, da die Skalarmultiplikation mit -1 auch die Abgeschlossenheit unter additiven Inversen sicherstellt.)
- $\mathbb{Z}_m$ für $m \geqslant 1$ ist keine Untergruppe von $\mathbb{Z}$: Die zugrundeliegende Menge $\{0, \ldots, m_1\}$ ist zwar eine Teilmenge von $\mathbb{Z}$ und $\mathbb{Z}_m$ ist eine Gruppe; die Addition in $\mathbb{Z}$ und in $\mathbb{Z}_m$ stimmen aber nicht überein. Bezüglich der Addition in $\mathbb{Z}$ ist $\mathbb{Z}_m$ nicht abgeschlossen.

Definition 8.7 *Wenn $\varphi : G \to H$ ein Gruppenhomomorphismus ist, so ist der Kern definiert als* $\mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = e\}$. Kern

Satz 8.8 *Wenn $\varphi : G \to H$ ein Gruppenhomomorphismus ist, so ist der Kern von φ eine Untergruppe von G und das Bild von φ eine Untergruppe von H.*

Beweis: Wie beim analogen Beweis für lineare Abbildungen. □

Definition 8.9 *Der Schnitt einer Menge von Untergruppen von G ist wieder eine Untergruppe von G. Also existiert zu jeder Teilmenge $A \subseteq G$ die kleinste Untergruppe von G, die A enthält. Diese Untergruppe wird die von A erzeugte Untergruppe genannt und mit $\langle A \rangle$ bezeichnet.*

erzeugte Untergruppe

Satz 8.10 *Es gilt*

$$\langle A \rangle = \left\{ {a_1}^{\pm 1} \circ \ldots \circ {a_n}^{\pm 1} \;\middle|\; a_i \in A, n \in \mathbb{N} \right\}$$

mit der Konvention, dass $a^{\pm 1}$ für jede Auswahl der Möglichkeit von $a^{+1} := a$ und a^{-1} steht.

Beweis: Zum einen muss offensichtlich jede A enthaltende Untergruppe auch jedes der Produkte ${a_1}^{\pm 1} \circ \ldots \circ {a_n}^{\pm 1}$ enthalten. Zum andern bildet die Menge dieser Produkte eine A enthaltende Untergruppe: Für $n = 0$ enthält man das neutrale Element („leeres Produkt“); mit $n = 1$ enthält man jedes Element von A. Die Menge ist zudem offensichtlich unter der Gruppenoperation abgeschlossen und ebenso unter Inversen, da $({a_1}^{\pm 1} \circ \ldots \circ {a_n}^{\pm 1})^{-1} = {a_n}^{\mp 1} \circ \ldots \circ {a_1}^{\mp 1}$. □

Es gelten die gleichen notationellen Konventionen wie bei Vektorräumen, man schreibt also z. B. kurz $\langle g_1, \ldots, g_k \rangle$ statt $\langle \{g_1, \ldots, g_k\} \rangle$.

8.2 Zyklische Gruppen

Definition 8.11 *Sei G eine Gruppe und $g \in G$. Man definiert für $n \in \mathbb{Z}$:*

Potenzieren in Gruppen

$$g^n := \begin{cases} \underbrace{g \circ \cdots \circ g}_{n \text{ mal}} & n > 1 \\ e & n = 0 \\ (\underbrace{g \circ \cdots \circ g}_{|n| \text{ mal}})^{-1} & n < 1 \end{cases}$$

Man kann die Definition alternativ auch in induktiver Form angeben:

$$\begin{aligned} g^0 &:= e \\ g^{n+1} &:= g \circ g^n \text{ für } n \in \mathbb{N} \\ g^n &:= (g^{-n})^{-1} \text{ für } n \in \mathbb{Z} \setminus \mathbb{N} \end{aligned}$$

Ist die Gruppe $(G, +)$ additiv geschrieben, so schreibt man $n \cdot g$ oder ng statt g^n.

Insbesondere gilt $g^1 = g$, und g^{-1} bezeichnet wie bisher das Inverse von g, d. h die Notation ist verträglich mit den bisherigen Schreibweisen.

- In $\mathbb{Z}$ ist $n \cdot z$ die normale Multiplikation; in $\mathbb{Z}_m$ ist es die „Multiplikation modulo$m$“.
- In $\mathrm{GL}(2, \mathbb{R})$ ist beispielsweise

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 14 \\ 0 & 8 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}^{-2} = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}^2 = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{4} \end{pmatrix}$$

Satz 8.12 *Es gelten die Potenzgesetze, wie man sie vom Spezialfall der Gruppe* $(\mathbb{R}\setminus\{0\},\cdot)$ *her kennt, d. h.:*

$$g^{n+m} = g^n \circ g^m \qquad \text{und} \qquad (g^n)^m = g^{nm}$$

bzw. in der additiven Schreibweise

$$(n+m)g = ng + mg \qquad \text{und} \qquad m(ng) = (mn)g$$

für alle $g \in G$ *und* $n, m \in \mathbb{Z}$.

Beweis: Man sieht zunächst an der Definition, dass $g^{-n} = (g^n)^{-1}$.

Für die erste Regel sollte man Fallunterscheidungen nach den Vorzeichen von n und m machen; jeder einzelne Fall ist aber nach Definition klar. Die zweite Regel ist ebenfalls unmittelbar einsichtig für $n, m > 0$. Falls $n = 0$ oder $m = 0$ kommt nach Definition von g^0 auf beiden Seiten e heraus. Ist mindestens einer der beiden Exponenten negativ, so kann man sich durch $g^{-n} = (g^n)^{-1}$ auf den positiven Fall zurückziehen. □

Die Regel $g \circ g^{-1} = g^{-1} \circ g = g^0 = e$ ist ein Spezialfall des ersten Potenzgesetzes; die Regel $(g^{-1})^{-1} = g$ ist ein Spezialfall des zweiten Potenzgesetzes. Ebenso als Spezialfall des zweiten Gesetzes erhält man $(g^{-1})^n = (g^n)^{-1} = g^{-n}$.

Bemerkung 8.13 Das erste Potenzgesetz besagt anders ausgedrückt, dass es für jedes $g \in G$ einen Homomorphismus gibt:

$$g^{\sqcup} : (\mathbb{Z}, +) \to (G, \circ),\ n \mapsto g^n.$$

Das Bild dieses Homomorphismus ist die von g erzeugte Untergruppe $\langle g \rangle$.

Definition 8.14 **(a)** *Eine Gruppe heißt zyklisch, wenn sie von einem Element erzeugt ist.* Zyklische Gruppe, Ordnung

(b) *Die Ordnung einer Gruppe* G *ist die Anzahl der Elemente von* G *(in* $\mathbb{N} \cup \{\infty\}$*).*

(c) Die Ordnung eines Gruppenelements $g \in G$, $\operatorname{ord}(g)$, ist die Ordnung der von g erzeugten Untergruppe $\langle g \rangle$.

- In jeder Gruppe ist e das einzige Element mit Ordnung 1.
- Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch; sie hat zwei Erzeuger: 1 und -1.
  Die Ordnung der Gruppe ist ∞; alle Elemente außer 0 haben Ordnung ∞.
- Die Gruppe $\mathbb{Z}_{12}$ ist zyklisch: 1, 5, 7 und 11 haben jeweils Ordnung 12 und sind daher Erzeuger. Die Ordnung aller Element sieht man in der folgenden Tabelle:

Element	0	1	2	3	4	5	6	7	8	9	10	11
Ordnung	1	12	6	4	3	12	2	12	3	4	6	12

- Die Gruppe S_3 hat die Ordnung 6. Die Identität hat Ordnung 1, die drei Transpositionen (Spiegelungen) jeweils Ordnung 2 und die beiden „3-Zykel“ (Drehungen) Ordnung 3. Man sieht insbesondere, dass die Gruppe nicht zyklisch ist.

  Allgemeiner hat die Gruppe S_n Ordnung $n!$ und ist für $n > 2$ nicht zyklisch, da nicht kommutativ.

Satz 8.15 *Zyklische Gruppen sind kommutativ.*

BEWEIS: Es gilt $g^m \circ g^n = g^{m+n} = g^{n+m} = g^n \circ g^m$. □

Eine zyklische Gruppe $\langle g\rangle$ ist das Bild der kommutativen Gruppe $\mathbb{Z}$ unter dem Homomorphismus $g^{\sqcup}$. Allgemeiner gilt, dass homomorphe Bilder kommutativer Gruppen wieder kommutativ sind, d. h. falls $\varphi : G \to H$ ein surjektiver Gruppenhomomorphismus ist und G kommutativ, dann ist H kommutativ, da $h_1 \circ h_2 = \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \circ g_2) = \varphi(g_2 \circ g_1) = \varphi(g_2) \circ \varphi(g_1) = h_2 \circ h_1$.

Satz 8.16 *Untergruppen und homomorphe Bilder zyklischer Gruppen sind wieder zyklisch.*

BEWEIS: Sei $\varphi : G = \langle g\rangle \to H$ ein Gruppenhomomorphismus. Dann ist Bild(φ) zyklisch, da

$$\text{Bild}(\varphi) = \{\varphi(g^n) \mid n \in \mathbb{Z}\} = \{\varphi(g)^n \mid n \in \mathbb{Z}\} = \langle\varphi(g)\rangle$$

Sei nun $U \leqslant G = \langle g\rangle$. Die triviale Untergruppe $U = \{e\}$ ist natürlich zyklisch. Falls $U \neq \{e\}$, so gibt es ein $u = g^n \in U \setminus \{e\}$. Dann ist auch $u^{-1} = (g^n)^{-1} = g^{-n} \in U$, d. h. man kann $n > 0$ annehmen. Wähle nun $k > 0$ minimal mit der Eigenschaft, dass $g^k \in U$. Dann ist offensichtlich $\langle g^k\rangle \subseteq U$. Falls $g^m \in U$, so schreibt man $m = qk + r$ mit $r \in \{0, \ldots, k-1\}$ (Division mit Rest) und sieht mit den Potenzgesetzen: $g^r = g^{m-qk} = g^m \circ (g^k)^{-q} \in U$. Aus der Minimalität von k folgt also $r = 0$, und somit $g^m = (g^q)^k \in \langle g^k\rangle = U$. □

Allgemein gilt bei einem Homomorphismus $\varphi : G \to H$ mit $X \subseteq G$, dass $\varphi[\langle X\rangle] = \langle\varphi[X]\rangle$, d. h. die Bilder von Erzeugern sind Erzeuger des Bilds.

Satz 8.17 *Eine zyklische Gruppe ist entweder von unendlicher Ordnung und isomorph zu* $(\mathbb{Z}, +)$ *oder von endlicher Ordnung* $m \geqslant 1$ *und isomorph zu* $(\mathbb{Z}_m, +_m)$.

BEWEIS: Sei $G = \langle g\rangle$ zyklisch. Man betrachtet den surjektiven Homomorphismus $g^{\sqcup} : \mathbb{Z} \to G$, $n \mapsto g^n$. Falls $g^{\sqcup}$ injektiv ist, ist $g^{\sqcup}$ ein Isomorphismus und dann gilt $G \cong \mathbb{Z}$. Andernfalls gibt es $k \neq l$ mit $g^k = g^l$. Es gilt nun

$$g^k = g^l \iff g^{k-l} = g^k \circ g^{-l} = g^l \circ g^{-l} = e \iff k - l \in \text{Kern}(g^{\sqcup})$$

also ist Kern($g^{\sqcup}$) $\neq \{0\}$. Nach dem Satz 8.16 ist Kern($g^{\sqcup}$) eine zyklische Untergruppe von $\mathbb{Z}$, also von der Form $\langle m\rangle = \{zm \mid z \in \mathbb{Z}\}$ mit $m \neq 0$. Dabei kann man $m > 0$ wählen, da $\langle m\rangle = \langle -m\rangle$, und es gilt also

$$(*) \quad g^k = g^l \iff k - l \in \text{Kern}(g^{\sqcup}) = \langle m\rangle \iff m \mid k - l$$

Daraus folgt nun $G = \{g^0, g^1, \ldots, g^{m-1}\}$ mit $|G| = m$, denn zum einem sieht man mit $(*)$, dass die Elemente $g^0, g^1, \ldots, g^{m-1}$ paarweise verschieden sind. Zum andern kann man jedes n schreiben als $n = qm + r$ mit $0 \leqslant r < m$, woraus $g^n = g^r \in \{g^0, g^1, \ldots, g^{m-1}\}$ folgt.

Wegen $g^n = g^{n-m}$ gilt für $k, l \in \{0, \ldots, m-1\}$ schließlich $g^k \circ g^l = g^{k+l} = g^{k +_m l}$, und damit ist die Abbildung $G \to \mathbb{Z}_m$, $g^i \mapsto i$ ein Gruppenisomorphismus. □

Man schreibt $m\mathbb{Z}$ für die zyklische Untergruppe $\{mz \mid z \in \mathbb{Z}\}$ von $\mathbb{Z}$. $m\mathbb{Z}$

Im nächsten Abschnitt werden wir sehen, dass im zweiten Fall „Kern($g^{\sqcup}$) $= m\mathbb{Z}$“ aus dem Homomorphiesatz unmittelbar $G \cong \mathbb{Z}/m\mathbb{Z}$ folgt, wobei $\mathbb{Z}/m\mathbb{Z}$ eine abstrakt gewonnene, zu $\mathbb{Z}_m$ isomorphe Gruppe ist.

Folgerung 8.18 *Die Ordnung eines Gruppenelements g ist das kleinste $m > 0$ mit $g^m = e$, sofern es existiert, und ∞ sonst. Es gilt genau dann $g^k = e$, wenn m ein Teiler von k ist.*

Wenn $G = \langle g \rangle \cong \mathbb{Z}$ eine unendliche zyklische Gruppe ist und H eine beliebige Gruppe, dann existiert zu jedem $h \in H$ ein eindeutig bestimmter Gruppenhomomorphismus $G \to H$ mit $g \mapsto h$, nämlich die Abbildung $g^n \mapsto h^n$. In diesem Aspekt ähnelt also der Erzeuger einer unendlichen zyklischen Gruppe der Basis eines Vektorraums.

Wenn $G = \langle g \rangle \cong \mathbb{Z}_m$ eine endliche zyklische Gruppe ist und H eine beliebige Gruppe, dann existiert nicht unbedingt ein Gruppenhomomorphismus $G \to H$ mit $g \mapsto h$, denn es gilt $g^m = e$, also muss auch $h^m = \varphi(g)^m = \varphi(g^m) = \varphi(e) = e$ gelten. Dies ist aber das einzige Hindernis, d. h. man kann zeigen, dass ein (eindeutig bestimmter) Gruppenhomomorphismus $G \to H$ mit $g \mapsto h$ genau dann existiert, wenn $h^m = e$, also wenn $\operatorname{ord}(h) \mid \operatorname{ord}(g)$.

Anders als bei Vektorräumen kann man bei Gruppen also nicht Homomorphismen beliebig auf minimalen Erzeugendensystemen vorschreiben, Das liegt daran, dass in Vektorräumen Basen „frei“ sind, also keine besonderen Abhängigkeiten vorweisen können, während in Gruppen zusätzliche Gleichungen gelten können.

Definition 8.19 *Ein Automorphismus einer Gruppe G ist ein Isomorphismus $G \to G$. Die Menge der Automorphismen von G bildet unter der Hintereinanderausführung von Abbildungen die Automorphismengruppe von G, $\operatorname{Aut}(G)$.*

Automorphismus

Satz 8.20 *Sei $G = \langle g \rangle$ zyklisch. Dann sind die Automorphismen von G genau die Homomorphismen $\varphi : G \to G$, für die $\varphi(g)$ ein Erzeuger von G ist.*

Beweis: Wegen $\operatorname{Bild}(\varphi) = \langle \varphi(g) \rangle$ ist ein Homomorphismen $\varphi : G \to G$ genau dann surjektiv, wenn $\varphi(g)$ ein Erzeuger von G ist. Im endlichen Fall $G \cong \mathbb{Z}_m$ sind surjektive Abbildungen zwischen gleichmächtigen Mengen stets auch injektiv. Im Fall $G \cong \mathbb{Z}$ hat G zwei Erzeuger, die 1 und -1 in $\mathbb{Z}$ entsprechend. Die zugehörigen Homomorphismen sind id und $g^n \mapsto g^{-n}$ und sind beide ebenfalls injektiv. □

$\mathbb{Z}_{12}$ hat vier Erzeuger, nämlich $1, 5, 7, 11$, also auch vier Automorphismen: die durch $1 \mapsto 1$ gegebene Identität; die durch $1 \mapsto 11$ gegebene „Spiegelung“ $n \mapsto -n$, die auf der Uhr der Spiegelung an der Mittelsenkrechten entspricht, und zwei durch $1 \mapsto 5$ und $1 \mapsto 7$ bestimmte Automorphismen. Diese Automorphismen haben die folgenden Wertetabellen:

	0	1	2	3	4	5	6	7	8	9	10	11
$1 \mapsto 1$	0	1	2	3	4	5	6	7	8	9	10	11
$1 \mapsto 11$	0	11	10	9	8	7	6	5	4	3	2	1
$1 \mapsto 5$	0	5	10	3	8	1	6	11	4	9	2	7
$1 \mapsto 7$	0	7	2	9	4	11	6	1	8	3	10	5

Dies sind also die einzigen mit der Addition $+_{12}$ verträglichen Permutationen von $\{0, \ldots, 11\}$. (Wir werden noch sehen, dass es gerade die Multiplikationen mit $1, 11, 5$ bzw. 7 im Ring $\mathbb{Z}_{12}$ sind.)

Die Existenz dieser Automorphismen bedeutet folgendes: Wenn man in der Gruppentafel von $\mathbb{Z}_{12}$ die Reihenfolge der Spalten und Zeilen beliebig vertauscht und die Zahlen $0, \ldots, 11$ durch irgendwelche Symbole ersetzt, kann man nicht mehr herausfinden, welches Symbol für welche

Zahl stand. Man kann die Ordnung der Elemente erkennen, kann aber die vier Elemente mit Ordnung 12 nicht unterscheiden.

Am Beispiel einer Gruppe G der Ordnung 4: Wenn die Gruppentafel gegeben ist als

$+$	$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$
$\diamondsuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
$\spadesuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$
$\clubsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$

kann man erkennen, dass $\spadesuit$ das neutrale Element ist, dass folglich $\diamondsuit$ ein Element der Ordnung 2 ist (da $\diamondsuit + \diamondsuit = \spadesuit$) und dass $\heartsuit$ und $\clubsuit$ Elemente der Ordnung 4 sind (da z.B. $2 \cdot \heartsuit = \diamondsuit \neq \spadesuit$, $3 \cdot \heartsuit = \diamondsuit + \heartsuit = \clubsuit \neq \spadesuit$, aber $4 \cdot \heartsuit = \clubsuit + \heartsuit = \spadesuit$).

Also bekommt man zwei mögliche Isomorphimsen $\mathbb{Z}_4 \to G$, die durch $i_\heartsuit : 1 \mapsto \heartsuit$ und $i_\clubsuit : 1 \mapsto \clubsuit$ festgelegt sind. $\mathbb{Z}_4$ hat genau einen nicht-trivialen Automorphsimus, nämlich $n \mapsto -n$, durch die $i_\heartsuit$ und $i_\clubsuit$ ineinander übergehen: $i_\heartsuit(x) = i_\clubsuit(-x)$.

Zusammenfassung der Ergebnisse über zyklische Gruppen

unendliche Ordnung, somit $\cong \mathbb{Z}$	**endliche Ordnung** m**, somit** $\cong \mathbb{Z}_m$
Die Ordnung von 0 ist 1, die Ordnung aller anderer Elemente ist ∞.	Die Ordnung von k in $\mathbb{Z}_m$ ist $\frac{m}{\mathrm{ggT}(k,m)}$ (*das kleinste l, für das m ein Teiler von $l \cdot k$ ist*)
Die Erzeuger von $\mathbb{Z}$ sind 1 und -1.	Die Erzeuger von $\mathbb{Z}_m$ sind die zu m teilerfremden Zahlen k.
Die Untergruppen von $\mathbb{Z}$ sind $\langle m\rangle = m\mathbb{Z} := \{k \cdot m \mid k \in \mathbb{Z}\}$ für $m \in \mathbb{N}$. Es ist $0\mathbb{Z} = \{0\}$ und $1\mathbb{Z} = \mathbb{Z}$. Für $k \in \mathbb{Z}, k \neq 0$ ist $\langle k\rangle \cong \mathbb{Z}$.	Die Untergruppen von $\mathbb{Z}_m$ sind $\langle n\rangle = n\mathbb{Z}_m := \{0, n, 2n, \ldots, (\frac{m}{n} - 1)n\} \cong \mathbb{Z}_{\frac{m}{n}}$ für alle Teiler n von m. Es ist $m\mathbb{Z}_m = \{0\}$ und $1\mathbb{Z}_m = \mathbb{Z}_m$. Für $k \in \mathbb{Z}$ gilt $\langle k \cdot 1\rangle = \langle \mathrm{ggT}(k,m)\rangle \cong \mathbb{Z}_{\frac{m}{\mathrm{ggT}(k,m)}}$.
Die homomorphen Bilder von $\mathbb{Z}$ sind $\mathbb{Z}$ selbst und alle $\mathbb{Z}_m$.	Die homomorphen Bilder von $\mathbb{Z}_m$ sind die $\mathbb{Z}_k$ für Teiler k von m.
$\mathrm{Aut}(\mathbb{Z}) = (\{\mathrm{id}, n \mapsto -n\}, \circ) \cong \mathbb{Z}_2$	$\mathrm{Aut}(\mathbb{Z}_m)$ wird im Abschnitt 9.2 näher bestimmt.

Definition 8.21 *Seien $G_1, \ldots, G_n$ Gruppen. Dann wird das kartesische Produkt $G_1 \times \cdots \times G_n$ der zugrundeliegenden Mengen durch die komponentenweisen Operation* direktes Produkt

$$(g_1, \ldots, g_n) \circ (h_1, \ldots, h_n) := (g_1 \circ h_1, \ldots, g_n \circ h_n)$$

zu einer Gruppe, dem direkten Produkt der G_i. Diese Gruppe wird ebenfalls mit $G_1 \times \cdots \times G_n$ bezeichnet.

Man kann leicht nachprüfen, dass dadurch tatsächlich eine Gruppe definiert wird. Außerdem sieht man, dass $G_1 \times \cdots \times G_n$ genau dann kommutativ ist, wenn alle G_i es sind.

Die Gruppentafel von $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist:

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Man sieht, dass alle Elemente $\neq (0,0)$ die Ordnung 2 haben. Diese Gruppe ist also nicht isomorph zu $\mathbb{Z}_4$.
(Man kann übrigens zeigen, dass es keine weiteren Gruppen der Ordnung 4 gibt: Jede ist entweder zu $\mathbb{Z}_4$ oder zu $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorph.)

Satz 8.22 *Genau dann ist $\mathbb{Z}_m \times \mathbb{Z}_n$ zyklisch (also $\cong \mathbb{Z}_{mn}$), wenn m und n teilerfremd sind.*

Beweis: Aus Folgerung 8.18 sieht man, dass $k \cdot (a,b) = (k \cdot a, k \cdot b)$ genau dann $(0,0)$ ist, wenn k sowohl von $\mathrm{ord}_{\mathbb{Z}_m}(a)$ als auch von $\mathrm{ord}_{\mathbb{Z}_n}(b)$ geteilt wird. Das kleinste solche k, also $\mathrm{ord}_{\mathbb{Z}_m \times \mathbb{Z}_n}(a,b)$, ist gerade $\mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))$. Diese Zahl kann maximal den Wert $\mathrm{kgV}(m,n)$ annehmen, und tut dies z. B. für $a = b = 1$, oder allgemeiner für Wahl von Erzeugern a von $\mathbb{Z}_m$ und b von $\mathbb{Z}_n$. Also ist $\mathbb{Z}_m \times \mathbb{Z}_n$ genau dann zyklisch, wenn $\mathrm{kgV}(m,n) = mn$, was genau dann der Fall ist, wenn m und n teilerfremd sind. □

- Es ist $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$. Durch $(1,1) \mapsto 1$ wird ein Isomorphismus mit folgender Wertetabelle festgelegt:

		$2 \cdot (1,1)$	$3 \cdot (1,1)$	$4 \cdot (1,1)$	$5 \cdot (1,1)$
		$=$	$=$	$=$	$=$
$(0,0)$	$(1,1)$	$(2,0)$	$(0,1)$	$(1,0)$	$(2,1)$
0	1	2	3	4	5

  Diese Abbildung ist also mit der Gruppenoperation verträglich, d. h. es wird zum Beispiel $5 +_6 3 = 2$ abbgebildet auf $(2,1) +_{\mathbb{Z}_3 \times \mathbb{Z}_2} (0,1) = (2 +_3 0, 1 +_2 1) = (2,0)$.

- Dagegen ist $\mathbb{Z}_2 \times \mathbb{Z}_2$ nicht zyklisch, also nicht isomorph zu $\mathbb{Z}_4$. Beides sind verschiedene kommutative Gruppen der Ordnung 4.

- In der Ordnung $180 = 2^2 \cdot 3^2 \cdot 5$ gibt es vier paarweise nicht-isomorphe kommutative Gruppen. Für jede Zerlegung von 180 in Faktoren bekommt man ein entsprechendes direktes Produkt zyklischer Gruppen, wobei man nach dem vorherigen Satz teilerfremde Faktoren zusammenfassen kann:

  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{30}$
  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{45} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_{90}$
  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{20} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_{60}$
  $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9 \cong \mathbb{Z}_4 \times \mathbb{Z}_{45} \cong \mathbb{Z}_5 \times \mathbb{Z}_{36} \cong \mathbb{Z}_9 \times \mathbb{Z}_{20} \cong \mathbb{Z}_{180}$

  Man kann zeigen, dass es keine weiteren kommutativen Gruppen der Ordnung 180 gibt: Alle endlichen kommutativen Gruppen sind direkte Produkte zyklischer Gruppen.

8.3 Quotientengruppen

Sei nun stets $(G, +)$ eine kommutative Gruppe und U eine Untergruppe. (Der nicht-kommutative Fall wird am Ende des Abschnitts als Zusatzlektüre behandelt.)

Nebenklasse
Index

Definition 8.23 *Man definiert eine Äquivalenzrelation $\sim_U$ auf G durch*

$$g_1 \sim_U g_2 :\Longleftrightarrow g_1 - g_2 \in U$$

Die Äquivalenzklasse von $g \in G$ bezüglich $\sim_U$ ist die sogenannte Nebenklasse von U

$$g + U := \{g + u \mid u \in U\}$$

G/U bezeichnet die Menge der Nebenklassen; ihre Anzahl ist der Index $[G : U]$ von U in G.

(Die Behauptungen sind leicht nachzurechnen; oder siehe Satz 8.29)

Satz 8.24 *Je zwei Nebenklassen haben die gleiche Anzahl von Elementen.*

Beweis: $f : g_1 + U \to g_2 + U$, $x \mapsto g_2 + (-g_1) + x$ ist eine Bijektion, da $x \mapsto g_1 + (-g_2) + x$ offenbar eine beidseitige Umkehrabbildung ist. □

Folgerung 8.25 (Satz von Lagrange [28]) *Wenn G endlich ist und $U \leqslant G$, dann gilt*

$$|G| = |U| \cdot [G : U]$$

Die Ordnung einer Untergruppe teilt also die Gruppenordnung; insbesondere teilt auch die Ordnung eines Gruppenelementes die Gruppenordnung.

Der Satz von Lagrange gilt auch im nicht-kommutativen Fall!

- Falls $|G| = p$ eine Primzahl ist und $0 \neq g \in G$, dann muss die Ordnung von g ein Teiler von p, aber größer 1 sein. Also hat g die Ordnung p, ist somit Erzeuger der Gruppe, die also zyklisch ist und damit isomoprh zu $\mathbb{Z}_p$.
- Wichige Anwendungen des Satzes von Lagrange sind der kleine Satz von Fermat 9.18 und der Satz von Euler 9.17 aus dem nächsten Kapitel!

Satz 8.26 *G/U wird durch*

$$(g_1 + U) + (g_2 + U) := (g_1 + g_2) + U$$

zu einer Gruppe. Die Gruppenstruktur auf G/U ist also so, dass die Abbildung $G \to G/U$, $g \mapsto g+U$, die jedem Element ihre Nebenklasse zuordnet, ein (surjektiver) Gruppenhomomorphismus mit Kern U ist. G/U heißt die Quotientengruppe von G nach U.

Im nicht-kommutativen Fall geht dies nur für sehr spezielle Gruppen, sogenannte normale Untergruppen oder Normalteiler.

[28] Joseph-Louis Lagrange (1736–1813)

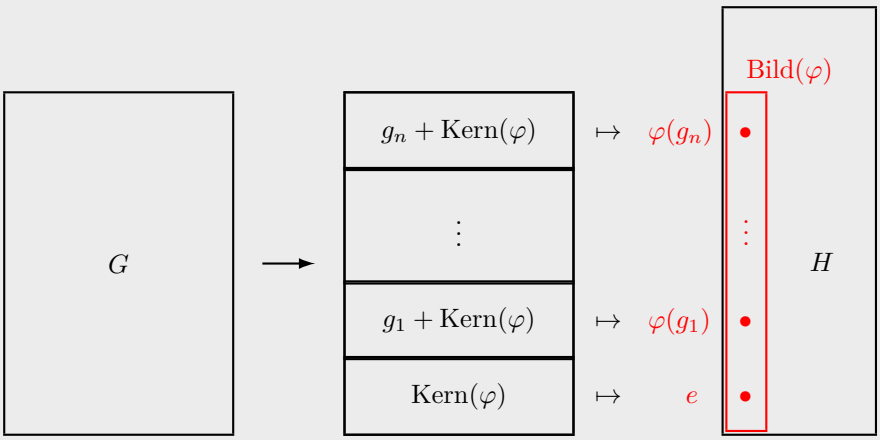
BEWEIS: Zu zeigen ist zunächst die Wohldefiniertheit: Gilt $g_1+U = g_1'+U$, also $g_1-g_1' = u_1 \in U$, und $g_2+U = g_2'+U$, also $g_2-g_2' = u_2 \in U$, dann ist $(g_1+g_2)-(g_1'+g_2') = (g_1-g_1')+(g_2-g_2') = u_1+u_2 \in U$, d. h. $(g_1+g_2)+U = (g_1'+g_2')+U$.

Die Addition auf G/U ist dann assoziativ, da die Addition auf G es ist und repräsentantenweise addiert wird. Ebenso sieht man, dass $0+U$ neutrales Element und $(-g)+U$ inverses Element zu $g+U$ ist. □

Satz 8.27 (Homomorphiesatz für kommutative Gruppen) *Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so kann man φ zusammensetzen als Komposition der folgenden Homomorphismen:*

	surjektiv		bijektiv		injektiv	
G	$\longrightarrow$	$G/\mathrm{Kern}(\varphi)$	$\xrightarrow{\cong}$	$\mathrm{Bild}(\varphi)$	$\longrightarrow$	H
g	$\mapsto$	$g+\mathrm{Kern}(\varphi)$	$\mapsto$	$\varphi(g)$	$\mapsto$	$\varphi(g)$

Illustration der Zerlegung:



BEWEIS: Man muss im Wesentlichen nur nachrechnen, dass

$$\begin{aligned}\varphi(g_1) = \varphi(g_2) &\iff \varphi(g_1-g_2) = \varphi(g_1)-\varphi(g_2) = 0\\ &\iff g_1-g_2 \in \mathrm{Kern}(\varphi) \iff g_1+\mathrm{Kern}(\varphi) = g_2+\mathrm{Kern}(\varphi)\end{aligned}$$

Dies zeigt die Wohldefiniertheit und Bijektivität der mittleren Abbildung. Dass sie ein Gruppenhomomorphismen ist, ergibt sich aus der Homomorphie-Eigenschaft von φ:

$$(g_1+\mathrm{Kern}(\varphi))+(g_2+\mathrm{Kern}(\varphi)) = (g_1+g_2)+\mathrm{Kern}(\varphi) \mapsto \varphi(g_1+g_2) = \varphi(g_1)+\varphi(g_2)$$

Für die linke Abbildung wurde alles im Satz 8.26 gezeigt, für die rechte Abbildung ist alles trivial. □

Wir betrachten den Homomorphismus „*modulo m*“: $\mathbb{Z} \to \mathbb{Z}_m$, der einer Zahl ihren Rest bei der Division durch m zuweist. Die Abbildung ist surjektiv und hat den Kern $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$. Also gilt $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

Die Elemente auf der linken Seite sind Teilmengen von $\mathbb{Z}$, nämlich die Nebenklassen von $m\mathbb{Z}$:

$$\begin{aligned} m\mathbb{Z} &= \{\dots, -2m, -m, 0, m, 2m, \dots\}, \\ 1 + m\mathbb{Z} &= \{\dots, -2m+1, -m+1, 1, m+1, 2m+1, \dots\}, \\ 2 + m\mathbb{Z} &= \{\dots, -2m+2, -m+2, 2, m+2, 2m+2, \dots\}, \\ &\dots \\ (m-1) + m\mathbb{Z} &= \{\dots, -2m-1, -m-1, -1, m-1, 2m-1, \dots\} \end{aligned}$$

Die Addition ist die normale Addition in $\mathbb{Z}$ auf den Repräsentanten:

$$13 + m\mathbb{Z} + (-140 + m\mathbb{Z}) = -127 + m\mathbb{Z}$$

Es ist vergleichsweise einfach zu zeigen, dass dies eine Gruppe ist.

Die Elemente auf der rechten Seite sind die Zahlen $0, 1, \dots, m-1 \in \mathbb{Z}$, also einfacherer Objekte als auf der linken Seite. Sie bilden ein Repräsentantensystem der Nebenklassen $\mathbb{Z}/m\mathbb{Z}$. Die Addition $+_m$ ist dagegen komplzierter; sie ist eine auf dieses Repräsentantensystem angepasste „korrigierte“ Addition. Es ist etwas mühsamer direkt zu zeigen, dass die Gruppenaxiome erfüllt sind.

Gilt $a + m\mathbb{Z} = b + m\mathbb{Z}$ für ganze Zahlen a und b, also $m \mid a - b$, so schreibt man dies auch als sogenannte *Kongruenzgleichung* $a \equiv b \bmod m$ („a ist kongruent zu b modulo m“), mit diversen Varianten. „$\dots \equiv \dots \bmod m$“ ist hier also eine zweistellige Relation auf $\mathbb{Z}$.

Gerne wird aber auch der Homomorphismus $\mathbb{Z} \to \mathbb{Z}_m$ mit „mod m“ bezeichnet, d. h. man schreibt $a \bmod m$ für den Rest von a bei der Division durch m.

Ist m fest, so schreibt man auch gerne kurz $\overline{a}$ für die Nebenklasse $a + m\mathbb{Z}$.

Sei $k \mid m$. Dann gibt es folgendermaßen einen Homomorphismus „*modulo* k“: $\mathbb{Z}_m \to \mathbb{Z}_k$:

Die Rest-Abbildung $\bmod_k : \mathbb{Z} \to \mathbb{Z}_k$ ist konstant auf den Nebenklassen von $\mathbb{Z}_m$ in $\mathbb{Z}$. Denn falls $m \mid a - b$, gilt erst recht $k \mid a - b$, d. h. was gleichen Rest modulo m lässt, lässt erst recht gleichen Rest modulo k. Die Nebenklassen sind nun gerade die Urbilder der Rest-Abbildung $\bmod_m : \mathbb{Z} \to \mathbb{Z}_m$. Daher kann man die Abbildung $\bmod_k : \mathbb{Z}_m \to \mathbb{Z}_k$ definieren durch „$\bmod_k \circ \bmod_m^{-1}$“, d. h. durch $z \mapsto \bmod_k(z')$ für ein z' mit $\bmod_m(z') = z$.

Man kann also den Rest einer ganzen Zahl bei der Division durch k erhalten, indem man erst den Rest bei der Division durch m nimmt und dann weiter dividiert durch k. (Falls k kein Teiler von m ist, geht dies nicht: Zum Beispiel lässt 9 bei der Division durch 5 den Rest 4 und 4 lässt bei der Division durch 2 den Rest 0. Teilt man dagegen 9 direkt durch 2, bleibt Rest 1!)

Der Kern des Homomorphimus $\bmod_k : \mathbb{Z}_m \to \mathbb{Z}_k$ ist die von dem Element $k \in \mathbb{Z}_m$ erzeugte Untergruppe $\langle k \rangle = k \cdot \mathbb{Z}_m = \{0, k, 2k, \dots, (\frac{m}{k} - 1) \cdot k\} \cong \mathbb{Z}_{\frac{m}{k}}$. Also hat man mit dem Homomorphiesatz $\mathbb{Z}_m / k\mathbb{Z}_m \cong \mathbb{Z}_k$.

In der „abstrakten“ Version betrachtet man die von $k + m\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$ erzeugte Untergruppe. Sie besteht aus allen Nebenklassen von $m\mathbb{Z}$, die in $k\mathbb{Z}$ enthalten sind. Schreibt man dafür $k\mathbb{Z}/m\mathbb{Z}$, erhält man $(\mathbb{Z}/m\mathbb{Z}) \,/\, (k\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/k\mathbb{Z}$. Man kann also gewissermaßen durch $m\mathbb{Z}$ kürzen.

Ist V ein K-Vektorraum und U ein Untervektorraum, wird die Quotientengruppe V/U durch die (repräsentantenunabhängige) Skalarmultiplikation $k \cdot (v+U) := (k \cdot v) + U$ sogar zu einem K-Vektorraum. Im Homomorphiesatz sind die Abbildungen dann alle linear.

Ist U ein k-dimensionaler Untervektorraum von $\mathbb{R}^n$, gilt $\mathbb{R}^n/U \cong \mathbb{R}^{n-k}$.

Nicht-kommutativer Fall:

Sei nun G eine beliebige, multiplikativ geschriebene Gruppe.

Definition 8.28 *Sei $U \subseteq G$. Man definiert die zweistelligen Relationen ${}_U\!\sim$ und $\sim_U$ durch*

$$g_1 \ {}_U\!\sim\ g_2 :\iff g_1^{-1} \cdot g_2 \in U.$$
$$g_1 \sim_U g_2 :\iff g_2 \cdot g_1^{-1} \in U$$

Satz 8.29 *${}_U\!\sim$ und $\sim_U$ sind genau dann Äquivalenzrelationen, wenn U eine Untergruppe ist.*

Beweis: Der Beweis wird nur für ${}_U\!\sim$ gezeigt; für $\sim_U$ muss man die Seiten vertauschen. Wegen $g \ {}_U\!\sim\ g \iff e = g^{-1} \cdot g \in U$ ist die Relation genau dann reflexiv, wenn $e \in U$.

Weiterhin gilt $g \ {}_U\!\sim\ h \Leftrightarrow g^{-1} \cdot h \in U \Leftrightarrow h^{-1} \cdot g = (g^{-1} \cdot h)^{-1} \in U^{-1} \Leftrightarrow h \ {}_{U^{-1}}\!\sim\ g$. Umgekehrt hat man: $u \in U \Leftrightarrow e^{-1}u \in U \Leftrightarrow e \ {}_U\!\sim\ u$ und $u^{-1} \in U \Leftrightarrow u^{-1}e \in U \Leftrightarrow u \ {}_U\!\sim\ e$. Die Relation ist also genau dann symmetrisch, wenn $U = U^{-1}$.

Schließlich: Falls $g \ {}_U\!\sim\ h$ und $h \ {}_U\!\sim\ i$, so hat man $g^{-1}h \in U$ und $h^{-1}i \in U$, also $g^{-1}i = g^{-1}hh^{-1} \in U \cdot U$, d. h. $g \ {}_{UU}\!\sim\ i$. Umgekehrt: sind $g, h \in U$, so ist $g^{-1} \ {}_U\!\sim\ e$ und $e \ {}_U\!\sim\ h$, und außerdem gilt $gh \in U \Leftrightarrow g^{-1} \ {}_U\!\sim\ h$. Die Relation ist also genau dann transitiv, wenn $U = U \cdot U$. □

Nebenklassen

Definition 8.30 *Wenn $U \leqslant G$, so heißen die Äquivalenzklassen von ${}_U\!\sim$ Linksnebenklassen von U in G. Die Äquivalenzklasse von $g \in G$ ist dabei von der Form $gU := \{gu \mid u \in U\}$. Die Menge der Linksnebenklassen von U in G wird mit G/U bezeichnet*

Die Äquivalenzklassen von $\sim_U$ heißen Rechtsnebenklassen von U in G. Die Äquivalenzklasse von $g \in G$ ist dabei von der Form $Ug := \{ug \mid u \in U\}$. Die Menge der Rechtsnebenklassen von U in G wird mit $U\backslash G$ bezeichnet.

Es gilt also

$$gU = hU \iff g \ {}_U\!\sim\ h \iff g^{-1}h \in U \iff g^{-1}hU = U$$
$$Ug = Uh \iff g \sim_U h \iff hg^{-1} \in U \iff Uhg^{-1} = U$$

Für $u \in U$ stimmen Rechts- und Linksnebenklasse überein und es gilt $uU = Uu = U$. In kommutativen Gruppen sind generell Rechtsnebenklassen auch Linksnebenklassen und umgekehrt, d. h. es gilt $gU = Ug$ (und man sagt kurz „Nebenklasse“). Falls die Gruppe additiv geschrieben wird, ist die Nebenklasse $g+U = \{g+u \mid u \in U\}$. In nicht-kommutativen Gruppen sind Rechts- und Linksnebenklassen dagegen im Allgemeinen verschieden.

Satz 8.31 *Sei $U \leqslant G$.*

(a) *Alle Nebenklassen haben die gleiche Anzahl von Elementen wie U.*
(b) *Es gibt ebenso viele Rechts- wie Linksnebenklassen; ihre Anzahl ist der Index $[G : U]$ von U in G*

BEWEIS: (a) $U \to Ug, u \mapsto ug$ ist offenbar eine Bijektion mit, da $x \mapsto xg^{-1}$ die Umkehrabbildung ist. Ebenso ist $U \to gU, u \mapsto gu$ eine Bijektion.

(b) $G/U \to U\backslash G, gU \mapsto Ug^{-1}$ ist eine Bijektion: Es gilt

$$gU = hU \iff U = g^{-1}h \iff g^{-1}h \in U \iff Ug^{-1}h = U \iff Ug^{-1} = Uh^{-1}$$

also ist die Abbildung wohldefiniert und injektiv, und $Ug \mapsto g^{-1}U$ ist die ebenso wohldefinierte Umkehrabbildung. □

Folgerung 8.32 (Satz von Lagrange) *Wenn G endlich ist und $U \leqslant G$, dann gilt*

$$|G| = |U| \cdot [G : U]$$

Die Ordnung einer Untergruppe teilt also die Gruppenordnung; insbesondere teilt die Ordnung eines Gruppenelementes die Gruppenordnung.

Definition 8.33 *Eine Untergruppe U von G heißt normale Untergruppe oder Normalteiler, falls ${}_U\sim$ und $\sim_U$ die gleiche Relation sind, also falls Linksnebenklassen und Rechtsnebenklassen übereinstimmen. Man schreibt dafür $U \trianglelefteq G$.* Normale Untergruppe

- Kerne von Homomorphismen sind normale Untergruppen:
  Sei $\varphi : G \to H$ ein Homomorphimus; wir wollen zeigen, dass $g\text{Kern}(\varphi) = \text{Kern}(\varphi)g$. Äquivalent hat man zu zeigen, dass es für jedes $u \in \text{Kern}(\varphi)$ ein $u' \in \text{Kern}(\varphi)$ mit $gu = u'g$ gibt, d. h. dass $gug^{-1} = u'$ im Kern liegt. Es ist aber $\varphi(gug^{-1}) = \varphi(g)\varphi(u)\varphi(g^{-1}) = \varphi(g)e_H\varphi(g)^{-1} = e_H$.
- $\{e\}$ und G sind stets normale Untergruppen einer Gruppe G.
- In kommutativen Gruppen sind alle Untergruppen normal.
- Eine Untergruppe U vom Index 2 ist normal, denn da U ein Rechts- wie Linksnebenklasse ist, ist $G \setminus U$ die jeweils andere Nebenklasse, also auch eine Rechts- und Linksnebenklasse.
- Die von einer Transposition erzeugten Untergruppen der S_3 vom Index 3 sind die kleinsten Beispiele von nicht normalen Untergruppen.

Definition 8.34 *Eine Äquivalenzrelation $\sim$ auf einer Gruppe G heißt Kongruenzrelation, falls die Menge $G/_\sim$ der Äquivalenzklassen so zu einer Gruppe gemacht werden kann, dass die natürliche Abbildung $G \to G/_\sim, g \mapsto g/_\sim$ ein Homomorphismus ist.* Kongruenzrelation

Eine Äquivalenzrelation $\sim$ auf einer Gruppe G ist genau dann eine Kongruenzrelation, wenn die Festlegung

$$(g/_\sim) \cdot (h/_\sim) := (g \cdot h)/_\sim$$

wohldefiniert ist, wenn also die Äquivalenzklasse des Produktes unabhängig von der Wahl der Repräsentanten ist. Die Operation ist dann automatisch assoziativ, da sie durch die assoziative Gruppenoperation auf G definiert ist, $e/_\sim$ ist neutrales Element und $(g/_\sim)^{-1}$ inverses Element zu $g^{-1}/_\sim$.

Satz 8.35 *Die Kongruenzrelationen für Gruppen sind genau die Nebenklassenrelationen normaler Untergruppen.*

BEWEIS: $\sim$ ist genau dann eine Kongruenzrelation, wenn die natürliche Abbildung $G \to G/_\sim$ ein Homomorphismus ist; also ist sie nach den Überlegungen oben die Nebenklassenrelation des Kerns.

Sei umgekehrt N eine normale Untergruppe und $g_1N = g_2N, h_1N = h_2N$, also $g_2 = g_1n$ und $h_2 = h_1n'$ mit $n, n' \in N$. Wegen $h_1N = Nh_1$ ist $nh_2 = h_1n''$ für ein $n'' \in N$. Es folgt $g_2h_2 = g_1nh_1n' = g_1h_1n''n' \in g_1h_1N$ und somit $g_2h_2N = g_1h_1N$. □

Definition 8.36 *Ist N eine normale Untergruppe von G, so heißt die Gruppenstruktur auf der Menge G/N der Nebenklassen von N in G die Faktorgruppe oder Quotientengruppe von G nach N.*

Faktor- oder Quotientengruppe

Satz 8.37 (Homomorphiesatz für Gruppen) *Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so kann man φ zusammensetzen als Komposition der folgenden Homomorphismen:*

$$\begin{array}{ccccccc} & \text{surjektiv} & & \text{bijektiv} & & \text{injektiv} & \\ G & \longrightarrow & G/\mathrm{Kern}(\varphi) & \xrightarrow{\cong} & \mathrm{Bild}(\varphi) & \longrightarrow & H \\ g & \mapsto & g\mathrm{Kern}(\varphi) & \mapsto & \varphi(g) & \mapsto & \varphi(g) \end{array}$$

Beweis: Wie im kommutativen Fall. □

Untergruppen und homomorphe Bilder bieten die Möglichkeit, aus einer Gruppe „kleinere Teile“ zu gewinnen und u. U. die Struktur der Gruppe zu verstehen, indem man z. B. die Struktur eines Normalteilers und der zugehörigen Faktorgruppe analysiert.

- Das Signum $\mathrm{sgn} : S_n \to (\{\pm 1\}, \cdot) \cong \mathbb{Z}_2$ ist ein Homomorphismus, dessen Kern die Alternierende Gruppe A_n ist, die aus den Permutationen besteht, die sich als Komposition einer geraden Anzahl von Transpositionen schreiben lassen. Es gilt also $S_n/A_n \cong \mathbb{Z}_2$.

  Für $n = 3$ und $n \geqslant 5$ hat die S_n keine anderen normalen Untergruppen außer $\{e\}$, A_n und S_n. Damit hängt zusammen, dass es für Polynomgleichungen vom Grad mindestens 5 keine allgemeine Lösungsformel mit Wurzelausdrücken gibt.
- Die Drehgruppe D des Würfels permutiert die vier Raumdiagonalen des Würfels; dadurch erhält man einen Homomorphismus $D \to S_4$, von dem man sich überzeugen kann, dass er injektiv ist. Da beide Gruppen die gleiche Anzahl von Elementen haben, ist also $D \cong S_4$. Außerdem permutiert D die drei Mittelsenkrechten des Würfels; dadurch erhält man einen Homomorphismus $S_4 \cong D \to S_3$, der surjektiv ist und dessen Kern die sogenannte Klein'sche Vierergruppe[29] ist, die isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist.
- $\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$ ist ein surjektiver Gruppenhomomorphimus, dessen Kern die Gruppe $\mathrm{SL}(n, \mathbb{R})$ der Matrizen der Determinante 1 ist (die also den orientierungs- und volumenerhaltenden Abbildungen entsprechen).

9 Ringe

9.1 Homomorphismen, Unterringe und Ideale

Zur Erinnerung an Abschnitt 3.4:

Definition 9.1 *Ein Ring (genauer: ein* Ring mit Eins *oder* unitärer Ring*) ist eine Struktur $(R, +, \cdot, 0, 1)$, wobei $(R, +, 0)$ eine kommutative Gruppe und $(R, \cdot, 1)$ ein Monoid ist, und die Multiplikation distributiv über der Addition ist.*

Ring

R heißt kommutativer Ring, wenn $\cdot$ zusätzlich kommutativ ist.

R heißt Körper, wenn $(R \setminus \{0\}, \cdot, 1)$ eine kommutative Gruppe ist.

Das Einselement 1 ist im Ring eindeutig bestimmt.

Wichtige Beispiele:

- der Ring der ganzen Zahlen $\mathbb{Z}$
- die endlichen Ring $(\mathbb{Z}_m, +_m, \cdot_m, 0, 1)$ mit $x \cdot_m y :=$ „*Rest von xy bei Division durch m*“
- alle Körper, z. B. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$
- Polynomringe wie etwa $\mathbb{R}[X], \mathbb{F}_2[X]$, aber auch $\mathbb{Z}[X]$
- die Matrizenringe $\mathrm{Mat}_{n\times n}(\mathbb{R})$, $\mathrm{Mat}_{n\times n}(\mathbb{F}_2)$, aber auch $\mathrm{Mat}_{n\times n}(\mathbb{Z})$
  Diese Ringe sind für $n > 1$ nicht kommutativ!

Unterring

Definition 9.2 *Sei R ein Ring, dann ist $U \subseteq R$ ein Unterring, falls U eine Untergruppe bzgl. der Addition ist, die unter der Multiplikation abgeschlossen ist (d. h. für alle $u_1, u_2 \in U$ gilt $u_1 u_2 \in U$). Man schreibt $U \leqslant R$.*

U heißt unitärer Unterring, falls U zusätzlich die 1 enthält.

Ringhomomorphismus

Definition 9.3 *Eine Abbildung $\varphi : R \to S$ zwischen zwei Ringen heißt Ringhomomorphismus, falls $\varphi : (R, +) \to (S, +)$ ein Gruppenhomomorphismus ist, der mit der Multiplikation verträglich ist (d. h. für alle $r_1, r_2 \in R$ gilt $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$).*

φ heißt unitärer Ringhomomorphismus, falls zusätzlich $\varphi(1_R) = 1_S$ gilt.

φ heißt Ringisomorphismus, falls φ ein bijektiver Ringhomomorphismus ist, dessen Umkehrabbildung ebenfalls ein Ringhomomorphismus ist. Zwei Ringe R und S heißen isomorph zueinander, $R \cong S$, falls es einen Ringisomorphismus zwischen ihnen gibt.

Wie bei Gruppen und Vektorräumen sind bijektive Ringhomomorphismus automatisch Isomorphismen. Man kann zudem leicht zeigen, dass surjektive Ringhomomorphismen immer unitär sind. Also sind insbesondere Ringisomorphismen unitär!

Ist $\varphi : R \to S$ ein Ringhomomorphismus, dann gilt $\varphi(r) = \varphi(1 \cdot r) = \varphi(1) \cdot \varphi(r)$, d. h. $\varphi(1)$ ist neutrales Element der Multiplikation im Bild von φ. Falls φ surjektiv ist, folgt $\varphi(1) = 1_S$ aus der Eindeutigkeit des neutralen Elements in Monoiden.

Aber Achtung: Das neutrale Element ist nur als neutrales Element des gesamten Monoids eindeutig! Es kann durchaus andere Elemente geben, die für eine Teilmenge des Monoids ebenfalls neutral sind. Jeder nicht-unitäre Ringhomomorphismus liefert dafür ein Beispiel. Ein minimales Beispiel ist das Monoid $\{0, 1\} \subseteq \mathbb{N}$ bzgl. der Multiplikation: 0 ist neutrales Element für die Teilmenge $\{0\}$, aber 1 ist das einzige neutrale Element für $\{0, 1\}$.

In einer Gruppe folgt dagegen bereits aus einer einzigen Gleichung $g \circ h = g$, dass $h = g^{-1} \circ g = e$.

Satz 9.4 *Wenn $\varphi : R \to S$ ein (unitärer) Ringhomomorphismus ist, ist* Bild(φ) *ein (unitärer) Unterring von S.*

Beweis: Analog zum entsprechenden Ergebnis für Gruppen oder Vektorräume. □

Beispiele für Ringhomomorphismen:

- Die Abbildung $\mathbb{R} \to \mathbb{R}[X]$, die ein $r \in \mathbb{R}$ auf das konstante Polynom $r \cdot X^0$ abbildet.

- Für jedes $a \in \mathbb{R}$ der „Auswertungshomomorphismus“ $\mathbb{R}[X] \to \mathbb{R}$, der einem Polynom $P(X)$ den Wert $P(a)$ an der Stelle a zuweist.
- Die „Rest-Abbildung“ $\mathrm{mod}_m : \mathbb{Z} \to \mathbb{Z}_m$.

  Umgekehrt ist $\mathbb{Z}_m$ zwar eine Teilmenge von $\mathbb{Z}$, aber kein Unterring.
- Die Abbildung $\varphi : \mathbb{R} \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$, $r \mapsto \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$ ist ein nicht-unitärer Ringhomomorphismus, da $\varphi(1)$ nicht das neutrale Element I_2 im Matrizenring ist.

  Dagegen ist die Abbildung $\psi : \mathbb{R} \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$, $r \mapsto \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ ein unitärer Ringhomomorphismus!
- Sind R und S Ringe, dann ist das direkte Produkt $R \times S$ mit den komponentenweisen Operationen ein Ring. Durch $r \mapsto (r, 0)$ und $s \mapsto (0, s)$ sind injektive Ringhomomorphismen $R \to R \times S$ und $S \to R \times S$ gegeben, die R und S bijektiv auf die Unterringe $R \times \{0\}$ und $\{0\} \times S$ abbilden. Es sind dies aber keine unitären Homomorphismen bzw. Unterringe, da die 1 des Rings $R \times S$ das Element $(1, 1)$ ist.

Definition 9.5 Kern Ideal

(a) *Der Kern eines Ringhomomorphismus $\varphi : R \to S$ ist $\{r \in R \mid \varphi(r) = 0\}$, also der Kern von φ als Gruppenhomomorphismus.*

(b) *Ein* Ideal *von R ist eine additive Untergruppe I mit folgender zusätzlicher Eigenschaft: Für alle $r \in R$ und $i \in I$ gilt $r \cdot i \in I$ und $i \cdot r \in I$. Man schreibt dafür $I \trianglelefteq R$.*

Die Untergruppe $m\mathbb{Z}$ ist sogar ein Ideal von $\mathbb{Z}$ (da jedes Vielfache eines Vielfachen von m natürlich ein Vielfaches von m bleibt).

Allgemeiner: Für einen kommutativen Ring R und ein $a \in R$, ist $aR := \{ar \mid r \in R\}$ ein Ideal von R. (Solche Ideale heißen *Hauptideale*.)

Satz 9.6 **(a)** *Der Kern eines Ringhomomorphismus $\varphi : R \to S$ ist ein Ideal von R.*

(b) *Umgekehrt ist jedes Ideal der Kern eines Ringhomomorphismus.*
Konkreter: Für $I \trianglelefteq R$ wird die Quotientengruppe R/I durch $(r_1 + I) \cdot (r_2 + I) := r_1 r_2 + I$ zu einem Ring, dem Quotientenring „R nach I“, wodurch $R \to R/I, r \mapsto r+I$ zu einem surjektiven Ringhomomorphismus mit Kern I wird.

Beweis: (a) Wir wissen bereits, dass der Kern I eine Untergruppe ist. Für $r \in R$ und $i \in I$ gilt dann $\varphi(r \cdot i) = \varphi(r) \cdot \varphi(i) = \varphi(r) \cdot 0 = 0$, also $r \cdot i \in I$. Analog sieht man $i \cdot r \in I$.

(b) Wir wissen bereits, dass R/I eine Gruppe ist. Zu zeigen ist zunächst die Wohldefiniertheit der Multiplikation. Die Gültigkeit der Ringaxiome für R/I folgt dann wie bei den Gruppen daraus, dass sie auf den Repräsentanten gelten.

Sei also $r_1 + I = r_1' + I$ und $r_2 + I = r_2' + I$, d. h $r_j - r_j' = i_j \in I$ für $j = 1, 2$. Dann ist

$$r_1 r_2 - r_1' r_2' = r_1 r_2 - r_1 r_2' + r_1 r_2' - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' = r_1 i_2 - i_1 r_2' \in I$$

da I ein Ideal ist. Mithin gilt $r_1 r_2 + I = r_1' r_2' + I$. □

Satz 9.7 (Homomorphiesatz für Ringe) *Ist $\varphi : R \to S$ ein Ringhomomorphismus, so kann man φ zusammensetzen als Komposition der folgenden Homomorphismen:*

$$\begin{array}{ccccccc} & \text{surjektiv} & & & \text{bijektiv} & & \text{injektiv} \\ R & \longrightarrow & R/\mathrm{Kern}(\varphi) & \xrightarrow{\cong} & \mathrm{Bild}(\varphi) & \longrightarrow & S \\ r & \mapsto & r+\mathrm{Kern}(\varphi) & \mapsto & \varphi(r) & \mapsto & \varphi(r) \end{array}$$

Ist φ unitär, sind alle Zwischenschritte auch unitär.

Beweis: Durch den Gruppenfall ist schon alles klar außer der Verträglichkeit mit der Multiplikation und ggf. der 1, die aus Satz 9.6 folgen. □

Folgerung 9.8 *$\mathbb{Z}/m\mathbb{Z}$ ist ein Ring. Über die Rest-Abbildung „$\bmod m$“ ist er isomorph zu $\mathbb{Z}_m$.*

Der strukturiertere Zugang zu den Ringen $\mathbb{Z}_m$ ist allerdings umgekehrt: Man bekommt über die allgemeine Theorie, dass $\mathbb{Z}/m\mathbb{Z}$ ein Ring ist. Dann nimmt man das Repräsentantensystem $\mathbb{Z}_m = \{0, \ldots, m-1\}$ und überträgt die Addition und Multiplikation von $\mathbb{Z}/m\mathbb{Z}$ so auf $\mathbb{Z}_m$, dass $\mathbb{Z}_m \to \mathbb{Z}/m\mathbb{Z}$, $z \mapsto z + m\mathbb{Z}$ ein Ringisomorphismus ist. Dann analysiert man, dass dies gerade die Operationen $+_m$ und $\cdot_m$ sind.

Bei der Vorgehensweise, mit $\mathbb{Z}_m$ zu beginnen, hat man zwar zunächst eine zugänglichere Struktur, aber wesentlich mehr Mühe zu zeigen, dass zum einen ein Ring vorliegt und dass zum anderen die „modulo m“-Abbildung ein Homomorphismus ist (was beides hier im Skript nicht getan wird.)

Im Ring $\mathbb{R}[X]$ gibt es das von dem Polynom X^2+1 Hauptideal, also das Ideal $I = (X^2+1)\cdot\mathbb{R}[X]$ aller Polynome, die von X^2+1 geteilt werden. Man erhält also den Quotientenring $\mathbb{R}[X]/I$.

Man kann nun zeigen, dass (a) die Kompositionsabbildung $\mathbb{R} \to \mathbb{R}[X] \to \mathbb{R}[X]/I$ injektiv ist und (b) der Ring $\mathbb{R}[X]/I$ sogar ein Körper ist (weil das Polynom X^2+1 in $\mathbb{R}[X]$ irreduzibel ist).

In diesem Körper hat die Gleichung $x^2 = -1$ eine Lösung, nämlich in dem Element $X+I$ (also der Nebenklasse des Polynoms $X \in \mathbb{R}[X]$). Denn es gilt:

$$(X+I)^2 + (1+I) = (X^2+1) + I = I = 0 + I$$

da $X^2+1 \in I$. Tatsächlich ist $\mathbb{R}[X]/I$ isomorph zu $\mathbb{C}$ und eine Möglichkeit, den Körper der komplexen Zahlen algebraisch zu konstruieren.

Für jeden Körper K und jedes irreduzible Polynom $P(X) \in K[X]$ erhält man aus diese Weise einen Erweiterungskörper von K, in dem P eine Nullstelle hat. Dadurch kann man die endlichen Körper konstruieren, die nicht von der Form $\mathbb{F}_p$ für eine Primzahl p sind. So ist zum Beispiel $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2+X+1)\cdot\mathbb{F}_2[X]$.

Definition 9.9 *Sei R kommutativer Ring mit Eins.*

Teiler
Einheiten
Nullteiler

- *Für $a, b \in R$ sagt man a teilt b (oder a* ist ein Teiler von *b oder b* ist Vielfaches von *a), wenn ein $c \in R$ existiert mit $a \cdot c = b$. Man schreibt $a \mid b$.*
- *Eine Einheit in R ist ein Element $r \in R$, das ein multiplikatives Inverses besitzt, d.h. ein Element r^{-1} mit $r \cdot r^{-1} = 1$. Die Menge der Einheiten von R wird mit R^* bezeichnet. Nach Lemma 3.4 ist $(R^*, \cdot, 1)$ eine Gruppe, die Einheitengruppe von R.*

- *Ein Nullteiler in R ist ein Element $a \in R \setminus \{0\}$, so dass ein $b \in R \setminus \{0\}$ existiert mit $a \cdot b = 0$.*

Die Einheiten sind also genau die Teiler des Einselements 1. Umgekehrt teilt 1 (und jede Einheit) jedes andere Element, da $r \cdot 1 = r$.

Jedes Ringelement ist ein Teiler der Null, da $r \cdot 0 = 0$. Nullteiler sind daher nur die Elemente, die die Null „nicht trivial“ teilen. Umgekehrt ist 0 das einzige Element, das von 0 geteilt wird.

Beispiele für Teiler:

- In $\mathbb{Z}$ gilt $2 \mid 6$, aber auch $-2 \mid 6$ und $2 \mid -6$ und $-2 \mid -6$.
  Allgemein gilt: sind r, s Einheiten und gilt $a \mid b$, dann gilt auch $ra \mid sb$
  (denn im kommutativen Ring R folgt aus $ac = b$ dann $(ra)(cr^{-1}s^{-1}) = sb$).
- In $\mathbb{Z}/12\mathbb{Z}$ ist $\overline{3} \cdot \overline{9} = \overline{27} = \overline{3}$, also ist $\overline{9}$ ein Teiler von $\overline{3}$.
- In $\mathbb{R}[X]$ ist zum Beispiel $X - 1$ ein Teiler von $X^2 - 1 = (X + 1)(X - 1)$.
  Es gilt auch $(-5X + 5) \mid X^2 - 1 = -\frac{1}{5}(X + 1)(-5X + 5)$.

Beispiele für Einheiten:

- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{Z}/12\mathbb{Z}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, denn es ist $\overline{5} \cdot \overline{5} = \overline{7} \cdot \overline{7} = \overline{11} \cdot \overline{11} = \overline{1}$, dagegen ist jedes Vielfache einer durch 2 oder 3 teilbaren Zahl wieder durch 2 oder 3 teilbar, also (auch in $\mathbb{Z}/12\mathbb{Z}$) niemals $= \overline{1}$.
- $\mathbb{R}[X]^* =$ die konstanten Polynome ungleich 0, also $\mathbb{R} \setminus \{0\}$

Beispiele für Einheitengruppen:

- $(\mathbb{Z}^*, \cdot) = (\{\pm 1\}, \cdot) \cong \mathbb{Z}_2$
- $(\mathbb{R}[X], \cdot) = (\mathbb{R} \setminus \{0\}, 0)$
- $((\mathbb{Z}/12\mathbb{Z})^*, \cdot) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Beispiele für Nullteiler:

- In $\mathbb{Z}/12\mathbb{Z}$ ist zum Beispiel $\overline{3}$ ein Nullteiler, denn $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$, aber $\overline{3} \neq \overline{0} \neq \overline{4}$.
- $\mathbb{Z}$ und $\mathbb{R}[X]$ haben keine Nullteiler!

9.2 Die endlichen Ringe $\mathbb{Z}/m\mathbb{Z}$

Zunächst als Vorbereitung ein Ergebnis über die ganzen Zahlen:

Satz 9.10 *Für alle $a, b \in \mathbb{Z}$ gibt es $k, l \in \mathbb{Z}$ mit $k \cdot a + l \cdot b = \mathrm{ggT}(a, b)$.*

Beweis: Dies folgt wie im nächsten Beispiel aus dem Euklidischen Algorithmus. [30] □

Gegeben seien etwa $a = 33$ und $b = 24$. Der Euklidische Algorithmus führt zunächst die Rechnungen in der linken Spalte aus; durch das sogenannte „Rückwärtseinsetzen“ erhält man dann in der rechten Spalte von unten nach oben die gewünschte $\mathbb{Z}$-Linearkombination.

Euklidischer Algorithmus:	daraus folgt:	Berechnung der Lineardarstellung:
	$? = \mathrm{ggT}(33, 24)$	
$33 = 1 \cdot 24 + 9$	$= \mathrm{ggT}(24, 9)$	$= (-1) \cdot 24 + 3 \cdot (33 - 24) = \boxed{3 \cdot 33 - 4 \cdot 24}$
$24 = 2 \cdot 9 + 6$	$= \mathrm{ggT}(9, 6)$	$= 9 - (24 - 2 \cdot 9) = (-1) \cdot 24 + 3 \cdot 9$
$9 = 1 \cdot 6 + 3$	$= \mathrm{ggT}(6, 3)$	$\boxed{3} = 9 - 1 \cdot 6$
$6 = 2 \cdot 3 + 0$	$= \mathrm{ggT}(3, 0) = 3$	$\uparrow$ *Rückwärtseinsetzen*

Satz 9.11 *n Sei $0 \neq a \in \mathbb{Z}_m$. Dann sind äquivalent:*

(1) *$a \in \mathbb{Z}_m^*$, d. h. a ist eine Einheit*
(2) *a ist kein Nullteiler*
(3) *$\mu_a : \mathbb{Z}_m \to \mathbb{Z}_m$, $z \mapsto az$, d. h. die Multiplikation mit a, ist eine bijektive Abbildung*
(4) *$\mathrm{ggT}(a, m) = 1$, d. h. a und m sind teilerfremd*

Die Äquivalenz der ersten drei Aussagen gilt in jedem *endlichen* komutativen Ring; die Äquivalenzen „μ_a injektiv $\iff$ a Einheit“ und „μ_a surjektiv $\iff$ a kein Nullteiler“ aus dem Beweis gelten sogar in jedem beliebigen kommutativen Ring.

Beweis: Das Distributivgesetz besagt gerade, dass μ_a ein Gruppenhomomorphismus der additiven Gruppen $(\mathbb{Z}_m, +_m)$ ist. Da $\mathbb{Z}_m$ endlich ist, ist μ_a genau dann bijektiv, wenn injektiv oder surjektiv.

Injektiv ist μ_a genau dann, wenn $\mathrm{Kern}(\mu_a) = \{0\}$, also genau dann, wenn aus $\mu_a(z) = az = 0$ folgt, dass $z = 0$, also genau dann, wenn a kein Nullteiler ist.

Wenn μ_a surjektiv ist, ist inbesondere $1 \in \mathrm{Bild}(\mu_A)$. Dann gibt es also ein $b \in R$ mit $a \cdot b = 1$, d. h. a ist Einheit. Ist umgekehrt a Einheit, dann liegt jedes Ringelement $z = a \cdot (a^{-1} \cdot z)$ im Bild von μ_a, d. h. μ_a ist surjektiv.

Sind a und m teilerfremd, so findet man ganze Zahlen $k, l \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(a, m) = ka + lm$. Es ist dann $k + m\mathbb{Z}$ ein Inverses von $a + m\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Ist $1 \neq \mathrm{ggT}(a, m)$, dann ist $a \cdot \frac{m}{\mathrm{ggT}(a,m)} = 0$ und $m \nmid \frac{m}{\mathrm{ggT}(a,m)}$, also ist a ein Nullteilter in $\mathbb{Z}_m$. □

Folgerung 9.12 *$\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn eine m Primzahl ist.*

Beweis: Genau dann, wenn m eine Primzahl ist, sind alle Zahlen in $\{1, \ldots, m-1\}$ teilerfremd zu m, also invertierbar in $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$. □

[30] ebenfalls nach Euklid von Alexandria

Aus Satz 9.11 ergibt sich ein **Verfahren zur Berechnung der Inverse** a^{-1} von $a \in \mathbb{Z}_m^*$:

Man bestimmt mit dem Euklidischen Algorithmus Zahlen $k, l \in \mathbb{Z}$ mit $1 = \text{ggT}(a, m) = ka + lm$. Dann gilt $k + m\mathbb{Z} = (a + \mathbb{Z})^{-1}$, d. h. für den Rest r von k modulo m ist $r = a^{-1}$ in $\mathbb{Z}_m$.

Im Beispiel $m = 12$ und $a = 7$ liefert der Euklidische Algorithmus zunächst

$$12 = 1 \cdot 7 + 5,\ 7 = 1 \cdot 5 + 2,\ 5 = 2 \cdot 2 + 1,\ 2 = 2 \cdot 1 + 0$$

Rückwärtseinsetzen ergibt

$$1 = 5 - 2 \cdot 2 = (-2) \cdot 7 + 3 \cdot 5 = 3 \cdot 12 - 5 \cdot 7$$

Also ist $(-5) + 12\mathbb{Z} = (7 + 12\mathbb{Z})^{-1}$ bzw. $7 = 7^{-1}$ in $\mathbb{Z}_{12}$, da $-5 = (-1) \cdot 12 + 7$ bei der Division durch 12 den Rest 7 lässt. Die Probe ergibt: $7 \cdot 7 = 49 = 4 \cdot 12 + 1 \equiv 1 \bmod 12$.

Satz 9.13 (Chinesischer Restsatz) *Seien $m_1, \ldots, m_k$ paarweise teilerfremde Zahlen.*

$$\begin{aligned} \chi : \mathbb{Z}/(m_1 \cdot \ldots \cdot m_k)\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ a + (m_1 \cdot \ldots \cdot m_k)\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_k\mathbb{Z}) \end{aligned}$$

ist dann ein Ringisomorphismus. Daraus folgt insbesondere die Isomorphie der Gruppen

$$(\mathbb{Z}/(m_1 \cdot \ldots \cdot m_k)\mathbb{Z})^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^*$$

Die Zahlen $2, 3, 4$ sind ein Beispiel *teilerfremder* Zahlen, die nicht *paarweise teilerfremd* sind: Es ist also $\text{ggT}(2, 3, 4) = 1$ (und auch $\text{ggT}(2, 3) = \text{ggT}(3, 4) = 1$), aber $\text{ggT}(2, 4) \neq 1$.

$2, 3, 5$ dagegen sind paarweise teilerfremd.

Beweis: Sei $m := m_1 \cdot \ldots \cdot m_k$. Da $m_i \mid m$, gibt es den Gruppenhomomorphismus $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$, $a + m\mathbb{Z} \mapsto a + m_i\mathbb{Z}$ aus dem Beispiel auf Seite 80, der aber auch ein Ringhomomorphismus ist, da die Multiplikation der Repräsentanten auf beiden Seiten die in $\mathbb{Z}$ ist. Aufgrund der komponentenweisen Definition der Operationen im direkten Produkt kann man diese Homomorphismen zu dem Homomorphismus χ aus dem Satz zusammensetzen.

Da $|\mathbb{Z}/m\mathbb{Z}| = m = m_1 \cdot \ldots \cdot m_k = |\mathbb{Z}/m_1\mathbb{Z}| \cdot \ldots \cdot |\mathbb{Z}/m_k\mathbb{Z}| = |\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}|$ reicht es zu zeigen, dass χ injektiv ist.

Sei also $a + m\mathbb{Z} \in \text{Kern}(\chi)$, d. h. $a + m_i\mathbb{Z} = 0 + m_i\mathbb{Z}$ bzw. $m_i \mid a$ für alle i. Somit ist $\text{kgV}(m_1, \ldots, m_k) \mid a$, und da die m_i paarweise teilerfremd sind, ist $\text{kgV}(m_1, \ldots, m_k) = m$. Es ist also $m \mid a$ bzw. $a + m\mathbb{Z} = 0 + m\mathbb{Z}$, d. h. χ ist injektiv und damit bijektiv, also ein Isomorphismus. □

Unter dem Namen „Chinesischer Restsatz“ ist vor allem auch die folgende Art und Weise bekannt, die Surjektivität von χ auszudrücken:

Folgerung 9.14 *Für paarweise teilerfremde ganze Zahlen $m_1, \ldots, m_k$ und vorgegebene Reste*

$r_1, \ldots, r_n$ existiert stets ein $a \in \mathbb{Z}$ mit

$$\begin{aligned} a &\equiv r_1 \bmod m_1 \\ &\vdots \qquad\quad \vdots \\ a &\equiv r_k \bmod m_k \end{aligned}$$

Falls $a \in \mathbb{Z}$ eine Lösung dieses Kongruenzensystems ist, ist die Menge sämtlicher Lösungen gerade die Nebenklasse $a + m_1 \cdot \ldots \cdot m_k\mathbb{Z}$.

Verfahren zum Finden einer Lösung:

- Im Fall $k = 2$ sucht man $a_1, a_2 \in \mathbb{Z}$ mit $a_1 m_1 + a_2 m_2 = 1$.
  Dann ist $a = r_2 a_1 m_1 + r_1 a_2 m_2$ eine Lösung des Kongruenzensystems.
- Für $k > 2$ konstruiert man eine Lösung per Induktion. Sei b_{nk1} mit

  $$\begin{aligned} b_{k-1} &\equiv r_1 \quad\quad \bmod m_1 \\ &\vdots \qquad\quad \vdots \\ b_{k-1} &\equiv r_{k-1} \quad \bmod m_{k-1} \end{aligned}$$

  bereits konstruiert. Mit dem Fall $k = 2$ sucht man a mit

  $$\begin{aligned} a &\equiv b_{k-1} \quad \bmod m_1 \cdot \ldots \cdot m_{k-1} \\ a &\equiv r_k \quad\quad \bmod m_k \end{aligned}$$

  Dieses a ist dann eine Lösung des Kongruenzensystems.

Beweis für die Gültigkeit des Verfahrens:
Im Fall $k = 2$ gilt, modulo m_1 gerechnet

$$a = r_2 a_1 m_1 + r_1 a_2 m_2 \equiv r_1 a_2 m_2 = r_1(1 - a_1 m_1) = r_1 - r_1 a_1 m_1 \equiv r_1 \mod m_1$$

und entsprechend durch symmetrische Rechnung $a \equiv r_2 \bmod m_2$.
Im Fall $k > 2$ hat man $a \equiv b_{k-1} \bmod m_1 \ldots m_{k-1}$, also erst recht $a \equiv b_{k-1} \bmod m_i$. Es folgt $a \equiv b_{k-1} \equiv r_i \bmod m_i$ für $i < k$. Nach Konstruktion gilt bereits $a \equiv r_k \bmod m_k$.

Wir betrachten das Kongruenzensystem

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 3 \bmod 5 \end{aligned}$$

Der Euklidische Algorithmus liefert $5 = 3 + 2, 3 = 2 + 1$, rückwärts eingesetzt also $1 = 3 - 2 = (-1) \cdot 5 + 2 \cdot 3$. Eine Lösung ist also

$$a = 1 \cdot (-1) \cdot 5 + 3 \cdot 2 \cdot 3 = 13$$

(Probe: $13 = 4 \cdot 3 + 1 = 2 \cdot 5 + 3$) und alle Lösungen sind

$$13 + 15\mathbb{Z}$$

($15 = \mathrm{kgV}(3,5)$ hat modulo 3 und modulo 5 den Rest 0; die Addition eines Vielfachen von 15 ändert daher bei beiden Kongruenzgleichungen nicht den Rest).

Inversenberechnung mittels des Chinesischen Restsatzes:

Möchte man a^{-1} in $\mathbb{Z}_m$ berechnen, kann man versuchen, m in ein Produkt paarweise teilerfremder Zahlen $m_1, \ldots, m_k$ zu zerlegen. Kennt man die Primfaktorzerlegung $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ (mit paarweise verschiedenen Primzahlen p_i), ist $m_i := p_i^{\alpha_i}$ solch eine Zerlegung.

Nun berechnet man $b_i + m_i\mathbb{Z} = (a + m_i\mathbb{Z})^{-1}$ in $\mathbb{Z}/m_i\mathbb{Z}$ für $i = 1, \ldots, k$ nach dem oben angegebene Verfahren mit Hilfe des Euklidischen Algorithmus. Dann erhält man $(a + m\mathbb{Z})^{-1}$ als das Urbild von $(b_1 + m_1\mathbb{Z}, \ldots, b_k + m_k\mathbb{Z})$ unter dem Homomorphismus χ aus dem Chinesischen Restsatz, wie gerade eben beschrieben.

Dieses Verfahren kann schneller sein als die direkte Berechnung mit dem Euklidischen Algorithmus. Insbesondere gilt dies, wenn mehrere multiplikative Inverse im gleichen Ring $\mathbb{Z}_m$ bestimmt werden müssen, da man die $\mathbb{Z}$-Linearfaktoren, die man für χ^{-1} braucht, nur einmal berechnet werden müssen.

Man möchte 7^{-1} in $\mathbb{Z}_{15} \xrightarrow[\chi]{\cong} \mathbb{Z}_3 \times \mathbb{Z}_5$ berechnen. Man sieht zunächst, dass $\chi(7) = (1, 2)$.

Nun ist $1^{-1} = 1$ in $\mathbb{Z}_3$ und $2^{-1} = 3$ in $\mathbb{Z}_5$ (das sieht man hier ohne große Berechnung). Also ist $7^{-1} = \chi^{-1}(1, 3)$ in $\mathbb{Z}_{15}$. Im Beispiel zum Chinesischen Restsatz wurde gerade ausgerechnet, dass $\chi^{-1}(1, 3) = 13$.

Definition 9.15 $\varphi(m) := |(\mathbb{Z}/m\mathbb{Z})^*|$ *ist die Anzahl der Zahlen in* $\{1, \ldots, m-1\}$*, die zu* m *teilerfremd sind. Die Funktion* φ *heißt die Euler'sche* φ*-Funktion.*[31]

Euler'sche φ-Funktion

Für eine Primzahl p ist offensichtlich $\varphi(p) = p - 1$ (und eine Zahl $m > 1$ ist genau dann eine Primzahl, wenn $\varphi(m) = m - 1$).

Für die Berechnung von $\varphi(p^\alpha)$ bemerkt man, dass genau die Vielfachen von p, also $p, 2p, 3p, \ldots$ nicht teilerfremd zu p sind. Bis $p^\alpha = p^{\alpha-1} \cdot p$ sind dies genau $p^{\alpha-1}$ viele Zahlen. Also ist

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Satz 9.16 (Berechnung der Euler'schen φ−Funktion) *Sei* $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ *die Primfaktorzerlegung von* m*. Dann gilt*

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_k - 1)$$

Beweis: Die Zahlen $p_1^{\alpha_1}, \ldots, p_n^{\alpha_k}$ sind paarweise teilerfremd (da die p_i paarweise verschiedene Primzahlen sind), somit hat man nach dem Chinesischen Restsatz

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (Z/p_k^{\alpha_k}\mathbb{Z})^*$$

[31] nach Leonhard Euler (1707–1783)

Also ist $\varphi(m) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$. Zusammen mit der Berechnung von $\varphi(p^\alpha)$ aus dem vorherigen Beispiel ergibt sich daraus das Ergebnis! □

- $600 = 2^3 \cdot 3 \cdot 5^2$, also ist $\varphi(600) = (2-1) \cdot 2^2 \cdot (3-1) \cdot 3^0 \cdot (5-1) \cdot 5^1 = 4 \cdot 2 \cdot 4 \cdot 5 = 160$
- $\varphi(2^n) = 2^{n-1}$ (teilerfremd zu 2^n sind gerade die ungeraden Zahlen!)
- $\varphi(10^n) = 1 \cdot 2^{n-1} \cdot 4 \cdot 5^{n-1} = 4 \cdot 10^{n-1}$.
- $\varphi(8!) = \varphi(40\,320) = 9216$, dagegen ist $\varphi(40\,343) = 40\,342$, da es sich um eine Primzahl handelt. φ ist also eine in ihren Werten stark schwankende Funktion.

Erinnerung: Der Satz von Lagrange besagte für eine endliche Gruppe G, dass die Ordnung jedes Gruppenelements $g \in G$ ein Teiler von $|G|$ ist. Insbesondere folgt daraus $g^{|G|} = e$. Für $\mathbb{Z}_m^*$ ergibt sich daraus:

Satz 9.17 (Satz von Euler) *Für $a \in \mathbb{Z}_m^*$ gilt $a^{\varphi(m)} = 1$ (gerechnet in $\mathbb{Z}_m^*$).*
Das heißt, für alle zu m teilerfremden $a \in \mathbb{Z}$ ist $a^{\varphi(m)} \equiv 1 \bmod m$.

Im Spezialfall, dass $m = p$ eine Primzahl ist, lautete der Satz wie folgt:

Satz 9.18 (Kleiner Satz von Fermat [32]) *Ist p eine Primzahl, so gilt $a^{p-1} = 1$ für $a \in \mathbb{Z}_p^*$.*
Das heißt, für alle $a \in \mathbb{Z}$ mit $p \nmid a$ ist $a^{p-1} \equiv 1 \bmod p$. Es folgt $a^p \equiv a \bmod p$ für alle $a \in \mathbb{Z}$.

Beweis: Der Satz von Euler und damit der erste Teil des kleinen Satzes von Fermat ist nichts anderes als die Aussage $g^{|G|} = e$. Gilt $a^{p-1} \equiv 1 \bmod p$, folgt daraus $a^p = a^{p-1} \cdot a \equiv 1 \cdot a = a \bmod p$. Im Falle, dass $p \mid a$, ist $a^p \equiv a \equiv 0 \bmod p$. □

- Es ist $\varphi(10) = \varphi(2 \cdot 5) = 4$ (die vier zu 10 teilerfremden Zahlen sind $1, 3, 7, 9$). Es gilt also $3^4 \equiv 7^4 \equiv 9^4 \equiv 1 \bmod 10$, d. h. die letzte Ziffer von 3^4, 7^4 und 9^4 ist jeweils eine 1.

  Die Endziffern z. B. der Dreierpotenzen wiederholen sich daher in einem 4er-Rhythmus:

$$3^n \equiv \begin{cases} 1 & \text{falls } n \equiv 0 \bmod 4 \\ 3 & n \equiv 1 \bmod 4 \\ 9 & n \equiv 2 \bmod 4 \\ 7 & n \equiv 3 \bmod 4 \end{cases}$$

  Dagegen ist $2^4 = 16 \equiv 6 \bmod 10$; die Teilerfremdheit ist also eine notwendige Voraussetzung im Satz von Euler. Man sieht dann z. B. auch $6^4 = 2^4 \cdot 3^4 \equiv 2^4 \equiv 6 \bmod 10$.

- Achtung: $\varphi(m)$ ist nicht unbedingt die Ordnung von $a \in \mathbb{Z}_m^*$, also nicht unbedingt die kleinste Zahl $k > 0$ mit $a^k \equiv 1 \bmod m$. Zum Beispiel ist $\varphi(7) = 6$ und folgtlich $2^6 = 64 \equiv 1 \bmod 7$, aber es gilt bereits $2^3 = 8 \equiv 1 \bmod 7$. Der kleinste solche Exponent ist aber nach dem Satz von Lagrange ein Teiler von $\varphi(m)$.
- Der Satz von Euler bzw. der kleine Satz von Fermat kann eine Hilfe bei der schnellen Exponentiation modulo m sein; siehe Beispiel unten.

[32] Pierre de Fermat (1607–1665)

- Der kleine Satz von Fermat kann außerdem als Prinzahltest verwendet werden. Angenommen, man möchte herausfinden, ob m eine Primzahl ist. Falls man eine Zahl $1 < a < m$ finte mit $a^{m-1} \not\equiv 1 \bmod m$, kann m keine Primzahl sein. Zum Beispiel ist $2^5 = 32 \equiv 2 \bmod 6$, also ist 6 keine Primzahl.

  Es gibt unendlich viele sogenannte Carmichael-Zahlen [33], die diesen Test immer bestehen, aber keine Primzahlen sind (die kleinste ist 561). Daher kann man aus diesem Test keinen sicheres Verfahren ableiten. Außerdem kann man die Wahrscheinlichkeit nicht quantifizieren, dass eine zusammengesetzte Zahl den Test besteht. In der Praxis angewandte Primzahltests sind in der Regel probabilistische Tests, die mit einer vorgebbaren Wahrscheinlichkeit ein richtiges Ergebnis liefern (z. B. der Solovay-Strassen-Test [34]). Solche Test kombinieren in der Regel verschiedene algebraische Ergebnisse über Primzahlen; meist ist der kleine Satz von Fermat ein Baustein solcher Tests.

Schnelle Exponentiation modulo m

Möchte man $a^k \bmod m$ ausrechnen, sollte man außer bei ganz kleinen Zahlen keineswegs zunächst a^k ausrechnen, da diese Zahl in der Regel sowieso zu groß wird und außerdem der Rechenweg fehlerbehaftet ist.

Will man z. B. den Rest von $7^{1\,000\,000}$ modulo 13 bestimmen, sollte man nicht $7^{1\,000\,000}$ ausrechnen, denn dies ist eine Zahl mit etwa 850 000 Stellen (genau: $\lceil \log_{10} 7 \cdot 10^6 \rceil$).

Methode 1 (langsam): Man betrachtet die kleinste Potenz von a, die größer als m wird, und reduziert zunächst diese modulo m. Zum Ergebnis multipliziert man solange Faktoren a, bis man wieder größer als m ist, und reduziert wieder, etc. Im Beispiel:

$$\begin{aligned} 7^{1\,000\,000} &= 49 \cdot 7^{999\,998} \equiv 10 \cdot 7^{999\,998} \\ &= 70 \cdot 7^{999\,997} \equiv 5 \cdot 7^{999\,997} \\ &= \ldots \qquad\qquad \bmod 13 \end{aligned}$$

Mit dieser Methode muss man zwar nur kleine Zahlen verwalten, braucht aber viele Reduktionsschritte (etwa k viele).

Minimal günstiger wird die Berechnung, wenn man als Rest die betragsmäßig kleinste Zahl nimmt, also etwa

$$\begin{aligned} 7^{1\,000\,000} \equiv (-6)^{1\,000\,000} &\equiv 36 \cdot (-6)^{999\,998} \equiv (-3) \cdot (-6)^{999\,998} \\ &= 18 \cdot (-6)^{999\,997} \equiv 5 \cdot (-6)^{999\,997} \\ &= \ldots \qquad\qquad \bmod 13 \end{aligned}$$

[33] Robert Daniel Carmichael (1879–1967)
[34] Volker Strassen (∗ 1936), Robert Martin Solovay (∗ 1938)

Methode 2 (schnell): Man schreibt a^k anhand der Binärdarstellung von k als Produkt von Türmen von 2er-Potenzen, und reduziert dann sukzessive die auftretenden Quadrate.

Im Beispiel ist $1\,000\,000 = 11110100001001000000_{\text{binär}}$ und somit

$$\begin{aligned}
& & 7^{1\,000\,000} &= 7^{2^{19}} \cdot 7^{2^{18}} \cdot 7^{2^{17}} \cdot 7^{2^{16}} \cdot 7^{2^{14}} \cdot 7^{2^9} \cdot 7^{2^6} \\
(7^2 \equiv 10 \bmod 13) & & &\equiv 10^{2^{18}} \cdot 10^{2^{17}} \cdot 10^{2^{16}} \cdot 10^{2^{15}} \cdot 10^{2^{13}} \cdot 10^{2^8} \cdot 10^{2^5} \\
(10^2 \equiv 9 \bmod 13) & & &\equiv 9^{2^{17}} \cdot 9^{2^{16}} \cdot 9^{2^{15}} \cdot 9^{2^{14}} \cdot 9^{2^{12}} \cdot 9^{2^7} \cdot 9^{2^4} \\
(9^2 \equiv 3 \bmod 13) & & &\equiv 3^{2^{16}} \cdot 3^{2^{15}} \cdot 3^{2^{14}} \cdot 3^{2^{13}} \cdot 3^{2^{11}} \cdot 3^{2^6} \cdot 3^{2^3} \\
(3^2 \equiv 9 \bmod 13) & & &\equiv 9^{2^{15}} \cdot 9^{2^{14}} \cdot 9^{2^{13}} \cdot 9^{2^{12}} \cdot 9^{2^{10}} \cdot 9^{2^5} \cdot 9^{2^2} \\
(9^2 \equiv 3 \bmod 13) & & &\equiv 3^{2^{14}} \cdot 3^{2^{13}} \cdot 3^{2^{12}} \cdot 3^{2^{11}} \cdot 3^{2^9} \cdot 3^{2^4} \cdot 3^2 \\
(3^2 \equiv 9 \bmod 13) & & &\equiv 9^{2^{13}} \cdot 9^{2^{12}} \cdot 9^{2^{11}} \cdot 9^{2^{10}} \cdot 9^{2^8} \cdot 9^{2^3} \cdot 9 \\
(9^2 \equiv 9 \bmod 13) & & &\equiv 3^{2^{13}} \cdot 3^{2^{11}} \cdot 3^{2^{10}} \cdot 3^{2^9} \cdot 3^{2^7} \cdot 3^{2^2} \cdot 9 \\
& & &\vdots \qquad \vdots \\
& & &\equiv 3 \cdot 9 \cdot 3 \cdot 9 \cdot 9 \cdot 3 \cdot 9 \quad (\equiv 9) \qquad \bmod 13
\end{aligned}$$

Das übrig bleibende Produkt reduziert man z. B. nach Methode 1.

Bei dieser Methode hat man wenige (nämlich etwa $\log_2 k$ viele) Reduktionsschritte, um zu einer vergleichsweise kleinen Zahl zu kommen.

Man kann diese Methode sehr kompakt verwalten (sollte aber verstehen, was dabei passiert):

1	1	1	1	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0
3	9	3	9	3	9	3	9	3	9	3	9	3	9	3	9	3	9	10	7

In der oberen Zeile steht die Binärdarstellung $k_l \dots k_2 k_1 k_0$ des Exponenten $k = \sum_{i=1}^{l} k_i 2^i$ (die in Computeranwendungen im Hintergrund sowieso vorhanden ist, also nicht eigens ausgerechnet werden braucht). Die untere Zeile füllt man von rechts nach links: Unter k_0 steht die Basis $a = a_0$ der auszurechnenden Potenz, dann rechnet man induktiv a_{n+1} als „a_n^2 mod m“ aus. (Wenn sich wie im Beispiel eine Zahl wiederholt, muss man natürlich nicht mehr rechnen, sondern nur noch kopieren.) Anschließend nimmt man das Produkt der Zahlen a_i, die unter Ziffern $k_i = 1$ stehen (im Beispiel rot markiert). Von dieser vergleichsweise kleinen Zahl rechnet man weiter den Rest modulo m aus. Hat man wie im Beispiel viele gleiche Faktoren, kann man sogar wieder Methode 2 anwenden.

Methode 3: Falls man $\varphi(m)$ kennt und $\text{ggT}(a, m) = 1$ ist, kann man den Satz von Euler ausnutzen, um zunächst den Exponenten modulo $\varphi(m)$ zu reduzieren. Es ist dann

$$a^k \equiv a^{k \bmod \varphi(m)} \bmod m$$

Im Beispiel ist $\varphi(13) = 12$ und $1\,000\,000 = 83\,333 \cdot 12 + 4$, also

$$7^{1\,000\,000} = (7^{12})^{83\,333} \cdot 7^4 \equiv 1^{83\,333} \cdot 7^4 = 7^4 \ (= 2401 \equiv 9) \mod 13$$

Die Potenz 7^4 reduziert man nach Methode 1 oder 2.

RSA-Verschlüsselung

RSA ist ein kryptografisches Verfahren, das 1977 von Rivest, Shamir und Adleman entwickelt wurde. Es ist ein Beispiel einer *Public Key*-Verschlüsselung: Eine Nachricht soll zwischen von einer Person (dem „Sender“ **S**) einer anderen Person (dem „Empfänger“ **E**) in verschlüsselter Weise übermittelt werden, ohne dass ein Spion („Lauscher“), der sie auf dem Übertragungsweg abfängt bzw. mitliest, mit einem brauchbaren Zeitaufwand entschlüsselt werden kann. Sender und Empfänger haben dabei keine Möglichkeit, sich vorher unter geheimen Umständen über eine Verschlüsselungsart zu verständigen. Die Grundidee besteht nun darin, dass *der Empfänger* die Verschlüsselungsmethode zur Verfügung stellt: Er macht den Teil davon öffentlich (den „öffentlichen Schlüssel“), der zum Verschlüsseln dient, und behält einen anderen Teil davon für sich (den „privaten Schlüssel“), der zum Entschlüsseln nötig ist. Da das Entschlüsseln die Umkehrabbildung des Verschlüsselns darstellt, kann ein solches Verfahren nur funktionieren, wenn es Funktionen gibt, deren Anwendung einfach zu berechnen ist, deren Umkehrfunktion ohne Zusatzinformation aber rechnerisch viel aufwendiger ist. Ob es solche Funktionen (in einem präzisen komplexistätstheoretischen Sinn) tatsächlich gibt, ist ein offenes Problem der theoretischen Informatik. Es gibt schnell berechenbare Funktionen, für deren Umkehrprozess man bislang keine schnelle Verfahren kennt. Beim RSA-Verfahren besteht es im Multiplizieren von Primzahlen, was leicht zu berechnen ist, wogegen für die Umkehrung, das Faktorisieren von Zahlen, bisher kein schneller Algorithmus bekannt ist (außer für Quantencomputer), aber auch nicht bewiesen ist, dass es keinen solchen Algorithmus gibt.

Hier wird nun der mathematische Kern der RSA-Verschlüsselung dargestellt. Bei der konkreten Umsetzung sind noch viele Punkte zu beachten, auf die hier nicht eingegangen werden kann.

Das RSA-Verfahren:

1. **E** sucht zwei große, verschiedene und unbekannte Primzahlen p und q und rechnet $n = p \cdot q$ sowie $\varphi(n) = (p-1)(q-1)$ aus.

   (*Die Primzahlen werden in der Praxis durch probabilistische Verfahren gefunden und sind etwa 200-stellig.*)

2. **E** wählt ein zu $\varphi(n)$ teilerfremdes, „zufälliges“ e (das weder zu klein noch zu groß sein darf und insbesondere keine Rückschlüsse auf $\varphi(n)$ erlauben darf, also nicht etwa $\varphi(n)-1$ sein darf) und berechnet das multiplikative Inverses $d = e^{-1}$ in $\mathbb{Z}_{\varphi(n)}$.

3. **E** veröffentlicht n und e als öffentlichen Schlüssel und behält $\varphi(n)$ und d als privaten Schlüssel.

   (*Mit heutigen Verfahren sind p und q und damit $\varphi(n)$ nicht in vernünftiger Zeit aus n berechenbar.*)

4. **S** codiert die Nachricht in geeigneter Weise als ein Tupel $(a_1, \ldots, a_l) \in (\mathbb{Z}_n)^l$.

   (*Die Codierung darf zum Beispiel nicht Zeichen für Zeichen geschehen, indem man etwa den ASCII-Code nimmt, da sonst eine Häufigkeitsanalyse den Code knacken würde.*)

5. **S** rechnet nun komponentenweise $(a_1^e, \ldots, a_l^e)$ in $\mathbb{Z}_n$ aus (mit Hilfe der schnellen Exponentiation modulo n). Dies ist die verschlüsselte Nachricht, die **S** für alle offen lesbar an **E** schickt.

6. Zur Entschlüsselung berechnet **E** $((a_1^e)^d, \ldots, (a_l^e)^d)$ in $(\mathbb{Z}_n)^l$. Der folgende Satz zeigt, dass dies gerade die Originalnachricht $(a_1, \ldots, a_l)$ ist.

Satz 9.19 *Im RSA-Verfahren gilt* $(a^e)^d = a$ *für alle* $a \in \mathbb{Z}_n$.

Beweis: Da d ein Inverses zu e in $\mathbb{Z}_{\varphi(n)}$ ist, gilt $e \cdot d = k \cdot \varphi(n) + 1$ für eine Zahl $k \in \mathbb{Z}$.

1. Fall: $a = 0$. Dann ist $a^e = 0$ und $(a^e)^d = 0^d = 0 = a$.

2. Fall: $\mathrm{ggT}(a, n) = 1$. Dann gilt nach dem Satz von Euler

$$a^{e \cdot d} = a^{l \cdot \varphi(n)+1} = (a^{\varphi(n)})^l \cdot a = a \quad \text{in } \mathbb{Z}_n$$

3. Fall: a von genau einer der beiden Primzahlen p und q geteilt, etwa p. (Der Fall ist symmetrisch in p und q.) Also ist $a = m \cdot p$ mit teilerfremden m und q.

Offensichtlich ist p ein Teiler von $a^{e \cdot d}$, und somit teilt p auch $a^{e \cdot d} - a$. Andererseits ist $\varphi(q) = q - 1$ ein Teiler von $\varphi(n) = (p-1)(q-1)$. Damit sind e und d auch invers zueinander in $\mathbb{Z}_{\varphi(q)}$, denn es gilt $e \cdot d = k \cdot \varphi(n) + 1 = k \cdot (p-1) \cdot (q-1) + 1 = k \cdot (p-1) \cdot \varphi(q) + 1$.

Also ist, wieder nach dem Satz von Euler,

$$a^{e \cdot d} = (a^{\varphi(q)})^{k(p-1)} \cdot a \equiv a \mod q$$

d. h. q teilt ebenfalls $a^{e \cdot d} - a$. Da p und q als verschiedene Primzahlen teilerfremd sind, ist auch $n = p \cdot q = \mathrm{kgV}(p, q)$ ein Teiler von $a^{e \cdot d} - a$, d. h. $a^{e \cdot d} = a$ in $\mathbb{Z}_n$. □

Der Satz gilt allgemeiner für alle „quadratfreien“ Zahlen n, also Zahlen, bei denen in der Primfaktorzerlegung keine Primzahl mehrfach vorkommt.

Man kann das RSA-Verfahren auch zur „digitalen Signatur“ verwenden:

S wählt ebenfalls einen privaten Schlüssel $p', q', \varphi(n'), d'$ und einen öffentlichen Schlüssel $n' = p' \cdot q'$ und e'. Die eigentliche Nachricht $(a_1, \ldots, a_l)$ kann man auch als Tupel in $(\mathbb{Z}_{n'})^l$ auffassen, da n und n' beides sehr große Zahlen sind, also größer als alle vorkommenden a_i. Der Sender **S** berechnet $(a_1^{d'}, \ldots, a_l^{d'})$ und verschickt diese Nachricht. **E** kann sie als $(a_1, \ldots, a_l) = ((a_1^{d'})^{e'}, \ldots, (a_l^{d'})^{e'})$ entschlüsseln und sich dann sicher sein, dass die Nachricht tatsächlich von **S** stammt und nicht von einer andern Person, die vorgibt, **S** zu sein, da nur **S** d' kennt.

Natürlich kann man beides kombinieren: **S** verschickt in diesem Fall $(a_1^{d'})^e, \ldots, (a_l^{d'})^e)$, wobei die erste Exponentiation in $\mathbb{Z}_{n'}$ und die zweite in $\mathbb{Z}_n$ stattfindet. Dies ist dann eine verschlüsselte und signierte Nachricht.

Kapitel III: Höherdimensionale Analysis

In diesem Kapitel werden nur Ergebnisse präsentiert, aber nicht bewiesen!

10 Totale und partielle Differenzierbarkeit

Wir betrachten Vektoren im $\mathbb{R}^n$, die ich der besseren Übersichtlichkeit halber mit einem Oberstrich schreibe, also $\bar{a} = (a_1, \ldots, a_n) \in \mathbb{R}^n$. Hat der Vektor $\bar{a}_i$ bereits einen Index, heißen die Komponenten $a_{i1}, \ldots, a_{in}$. Der Einheitlichkeit wegen schreibe ich nun auch die Standardbasisvektoren als $\bar{e}_1, \ldots, \bar{e}_n$.

Sei $f : D \to \mathbb{R}^m$ eine Funktion mit einem Definitionsbereich $D \subseteq \mathbb{R}^n$ Die Funktion f bildet also einen Vektor $\bar{x} = (x_1 \ldots, x_n) \in D$ auf einen Vektor $f(\bar{x}) = (y_1, \ldots, y_m)$ ab. Um Probleme zu vermeiden, nehmen wir stets an, dass D eine *offene Menge* des $\mathbb{R}^n$ ist, d. h. zu jedem $\bar{x} \in D$ soll es ein (von $\bar{x}$ abhängiges) $\varepsilon > 0$ geben, so dass der *offene ε-Ball* $B_\varepsilon(\bar{x}) := \left\{\bar{x}' \in \mathbb{R}^n \;\middle|\; \|\bar{x}' - \bar{x}\| < \varepsilon\right\}$ ganz in D liegt. Man sagt dafür, dass *eine Umgebung von* $\bar{x}$ in D liegt. Der notationellen Einfachheit halber werde ich oft $D = \mathbb{R}^n$ annehmen; die Ergebnisse gelten aber in der Regel für ein beliebiges offenes D.

Von $\mathbb{R}^m$ nach $\mathbb{R}$ gibt es die *Projektionsabbildungen* $\pi_i : (y_1, \ldots, y_m) \mapsto y_i$. Die Verkettung

$$f_i := \pi_i \circ f : \mathbb{R}^n \to \mathbb{R}$$

heißt i-te Komponentenfunktion von f. Die Funktion f setzt sich aus ihren Komponentenfunktionen zusammen, da $f(\bar{x}) = \big(f_1(\bar{x}), \ldots\, f_m(\bar{x})\big)$. Viele Eigenschaften von f lassen sich auf die entsprechenden Eigenschaften der Komponentenfunktionen zurückführen; man kann also oft $m = 1$ annehmen.

Der Graph von f ist die Menge $\Gamma_f := \left\{(\bar{x}, f(\bar{x})) \;\middle|\; \bar{x} \in D\right\} \subseteq \mathbb{R}^{m+n}$. In den Fällen $n = 1$ und $m = 2$ bzw. $n = 2$ und $m = 1$ kann man sich den Graphen von f also als im dreidimensionalen Raum liegend vorstellen. Im ersten Fall sieht der Graph (im Falle einer stetigen Funktion) wie eine Linie aus, im zweiten Fall wie eine Fläche.

Konvergenz und Stetigkeit

Definition 10.1 *Sei $(\bar{a}_k)_{k\in\mathbb{N}}$ eine Folge im $\mathbb{R}^n$. Man sagt, dass die Folge gegen den Grenzwert $\bar{a} \in \mathbb{R}^n$ konvergiert, falls es zu jedem $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt mit $\|\bar{a}_k - \bar{a}\| < \varepsilon$ für alle $k \geqslant N$.* Konvergenz

Dafür schreibt man wie im Eindimensionalen $\lim\limits_{k\to\infty} \bar{a}_k = \bar{a}$ oder $(\bar{a}_k) \underset{k\to\infty}{\longrightarrow} \bar{a}$, oder Varianten davon. Es ist möglich, dass die Folgenglieder $\bar{a}_k$ auch nur für Indizes $k \geqslant k_0$ ab einem Startwert k_0 gegeben sind (häufig $k_0 = 1$).

Satz 10.2 *Der Konvergenzbegriff ist unabhängig von der Wahl der Norm im $\mathbb{R}^n$, d. h. eine Folge konvergiert bezüglich einer Norm genau dann, wenn sie bezüglich einer anderen Norm konvergiert.*

Man kann also für $\|(x_1, \ldots, x_n)\|$ einheitlich die Euklidische Norm $\sqrt{x_1^2 + \cdots + x_n^2}$ nehmen. (Erinnerung: Eine allgemeine Norm wurde am Rande auf Seite 51 definiert; als mögliche andere Normen wurden dort die 1-Norm und die Maximumsnorm beschrieben.)

In unendlich-dimensionalen $\mathbb{R}$-Vektorräumen stimmt dies nicht; hier gibt es verschiedene Konvergenzbegriffe.

Satz 10.3 *Eine Folge $(\bar{a}_k)_{k\in\mathbb{N}}$ im $\mathbb{R}^n$ konvergiert genau dann gegen $\bar{a}$, wenn alle* Komponentenfolgen *$(a_{ki})_{k\in\mathbb{N}}$ in $\mathbb{R}$ gegen a_i konvergieren, d. h. für alle $i = 1, \ldots, n$.*

Definition 10.4 *$f : \mathbb{R}^n \to \mathbb{R}^m$ heißt stetig in $\bar{a} \in \mathbb{R}^n$, falls für alle gegen $\bar{a}$ konvergenten Folgen $(\bar{a}_k) \underset{k\to\infty}{\longrightarrow} \bar{a}$ auch $f(\bar{a}_k) \underset{k\to\infty}{\longrightarrow} f(\bar{a})$ gilt, falls also die Funktionswerte in $\mathbb{R}^m$ ebenfalls konvergieren, und zwar gegen den Funktionswert des Grenzwertes.* stetig

Anders formuliert: $f(\lim\limits_{k\to\infty} \bar{a}_k) = \lim\limits_{k\to\infty} f(a_k)$ für jede gegen $\bar{a}$ konvergierende Folge.

f heißt stetig auf einer offenen Menge $U \subseteq \mathbb{R}^n$, falls f in jedem $\bar{a} \in U$ stetig ist.

Satz 10.5 *Eine Funktion $f : \mathbb{R}^n \to \mathbb{R}^m$ ist genau dann stetig in $\bar{a}$, wenn alle Komponentenfunktionen $f_1, \ldots, f_n : \mathbb{R}^n \to \mathbb{R}$ stetig in $\bar{a}$ sind.*

Beweis: Dies ergibt sich unmittelbar aus der Definition und Satz 10.3. □

Im Fall $n = 1$ ist die Stetigkeit einer Funktion $f : \mathbb{R} \to \mathbb{R}^m$ damit komplett auf die Stetigkeit eindimensionaler Funktionen zurückgeführt. Anschaulich ist eine Funktion $f : \mathbb{R} \to \mathbb{R}^m$ unstetig, wenn der Graph eine Sprungstelle hat.

Im Fall $n > 1$ gibt es bei unstetigen Funktionen zwar in gewissen Sinne auch Sprungstellen: Nimmt man eine Folge $(a_k)_{k\in\mathbb{N}}$, die die Unstetigkeit beweist, und „läuft entlang dieser Folge“ auf dem Graph von f, hat man im Grenzwert einen Sprung. Dies bedeutet aber anders als im Eindimensionalen nicht, dass der Graph in mehrere Stücke zerfallen muss.

Sei $f : \mathbb{R}^2 \to \mathbb{R}$ definiert durch

$$f(x_1, x_2) := \begin{cases} \dfrac{2x_1x_2}{x_1^2 + x_2^2} & \text{falls } (x_1, x_2) \neq (0, 0) \\ 0 & \text{falls } (x_1, x_2) = (0, 0) \end{cases}$$

Diese Funktion ist unstetig in $(0, 0)$, denn die gegen $(0, 0)$ konvergierende Folge $(\frac{1}{k}, \frac{1}{k})_{k\in\mathbb{N}}$ hat konstanten Wert $f(\frac{1}{k}, \frac{1}{k}) = 1$, aber $f(0, 0) \neq 1$.

Man kann dieses Beispiel auch so deformieren, dass die Folge in einem Bogen auf die Unstetigkeitsstelle zuläuft. Sei $g : \mathbb{R}^2 \to \mathbb{R}$ definiert durch

$$g(x_1, x_2) := \begin{cases} \dfrac{2x_1^3x_2}{x_1^6 + x_2^2} & \text{falls } (x_1, x_2) \neq (0, 0) \\ 0 & \text{falls } (x_1, x_2) = (0, 0) \end{cases}$$

Auch g ist unstetig in $(0, 0)$, denn die gegen $(0, 0)$ konvergierende Folge $(\frac{1}{\sqrt[3]{k}}, \frac{1}{k})_{k\in\mathbb{N}}$ hat konstanten Wert 1, aber $g(0, 0) \neq 1$.

Differenzierbarkeit

Erinnerung an den eindimensionalen Fall:

Eine Funktion $f : \mathbb{R} \to \mathbb{R}$ ist differenzierbar in a wenn der Grenzwert $f'(a) := \lim_{x \to a} \frac{f(x)-f(a)}{x-a}$ existiert. Anders ausgedrückt bedeutet dies, dass der Rest $R_0(x) := \frac{f(x)-f(a)}{x-a} - f'(a)$ für $x \to a$ gegen 0 konvergiert. Nach $f(x)$ aufgelöst bekommt man

$$\underbrace{f(x) \;=\; f'(a) \cdot (x-a) + f(a)}_{\text{Geradengleichung}} \;+\; \underbrace{R_0(x) \cdot (x-a)}_{=:\, R_1(x)}$$

Die Funktion $f(x)$ wird also angenähert durch die Gerade $y = f'(a) \cdot x$, die vom Punkte $(0, 0)$ an den Punkt $(a, f(a))$ verschoben wurde, und die Annäherung ist so gut, dass die Differenz $R_1(x)$ in der Nähe von a stark gegen 0 geht, d. h. so schnell, dass sogar $\lim_{x \to a} \frac{R_1(x)}{x-a} = 0$ gilt. Dies bedeutet, dass diese verschobene Gerade die Tangente am Graph von f im Punkte $(a, f(a))$ ist.

Üblicherweise wird in der Schule der Differentialquotient, also die Steigung der Tangente, als die Ableitung definiert und angesehen. Die Ableitung ist also eine Zahl. Mit Blick auf die höherdimensionale Verallgemeinerung ist es zielführender, die lineare Approximation des Graphen durch die Tangente als Ableitung aufzufassen. Erinnerung: Die Multiplikation mit der Zahl $f'(a)$ ist eine lineare Abbildung $A : x \mapsto f'(a) \cdot x$; die durch die Gleichung $y = f'(a) \cdot x$ beschriebene Gerade ist der Graph dieser Abbildung. Man definiert nun für höherdimensionale Funktionen:

Definition 10.6 *$f : \mathbb{R}^n \to \mathbb{R}^m$ heißt (total) differenzierbar in $\bar{a}$, falls es eine lineare Abbildung $A : \mathbb{R}^n \to \mathbb{R}^m$ gibt mit* total differenzierbar

$$f(\bar{x}) = A(\bar{x} - \bar{a}) + f(\bar{a}) + R_1(\bar{x}) \quad \textit{und} \quad \lim_{\bar{x} \to \bar{a}} \frac{R_1(\bar{x})}{\|\bar{x} - \bar{a}\|} = 0$$

Die Abbildung A heißt (totale) Ableitung von f in $\bar{a}$ und wird $f'(\bar{a})$ oder $Df(\bar{a})$ geschrieben.

f heißt (total) differenzierbar auf einer offenen Menge $U \subseteq \mathbb{R}^n$, falls f in jedem $\bar{a} \in U$ differenzierbar ist.

Im Fall $n = 1$ ist der Graph der Ableitung gerade die in den Ursprung verschobene Tangente an den Graphen von f im Punkt $(\bar{a}, f(\bar{a}))$, im Fall $n = 2$ die verschobene Tangentialebene und im allgemeinen Fall das *Tangential-Hyperebene* genannte n-dimensionale Analogon.

In der „Schulauffassung“ der Ableitung einer Funktion $\mathbb{R} \to \mathbb{R}$ ist die Ableitung einer Geraden $f(x) = px + q$ in jedem Punkt a die (konstante) Steigung $f'(a) = p$. Nun wird als Ableitung (in jedem Punkt a) die lineare Funktion $f'(a) : \mathbb{R} \to \mathbb{R}$ mit $f'(a)(x) = px$ aufgefasst (die die Multiplikation mit der Steigung ist).

Für eine überall differenzierbare Funktion $f : \mathbb{R} \to \mathbb{R}$ war nach der „Schulauffassung“ die Ableitung f' ebenfalls eine Funktion $\mathbb{R} \to \mathbb{R}$, also vom gleichen Typ. Nun ist die Ableitung eine Abbildung $f' : \mathbb{R} \to \mathrm{Lin}(\mathbb{R}, \mathbb{R})$. Die linearen Abbildungen $\mathbb{R} \to \mathbb{R}$ sind gerade die Multiplikationen mit reellen Zahlen, können also mit $\mathbb{R}$ identifiziert werden (als (1×1)-Matrizen). Bis auf diese Indentifizierung von $\mathrm{Lin}(\mathbb{R}, \mathbb{R})$ mit $\mathbb{R}$ ändert sich also an der traditionellen Ableitung nichts.

Im Höherdimensionalen funktioniert das nicht mehr: Für eine überall differenzierbare Funktion $f : \mathbb{R}^n \to \mathbb{R}^m$ ist die Ableitung eine Funktion $f' : \mathbb{R}^n \to \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)$, und für $n > 1$ ist die Dimension von $\mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)$ größer als m. Dann ist f' „von einem anderen Typ“ als f.

Satz 10.7 *$f : \mathbb{R}^n \to \mathbb{R}^m$ ist genau dann differenzierbar in $\bar{a}$, wenn alle Komponentenfunktionen $f_1, \ldots, f_n : \mathbb{R}^n \to \mathbb{R}$ differenzierbar in $\bar{a}$ sind.*

Beweis: Die Komponentenfunktionen der Ableitung $f'(\bar{a})$ sind die Ableitung der Komponentenfunktionen von f. Das Konvergenzverhalten des Restes überträge sich mit Satz 10.3 und den Abschätzungen $|x_i - y_i| \leqslant \|\bar{x} - \bar{y}\| \leqslant |x_1 - y_1|^2 + \cdots + |x_n - y_n|^2$. □

Definition 10.8 *Die $(m \times n)$-Matrix der linearen Abbildung $f'(\bar{a})$ bezüglich der Standardbasen heißt Jacobi-Matrix. Der (i,j)-Eintrag* Jacobi-Matrix

$$f_i'(\bar{a})(e_j) =: \frac{\partial f_i}{\partial x_j}(\bar{a}) \quad \text{oder} \quad \frac{\partial}{\partial x_j} f_i(\bar{a})$$

heißt j-te partielle Ableitung der Komponentenfunktion f_i in $\bar{a}$.

f heißt partiell differenzierbar in $\bar{a}$, wenn alle partiellen Ableitungen $\frac{\partial f_i}{\partial x_j}(\bar{a})$ in $\bar{a}$ existieren, und partiell differenzierbar auf einer offenen Menge $U \subseteq \mathbb{R}^n$, falls f in jedem $\bar{a} \in U$ partiell differenzierbar ist.

Die Jacobi-Matrix von f an der Stelle $\bar{a}$ hat also die Form

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\bar{a}) & \cdots & \frac{\partial f_1}{\partial x_n}(\bar{a}) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(\bar{a}) & \cdots & \frac{\partial f_m}{\partial x_n}(\bar{a}) \end{pmatrix}$$

Berechnung der partiellen Ableitungen:

Für $f : \mathbb{R}^n \to \mathbb{R}$ erhält man die j-te partielle Ableitung, indem man die Funktion f auf die durch $\bar{a}$ in Richtung des Standardbasisvektor $\bar{e}_j$ laufende Gerade einschränkt und im Punkt a_{0j} ableitet. Man betrachtet also die Funktion $\mathbb{R} \to \mathbb{R}$,

$$r \mapsto f(a_{01}, \ldots, a_{0j-1}, r, a_{0j+1}, \ldots, a_{0n})$$

und leitet in a_{0j} ab.

(Notationell ist es etwas einfacher, wenn man die verschobene Funktion $\mathbb{R} \to \mathbb{R}$, $r \mapsto f(\bar{a} + r \cdot \bar{e}_j)$ betrachtet und diese in $r = 0$ ableitet.)

Konkret bedeutet dies, dass man in f für die Variablen $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n$ die Werte $a_{01}, \ldots, a_{0j-1}, a_{0j+1}, \ldots, a_{0n}$ einsetzt und von der verbleibenden Funktion $\mathbb{R} \to \mathbb{R}$ in der Varibalen x_j die Ableitung in a_{0j} ausrechnet.

Für eine überall partiell differenzierbare Funktion f läuft es auf das gleiche hinaus, wenn man die Variablen $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n$ wie Konstanten behandelt, die Funktion nach x_j ableitet und dann den Wert $\bar{a}$ einsetzt.

$f : \mathbb{R}^2 \to \mathbb{R}$ sei gegeben durch $f(x_1, x_2) = 5x_1^3 x_2^2 - 3x_1 x_2$.

Die partiellen Ableitungen im Punkt $\bar{a} = (1, -2)$ errechnen sich dann als:

$$\frac{\partial f}{\partial x_1}(1,-2) = \underset{\text{im Punkt } a_1 = 1}{\text{Ableitung von } 5 \cdot x_1^3 \cdot (-2)^2 - 3 \cdot x_1 \cdot (-2)} = \underset{\text{im Punkt } a_1 = 1}{60x_1^2 + 6} = 66$$

$$\frac{\partial f}{\partial x_2}(1,-2) = \underset{\text{im Punkt } a_2 = -2}{\text{Ableitung von } 5 \cdot 1^3 \cdot x_2^2 - 3 \cdot 1 \cdot x_2} = \underset{\text{im Punkt } a_2 = -2}{10x_2 - 3} = -23$$

Alternativ – und meistens einfacher – berechnet man die „globalen“ partiellen Ableitungen, d. h. für einen beliebigen Punkt (x_1, x_2), und setzt dann den konkreten Punkt $(1, -2)$ ein:

$$\begin{array}{rcl@{\quad}rcl} \frac{\partial f}{\partial x_1}(x_1,x_2) & = & 15x_1^2x_2^2 - 3x_2 & \text{und einsetzen:} & \frac{\partial f}{\partial x_1}(1,-2) = & 15\cdot 1^2\cdot(-2)^2 - 3\cdot(-2) & = & 66 \\ \frac{\partial f}{\partial x_2}(x_1,x_2) & = & 10x_1^3x_2 - 3x_1 & & \frac{\partial f}{\partial x_2}(1,-2) = & 10\cdot 1^3\cdot(-2) - 3\cdot 1 & = & -23 \end{array}$$

Richtungsableitungen

Sei $f : \mathbb{R}^n \to \mathbb{R}^m$ differenzierbar in $\bar{a}$.

Definition 10.9 *Für $\bar{v} \in \mathbb{R}^n$ mit $\|\bar{v}\| = 1$ heißt* Richtungsableitung

$$D_v f(\bar{a}) := f'(\bar{a})(\bar{v})$$

die Richtungsableitung von f in $\bar{a}$ in Richtung $\bar{v}$.

Die Richtungsableitung ist gerade $g'(0)$ für die Abbildung $g : \mathbb{R} \to \mathbb{R}$, $r \mapsto f(\bar{a} + r \cdot \bar{v})$ und gibt im Fall $m = 1$ die Steigung der Tangentialhyperebene am Graph von f im Punkt $(\bar{a}, f(\bar{a}))$ in Richtung $\bar{v}$ an. Im Fall $\bar{v} = \bar{e}_j$ erhält man die j-ten partiellen Ableitungen

$$D_{e_j} f(\bar{a}) = \begin{pmatrix} \frac{\partial f_1}{\partial x_j}(\bar{a}) \\ \vdots \\ \frac{\partial f_m}{\partial x_j}(\bar{a}) \end{pmatrix}$$

Die Richtungsableitung von $f(x_1, x_2) = 5x_1^3x_2^2 - 3x_1x_2$ in $\bar{a} = (1, -2)$ in Richtung $\begin{pmatrix} -\frac{3}{5} \\ \frac{4}{5} \end{pmatrix}$ ist

$$\left(\frac{\partial f}{\partial x_1}(1,-2), \frac{\partial f}{\partial x_2}(1,-2)\right) \cdot \begin{pmatrix} -\frac{3}{5} \\ \frac{4}{5} \end{pmatrix} = (66, -23) \cdot \begin{pmatrix} -\frac{3}{5} \\ \frac{4}{5} \end{pmatrix} = -\frac{288}{5}$$

Definition 10.10 *Im Fall $m = 1$ heißt die Jacobi-Matrix von f in $\bar{a}$, aufgefasst als Vektor im $\mathbb{R}^n$, auch Gradient von f in $\bar{a}$* Gradient

$$\operatorname{grad} f(\bar{a}) := \left(\frac{\partial f}{\partial x_1}(\bar{a}), \ldots, \frac{\partial f}{\partial x_n}(\bar{a})\right)$$

Für $\|v\| = 1$ ist

$$D_{\bar{v}} f(\bar{a}) = f'(\bar{a})(\bar{v}) = \operatorname{grad} f(\bar{a}) \cdot \bar{v} = \langle \operatorname{grad} f(\bar{a}), \bar{v} \rangle = \|\operatorname{grad} f(\bar{a})\| \cdot \|\bar{v}\| \cdot \cos \measuredangle(\operatorname{grad} f(\bar{a}), \bar{v})$$

Man sieht, dass $D_{\bar{v}} f(\bar{a})$ gerade für den Fall maximal wird, dass $\bar{v}$ in die gleiche Richtung wie $\operatorname{grad} f(\bar{a})$ zeigt (vorausgesetzt der Gradient ist nicht null). Also zeigt $\operatorname{grad} f(\bar{a})$ in die Richtung maximaler Steigung!

Definition 10.11 *$f : \mathbb{R}^n \to \mathbb{R}^m$ heißt stetig partiell differenzierbar in $\bar{a} \in \mathbb{R}^n$, wenn es ein $\varepsilon > 0$ gibt, so dass f auf ganz $B_\varepsilon(\bar{a})$ partiell differenzierbar ist und die partiellen Ableitungen $\frac{\partial f_i}{\partial x_j}$ als Abbildungen von $B_\varepsilon(\bar{a}) \subseteq \mathbb{R}^n$ nach $\mathbb{R}^m$ stetig in $\bar{a}$ sind.* stetig partiell differenzierbar

Satz 10.12 *Es gelten die folgenden Implikationen (die Umkehrungen im Allgemeinen nicht):*

$$\begin{aligned} & f \text{ ist stetig partiell differenzierbar in } \bar{a} \\ \Longrightarrow\ & f \text{ ist total differenzierbar in } \bar{a} \\ \Longrightarrow\ & \text{alle Richtungsableitungen von } f \text{ in } \bar{a} \text{ existieren} \\ \Longrightarrow\ & f \text{ ist partiell differenzierbar in } \bar{a} \end{aligned}$$

Ableitungsregeln

Satz 10.13 *Seien $f, g : \mathbb{R}^n \to \mathbb{R}^m$ differenzierbar in $\bar{a}$, sei $h : \mathbb{R}^m \to \mathbb{R}^l$ differenzierbar in $f(\bar{a})$ und $r \in \mathbb{R}$. Dann sind die folgenden Funktionen ebenfalls differenzierbar in $\bar{a}$:*

	$f+g : \mathbb{R}^n \to \mathbb{R}^m$	*mit*	$(f+g)'(\bar{a}) = f'(\bar{a}) + g'(\bar{a})$
	$r \cdot f : \mathbb{R}^n \to \mathbb{R}^m$	*mit*	$(r \cdot f)'(\bar{a}) = r \cdot (f'(\bar{a}))$
	$h \circ f : \mathbb{R}^n \to \mathbb{R}^l$	*mit*	$(h \circ f)'(\bar{a}) = h'(f(\bar{a})) \circ f'(\bar{a})$
(*falls* $m = 1$)	$f \cdot g : \mathbb{R}^n \to \mathbb{R}$	*mit*	$(f \cdot g)'(\bar{a}) = f(\bar{a}) \cdot g'(\bar{a}) + g(\bar{a}) \cdot f'(\bar{a})$
(*falls* $m = 1$ *und* f *nie* 0)	$\frac{1}{f} : \mathbb{R}^n \to \mathbb{R}$	*mit*	$(\frac{1}{f})'(\bar{a}) = -\frac{1}{f^2(\bar{a})} \cdot f'(\bar{a})$

Man muss etwas vorsichtig sein in dem, was die Ableitungsregeln genau bedeuten: In der Produktregel sind etwa $f(\bar{a})$ und $g(\bar{a})$ Zahlen und $f'(\bar{a})$ und $g'(\bar{a})$ lineare Abbildungen. $(f \cdot g)'(\bar{a})$ ist also die lineare Abbildung mit

$$(f \cdot g)'(\bar{a})(\bar{x}) = f(\bar{a}) \cdot g'(\bar{a})(\bar{x}) + g(\bar{a}) \cdot f'(\bar{a})(\bar{x})$$

Bemerkung 10.14 Wenn $f : \mathbb{R} \to \mathbb{R}$ eine in a total differenzierbare Funktion ist, dann ist für jedes i die Funktion $\hat{f} = f \circ \pi_i : \mathbb{R}^n \to \mathbb{R}$, $(x_1, \ldots, x_n) \mapsto f(x_i)$ total differenzierbar in jedem $\bar{a}$ mit $a_i = a$.

Dies ergibt sich aus der Kettenregel in Satz 10.13 mit $\hat{f}'(\bar{a}) = f'(a) \circ \pi_i'(\bar{a}) = f'(a) \circ \pi_i$, da die Projektion π_i als lineare Abbildung ihre eigene Ableitung ist. Es ist also $\hat{f}'(\bar{a})(\bar{x}) = f'(a) \cdot x_i$.

Zusammen mit Satz 10.13 und Satz 10.7 lassen sich daraus viele Beispiele differenzierbarer Funktionen $\mathbb{R}^n \to \mathbb{R}^m$ bilden. Insbesondere sind alle polynomiellen Funktionen in mehreren Veränderlichen überall differenzierbar, ebenso alle polynomiellen Ausdrücke in den Funktionen $\sin(x_i), \cos(x_i), r^{x_i}, \log(x_i)$.

Die Funktion $\mathbb{R}^4 \to \mathbb{R}^2$, $\bar{x} \mapsto (e^{\sin(x_1 \cdot x_2^2 \cdot \cos(3x_4))}, \sqrt[3]{5} x_1^4 x_2^3 - e^{e^{x_2 - x_3}})$ ist auf ganz $\mathbb{R}^4$ total differenzierbar.

Unter bestimmten Umständen lässt sich auch auf die Differenzierbarkeit einer Umkehrabbildung schließen. Es gibt davon mehrere Version, die je nach Anforderungen an die Funktion. Hier ein Beispiel:

Satz 10.15 *Sei $f : \mathbb{R}^n \to \mathbb{R}^n$ bijektiv und differenzierbar in $\bar{a}$. Die Ableitung $f'(a)$ sei invertierbar, d. h.* $\det f'(a) \neq 0$*, und die Umkehrbabildung f^{-1} sei stetig in $f(\bar{a})$. Dann ist f^{-1} differenzierbar in $f(\bar{a})$ mit $(f^{-1})'(f(\bar{a})) = (f'(a))^{-1}$.*

11 Höhere Ableitungen

Für eine überall differenzierbare Funktion $f : \mathbb{R}^n \to \mathbb{R}^m$ ist die Ableitung eine Funktion $f' : \mathbb{R}^n \to \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)$. Dabei ist $\mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)$ ein $n{\cdot}m$-dimensionaler $\mathbb{R}$-Vektorraum, also isomorph zu $\mathbb{R}^{nm}$: Durch die Matrixdarstellung bezüglich der Standardbasen kann man $\mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)$ zunächst mit dem Raum $\mathrm{Mat}_{m\times n}(\mathbb{R})$ der $(m \times n)$-Matrizen über $\mathbb{R}$ identifizieren. Durch die Wahl einer Reihenfolge für die Matrixeinträge erhält man einen Isomorphismus mit $\mathbb{R}^{nm}$.

Daher kann man f' als eine Funktion $\mathbb{R}^n \to \mathbb{R}^{nm}$ auffassen, deren Komponentenfunktionen die partiellen Ableitungen $\frac{\partial f_i}{\partial x_j}$ sind. Als solche Funktion kann man sie nun mit wie im vorigen Abschnitt definiert auf Differenzierbarkeit untersuchen. Falls f' in $\bar{a} \in \mathbb{R}^n$ differenzierbar ist, erhält man also als Ableitung $f''(\bar{a}) \in \mathrm{Lin}(\mathbb{R}^n, \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m)) \cong \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^{nm}) \cong \mathbb{R}^{n^2\cdot m}$.

Auf diese Art und Weise kann man beliebig hohe Ableitungen $f^{(k)}$ definieren, sofern die Funktion entsprechend oft differenzierbar ist.

zweite partielle Ableitungen

Definition 11.1 *Die partiellen Ableitungen von f' heißen zweite partielle Ableitungen von f. Man schreibt für $\frac{\partial \frac{\partial f}{\partial x_j}}{\partial x_l}(\bar{a}) = \frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j} f(\bar{a})$ meistens*

$$\frac{\partial^2 f}{\partial x_l \partial x_j}(\bar{a}) \quad \textit{bzw. auch} \quad \frac{\partial^2 f}{\partial x_j^2}(\bar{a}) \quad \textit{falls} \quad j = l$$

Analog heißten die partiellen Ableitungen von $f^{(k-1)}$ k-te partielle Ableitungen von f, und man schreibt sie

$$\frac{\partial^k f}{\partial x_{j_1} \dots \partial x_{j_k}}(\bar{a})$$

$f : \mathbb{R}^2 \to \mathbb{R}$ ist gegeben durch $f(x_1, x_2) = 5x_1^3x_2^2 - 3x_1x_2$. Die ersten partiellen Ableitungen von f wurden auf Seite 101 berechnet als

$$\frac{\partial f}{\partial x_1}(x_1, x_2) = 15x_1^2x_2^2 - 3x_2 \quad \text{und} \quad \frac{\partial f}{\partial x_2}(x_1, x_2) = 10x_1^3x_2 - 3x_1$$

Die zweiten partiellen Ableitungen sind dann

$$\begin{aligned}
\frac{\partial^2 f}{\partial x_1^2}(x_1, x_2) &= \frac{\partial f}{\partial x_1}\Big(\frac{\partial f}{\partial x_1}(x_1, x_2)\Big) = \frac{\partial f}{\partial x_1}\big(15x_1^2x_2^2 - 3x_2\big) = 30x_1x_2^2 \\
\frac{\partial^2 f}{\partial x_2 \partial x_1}(x_1, x_2) &= \frac{\partial f}{\partial x_2}\Big(\frac{\partial f}{\partial x_1}(x_1, x_2)\Big) = \frac{\partial f}{\partial x_2}\big(15x_1^2x_2^2 - 3x_2\big) = 30x_1^2x_2 - 3 \\
\frac{\partial^2 f}{\partial x_1 \partial x_2}(x_1, x_2) &= \frac{\partial f}{\partial x_1}\Big(\frac{\partial f}{\partial x_2}(x_1, x_2)\Big) = \frac{\partial f}{\partial x_1}\big(10x_1^3x_2 - 3x_1\big) = 30x_1^2x_2 - 3 \\
\frac{\partial^2 f}{\partial x_2^2}(x_1, x_2) &= \frac{\partial f}{\partial x_2}\Big(\frac{\partial f}{\partial x_2}(x_1, x_2)\Big) = \frac{\partial f}{\partial x_2}\big(10x_1^3x_2 - 3x_1\big) = 10x_1^3
\end{aligned}$$

Möchte man die zweiten partiellen Ableitungen in einem festen Punkt, setzt man diesen ein. Beispielsweise $\frac{\partial^2 f}{\partial x_1 \partial x_2}(1, -2) = 30 \cdot 1^3 \cdot (-2) - 3 = -63$.

Dass im diesem Beispiel die beiden Funktionen $\frac{\partial^2 f}{\partial x_2 \partial x_1}(x_1, x_2)$ und $\frac{\partial^2 f}{\partial x_1 \partial x_2}(x_1, x_2)$ übereinstimmen, ist kein Zufall, sondern erklärt sich aus dem folgenden Satz.

Satz 11.2 (Satz von Schwarz) *Falls f zweimal differenzierbar in $\bar{a}$ ist, gilt*

$$\frac{\partial^2 f}{\partial x_l \partial x_j}(\bar{a}) = \frac{\partial^2 f}{\partial x_j \partial x_l}(\bar{a})$$

Allgemeiner: Falls f k-mal differenzierbar in $\bar{a}$ ist, kommt es bei den k-ten partiellen Ableitungen von f nicht auf die Reihenfolge der Ableitungsrichtungen an.

Die differenzierbaren Funktionen, die man einfach hinschreiben kann und typischerweise betrachtet – z. B. Polynome, Exponentialfunktionen, trigonometrische Funktionen – sind unendlich oft differenzierbar. Man muss sich einigermaßen anstrengen, um eine Funktion zu konstruieren, bei der die Reihenfolge von partiellen Ableitungen eine Rolle spielt.

Sind A, B, C beliebige Mengen, so lassen sich die Abbildungen in $\mathrm{Abb}(A, \mathrm{Abb}(B, C))$ mit den Abbildungen in $\mathrm{Abb}(A \times B, C)$ identifizieren, indem ein $h : A \to \mathrm{Abb}(B, C)$ umgewandelt wird in die Abbildung $\hat{h} : A \times B \to C$ mit $\hat{h}(a, b) := h(a)(b)$.[35]

Wendet man dies auf $f''(\bar{a}) \in \mathrm{Lin}(\mathbb{R}^n, \mathrm{Lin}(\mathbb{R}^n, \mathbb{R}^m))$ an, erhält man $\widehat{f''(\bar{a})} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^m$. Diese Abbildung ist zusätzlich linear in beiden Argumenten aus $\mathbb{R}^n$, also eine sogenannte *bilineare Abbildung*, die der Einfachheit halber ebenfalls $f''(\bar{a})$ geschrieben wird. Anschaulich ist $f''(\bar{a})(\bar{v}, \bar{w})$ die Änderung der Richtungsableitung $D_{\bar{v}} f(\bar{a})$, wenn man sich in Richtung $\bar{w}$ bewegt (nach dem Satz von Schwarz symmetrisch in $\bar{v}$ und $\bar{w}$).

Allgemeiner erhält man durch die analoge Identifikation eine *multilineare Abbildung*

$$f^{(k)}(\bar{a}) : \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_{k \text{ mal}} \to \mathbb{R}^m$$

Im Fall $m = 1$ kann die bilineare Abbildung $f''(\bar{a})$ durch eine doppelte Matrixmultiplikation beschrieben werden. Es ist nämlich

$$f''(\bar{a})(\bar{v}, \bar{w}) \;=\; (v_1, \ldots, v_n) \cdot \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2}(\bar{a}) & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(\bar{a}) \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(\bar{a}) & \cdots & \frac{\partial^2 f}{\partial x_n^2}(\bar{a}) \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

Definition 11.3 *Die $(n \times n)$-Matrix der zweiten partiellen Ableitungen von f in $\bar{a}$ heißt die Hesse-Matrix $\mathrm{H}f(\bar{a})$ von f in $\bar{a}$.* Hesse-Matrix

Ist f zweimal differenzierbar in $\bar{a}$, dann ist die Hesse Matrix $\mathrm{H}f(\bar{a})$ symmetrisch.

Sei $f : \mathbb{R}^2 \to \mathbb{R}$ wieder gegeben durch $f(x_1, x_2) = 5x_1^3 x_2^2 - 3x_1 x_2$. Die zweiten partiellen Ableitungen wurden auf Seite 103 berechnet. Die Hesse-Matrix von f in einem beliebigen Punkt (x_1, x_2) ist demnach die symmetrische Matrix

$$\begin{pmatrix} 30x_1 x_2^2 & 30x_1^2 x_2 - 3 \\ 30x_1^2 x_2 - 3 & 10x_1^3 \end{pmatrix}$$

Die Hesse-Matrix von f zum Beispiel im Punkt $(1, -2)$ erhält man durch Einsetzen:

$$\begin{pmatrix} 30 \cdot 1 \cdot (-2)^2 & 30 \cdot 1^2 \cdot (-2) - 3 \\ 30 \cdot 1^2 \cdot (-2) - 3 & 10 \cdot 1^3 \end{pmatrix} = \begin{pmatrix} 120 & -63 \\ -63 & 10 \end{pmatrix}$$

[35] Der umgekehrte Prozesse spielt in der Informatik eine gewisse Rolle und wird manchmal *Currying* genannt.

Ist $f : \mathbb{R}^n \to \mathbb{R}$ zweimal differenzierbar in $\bar{a}$, ist $\bar{a}$ ein *kritischer Punkt*, d. h. $\operatorname{grad} f(\bar{a}) = (0, \ldots, 0)$, und gilt für alle Vektoren $\bar{v} \in \mathbb{R}^n$ der Länge 1

$$\bar{v}^{\mathrm{T}} \cdot \mathrm{H}f(\bar{a}) \cdot \bar{v} > 0 \quad (\text{oder } < 0\ )$$

dann hat f in $\bar{a}$ ein lokales Minimum (bzw. Maximum).

Die Hesse-Matrix heißt in diesem Fall *positiv definit* bzw. *negativ definit*. Dafür gibt es relativ einfach nachprüfbare Kriterien. Findet man ein $\bar{v}$ mit $\bar{v}^{\mathrm{T}} \cdot \mathrm{H}f(\bar{a}) \cdot \bar{v} > 0$ und ein anderes mit $\bar{v}^{\mathrm{T}} \cdot \mathrm{H}f(\bar{a}) \cdot \bar{v} < 0$, heißt $\mathrm{H}f(\bar{a})$ *indefinit* und es liegt ein *Sattelpunkt* vor. In allen anderen Fällen kann man aus dem Verhalten der zweiten Ableitung in $\bar{a}$ allein keine Aussage darüber treffen, ob ein Maximum, Minimum oder Sattelpunkt vorliegt.

Der Wert $\bar{v}^{\mathrm{T}} \cdot \mathrm{H}f(\bar{a}) \cdot \bar{v}$ entspricht der zweiten Ableitung von f in $\bar{a}$ in Richtung $\bar{v}$, die man die *Richtungskrümmung* in Richtung $\bar{v}$ nennen könnte.

Sei $f : \mathbb{R}^2 \to \mathbb{R}$ wieder gegeben durch $f(x_1, x_2) = 5x_1^3x_2^2 - 3x_1x_2$. Die Hesse-Matrix von f im Punkt $(1, -2)$ (der allerdings keine kritischer Punkt ist) ist indefinit:

$$(v_1, v_2) \cdot \begin{pmatrix} 120 & -63 \\ -63 & 10 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 120v_1^2 - 126v_1v_2 + 10v_2^2$$

Für $(v_1, v_2) = (1, 0)$ erhält man den positiven Wert 120, für $(v_1, v_2) = \frac{1}{\sqrt{5}}(1, 2)$ den negativen Wert $-\frac{92}{5}$.

Ein brauchabres Kriterium, um eine Matrix auf positive Definitheit zu testen, ist das *Hurwirt-Kriterium*.

Satz 11.4 (Hurwitz–Kriterium) *Eine reelle $(n \times n)$-Matrix A ist genau dann positiv definit, wenn alle (Teil-)Matrizen*

$$\begin{pmatrix} a_{11} \end{pmatrix}$$
$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$
$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$
$$\vdots$$
$$\begin{pmatrix} a_{11} & \ldots & \ldots & a_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{n1} & \ldots & \ldots & a_{nn} \end{pmatrix} = A$$

Determinante > 0 haben.

A ist genau dann negativ definit, wenn $-A$ positiv definit ist.[36]

[36] Was nicht bedeutet, dass alle diese Determinanten negativ sind, sondern immmer abwechslend negativ und poitiv!

Für die Matrix

$$A = \begin{pmatrix} 120 & -63 \\ -63 & 10 \end{pmatrix}$$

muss man $\det(120) = 120 > 0$ und $\det A = -2769$ betrachten. Die Determinante ist daher nicht positiv definit (und auch nicht negativ definit).

Bestimmung lokaler Extrema

Sei eine Funktion $f : \mathbb{R}^n \to \mathbb{R}$ gegeben, z. B. mit $n = 2$ die Funktion

$$f(x, y) = 5x^3 + 4xy + 2y^2.$$

(1) Zunächst werden die ersten partiellen Ableitungen ausgerechnet und der Gradient gebildet:

$$\begin{aligned} \tfrac{\partial f}{\partial x}(x, y) &= 15x^2 + 4y \\ \tfrac{\partial f}{\partial y}(x, y) &= 4x + 4y \\ \operatorname{grad} f(x, y) &= \big(15x^2 + 4y, 4x + 4y\big) \end{aligned}$$

(2) Dann werden die kritischen Punkte bestimmt, also die $(a_1, \ldots, a_n) \in \mathbb{R}^n$ mit

$$\operatorname{grad} f(a_1, \ldots, a_n) = 0.$$

Das ist nur in besonderen Fällen explizit möglich; im Allgemeinen kann man mit numerischen Verfahren Näherungen bestimmen.

Im Beispiel: $(15x^2 + 4y, 4x + 4y) = 0 \iff \big[x = -y \text{ und } 15x^2 - 4x = (15x - 4)x = 0\big]$. Die beiden Lösungen für dieses (nicht-lineare) Gleichungssystem sind $(a_1, b_1) = (0, 0)$ und $(a_2, b_2) = (\frac{4}{15}, -\frac{4}{15})$.

(3) Anschließend werden die zweiten partiellen Ableitungen ausgerechnet und die Hesse-Matrix gebildet:

$$\begin{aligned} \tfrac{\partial^2 f}{\partial x^2}(x, y) &= 30x \\ \tfrac{\partial^2 f}{\partial x \partial y}(x, y) = \tfrac{\partial^2 f}{\partial y \partial x}(x, y) &= 4 \\ \tfrac{\partial^2 f}{\partial y^2}(x, y) &= 4 \\ \mathrm{H} f(x, y) &= \begin{pmatrix} 30x & 4 \\ 4 & 4 \end{pmatrix} \end{aligned}$$

(4) Schließlich wird die Hesse-Matrix an den kritischen Punkten auf Definitheit untersucht:

- $\mathrm{H} f(0, 0) = \left(\begin{smallmatrix} 0 & 4 \\ 4 & 4 \end{smallmatrix}\right)$ ist indefinit, da

  $$(v, w) \cdot \mathrm{H} f(0, 0) \cdot (v, w)^{\mathrm{T}} = 8vw + 4w^2$$

  und dies z. B. für $v = w = \frac{1}{\sqrt{2}}$ positiv und für $-v = \frac{1}{\sqrt{2}} = w$ negativ wird.

- $\mathrm{H} f(\frac{4}{15}, -\frac{4}{15}) = \left(\begin{smallmatrix} 8 & 4 \\ 4 & 4 \end{smallmatrix}\right)$ ist positiv definit, da

  $$(v, w) \cdot \mathrm{H} f(0, 0) \cdot (v, w)^{\mathrm{T}} = 8v^2 + 4vw + 4w^2 = 6v^2 + 2(v + w)^2 + 2w^2,$$

  was als Summe von Quadraten stets $\geqslant 0$ ist und nur für $v = w = 0$ null wird.

  Alternativ mit dem Hurwitz-Kriterium: $8 > 0$ und $\det \mathrm{H} f(\frac{4}{15}, -\frac{4}{15}) = 16 > 0$.

Also liegt in $(0, 0)$ ein Sattelpunkt und in $(\frac{4}{15}, -\frac{4}{15})$ ein lokales Minimum von f vor.