



Friedrich-Alexander-Universität
Naturwissenschaftliche Fakultät



Vorlesungsskript

Mathematik für Ingenieure I

Wintersemester 2009/10
Sommersemester 2011
Wintersemester 2011/12
Wintersemester 2013/14
Wintersemester 2017/18
Wintersemester 2019/20
Wintersemester 2021/22
Wintersemester 2023/24

Prof. Dr. Serge Kräutle

am

Lehrstuhl für Angewandte Mathematik (Modellierung und Numerik)

AM1

— Version vom 24.02.2024 —

Friedrich–Alexander–Universität Erlangen–Nürnberg

Inhaltsverzeichnis

1 Grundlagen	2
1.1 Grundzüge der Aussagenlogik	2
1.2 Mengen	5
1.3 Relationen	8
1.4 Abbildungen (Funktionen)	12
1.5 Kurzer Einblick in die Kombinatorik	15
2 Zahlensysteme	17
2.1 Die natürlichen und die ganzen Zahlen; Gruppen, Ringe, Körper	17
2.2 Die rationalen Zahlen	25
2.3 Die reellen Zahlen	27
2.4 Dezimaldarstellung rationaler und reeller Zahlen	31
2.5 Die komplexen Zahlen	34
3 Lineare Algebra	45
3.1 Lineare Gleichungssysteme: Das Gauß-Verfahren	45
3.2 Vektorräume	52
3.2.1 Definition und Beispiele	52
3.2.2 Unterräume und affine Unterräume	54
3.2.3 Lineare Unabhängigkeit, Erzeugendensysteme, Basen, Dimension	58
3.3 Lineare Abbildungen, Bild und Kern	67
3.4 Matrizen	75
3.5 Determinanten	88
3.6 Eigenwerte und Eigenvektoren	99
3.6.1 Berechnung von Eigenwerten, Charakteristisches Polynom	101
3.6.2 Eigenräume, Ähnlichkeitstransformationen, Diagonalisierbarkeit	103
3.7 Das Skalarprodukt und Anwendungen	108
3.7.1 Hyperebenen	112
3.7.2 Symmetrische Matrizen, Orthogonalmatrizen	115

Dieses Skript entstand im Wintersemester 2009/2010 semesterbegleitend für einen Kurs Mathematik für Ingenieure 1 für Informatiker und Wirtschaftsingenieure. Im Sommersemester 2011 wurde dieses Skript semesterbegleitend leicht überarbeitet.

Kleingedruckte Abschnitte können beim ersten Lesen ausgelassen werden; sie liefern dem interessierten Leser zusätzliche Hintergrundinformationen, sie sind nicht klausur-relevant.

1 Grundlagen

1.1 Grundzüge der Aussagenlogik

Aussagen in der Mathematik können mit Worten formuliert werden, z.B.

A := "Alle natürlichen Zahlen sind größer oder gleich 1",

B := "5 ist durch 2 teilbar"

C := "Wenn eine Zahl durch 8 teilbar ist, dann auch durch 2"

oder auch in formalisierter Schreibweise ('Formelschreibweise', siehe 'Quantoren' am Ende von Kap. 1.1).

Für mathematische Aussagen gilt:

Jede Aussage ist entweder wahr oder falsch.

(Bivalenzprinzip, Prinzip der Zweiwertigkeit, Tertium non datur)

Außerdem gibt es noch Aussagen (auch genannt Aussageformen), die von 'freien' Variablen abhängen, wie z.B. $A(x)$:= " x ist durch 3 teilbar" (kann entweder wahr oder falsch sein, je nachdem was x ist).

Bemerkung: Für Aussagen außerhalb der Mathematik, die in *natürlicher* Sprache formuliert werden, und die sich nicht in Formelschreibweise übertragen lassen, ist dieses Axiom i.a. *nicht* erfüllt. Zum einen gibt es in natürlichen Sprachen (zum Glück) die Möglichkeit, Halbwahrheiten, Meinungen, ungenaue Aussagen (z.B. 'Es regnet.' (Wo? Wann?)) etc. zu formulieren, deren Wahrheitswert sich nicht klar auf 'wahr' oder 'falsch' festlegen lässt. Um für mathematische Aussagen das Bivalenzprinzip zu erfüllen, ist also *Präzision* bei der Formulierung mathematischer Aussagen von extremer Wichtigkeit. Daneben gibt es noch ein tiefergehendes Problem in natürlichen Sprachen. So kann man selbstbezügliche Aussagen formulieren wie A := "Dieser Satz ist falsch." Ist A wahr oder falsch? Wenn A wahr wäre, so besagt A , dass A falsch ist. Und wenn A falsch wäre, so besagt A , dass A wahr ist. Ein weiteres berühmtes Beispiel ist der Satz B := "Der Friseur rasiert all diejenigen Leute, die sich nicht selbst rasieren". Der Aussage C := "Der Friseur rasiert sich selbst" kann dann ebenfalls kein Wahrheitswert zugewiesen werden.¹ Es wäre fatal, wenn solche Aussagen, denen man keinen Wahrheitswert zuordnen kann, auch innerhalb der Mathematik existieren würden, also das Bivalenzprinzip verletzt wäre; dazu mehr in Kap. 1.2.

Logische Verknüpfungen. Sind A und B (mathematische) Aussagen, so sind

¹Manchmal wird in diesem Zusammenhang auch das sog. Kreter-Paradoxon (als historisch ältestes Paradoxon dieser Art) genannt: *Epimenides (der Kreter) sagte: Alle Kreter sind Lügner.* Aus diesem 'Paradoxon' jedoch gibt es, dank der Ungenauigkeit natürlicher Sprachen, gewisse Ausflüchte. In der Formulierung "*Ich lüge (jetzt gerade)*" wird der Satz zu einem echten Paradoxon.

$C := A \wedge B$ (sprich: A und B),
 $D := A \vee B$ (sprich: A oder B),
 $E := \neg A$ (sprich: nicht A)

ebenfalls Aussagen. Der Wahrheitswert der Verknüpfungen wird durch folgende sog. **Wahrheitstabellen** definiert:

A	B	$A \wedge B$	$A \vee B$
f	f	f	f
f	w	f	w
w	f	f	w
w	w	w	w

A	$\neg A$
f	w
w	f

Hierbei steht "w" für "wahr" und "f" für "falsch". Es ist ebenfalls weit verbreitet, "1" für wahr und "0" für falsch zu schreiben.

Zwei Aussagen heißen *äquivalent* ($A \Leftrightarrow B$; alternative Schreibweise: $A = B$), wenn sie identische Wahrheitswerte besitzen. Wir können " \Leftrightarrow " ebenfalls als Verknüpfung von Aussagen auffassen, $C := (A \Leftrightarrow B)$, und diese Verknüpfung C soll genau dann wahr sein, wenn A und B den gleichen Wahrheitswert haben; in einer Wahrheitstabelle sieht das so aus:

A	B	$A \Leftrightarrow B$
f	f	w
f	w	f
w	f	f
w	w	w

Ferner definieren wir die Verknüpfung der Implikation $C := (A \Rightarrow B)$ (sprich: 'aus A folgt B ', 'wenn A dann B ', ' A impliziert B ', A ist hinreichend für B) durch die Wahrheitstafel

A	B	$A \Rightarrow B$
f	f	w
f	w	w
w	f	f
w	w	w

Bemerkung: Erfahrungsgemäß bereitet es einige Schwierigkeiten die Sinnhaftigkeit dieser Definition einzusehen. Am ehesten leuchten die beiden letzten Zeilen der Tabelle ein. Was die beiden ersten Zeilen angeht, so besagen sie, dass man festgelegt hat: Wenn man unter falschen Voraussetzungen startet, so darf man daraus beliebiges folgern; die Folgerung als ganzes ist dann wahr ("Wenn $1=0$ ist, so sind alle Zahlen durch 7 teilbar" wird als wahre Aussage angesehen (Zeile 1). Ebenso: "Wenn alle Zahlen ungerade sind, so ist 5 ungerade" (Zeile 2), sowie: "Wenn alle Zahlen ungerade sind, so ist 4 ungerade" (Zeile 1)). Selbst die Implikation "Wenn alle Zahlen ungerade sind, so ist 5 gerade" ist wahr (weil ja 4 dann ungerade ist, muss 5 gerade sein); kurz: aus etwas Unwahren darf man alles folgern. In der natürlichen Sprache können Sie Sätze bilden die anfangen mit "Wenn Schweine fliegen können dann..."; Sie können diesen Satz *beliebig* fortsetzen, in jedem Fall bleibt der Satz wahr, da der Wenn-Teil des Satzes falsch ist.

Neben der Definition von logischen Verknüpfungen kann man Wahrheitstabellen benutzen, um die Äquivalenz von Aussagen zu überprüfen. Z.B. sind " $A \Leftrightarrow B$ " und " $A \Rightarrow B \wedge B \Rightarrow A$ " äquivalent:

$$(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B \wedge B \Rightarrow A)$$

Beweis durch Wahrheitstafel:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$	$A \Leftrightarrow B$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	1	1	1	1

Die letzten beiden Spalten stimmen überein. □

Ebenso durch Wahrheitstafeln (siehe Übung) kann man die folgenden Äquivalenzen zeigen:

- (i) $A \vee B \Leftrightarrow B \vee A$
- (ii) $A \wedge B \Leftrightarrow B \wedge A$
- (iii) $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
- (iv) $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$
- (v) $(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$
- (vi) $(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$
- (vii) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$
- (viii) $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
- (ix) $\neg\neg A \Leftrightarrow A$
- (x) $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$
- (xi) $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
- (xii) $A \vee \neg A \Leftrightarrow \text{wahr}$
- (xiii) $A \wedge \neg A \Leftrightarrow \text{falsch}$
- (xiv) $A \vee \text{wahr} \Leftrightarrow \text{wahr}$
- (xv) $A \vee \text{falsch} \Leftrightarrow A$
- (xvi) $A \wedge \text{wahr} \Leftrightarrow A$
- (xvii) $A \wedge \text{falsch} \Leftrightarrow \text{falsch}$
- (xviii) $A \vee A \Leftrightarrow A$
- (xix) $A \wedge A \Leftrightarrow A$

(i) und (ii) sind *Kommutativgesetze*, (iii) und (iv) sind *Assoziativgesetze*, (v) und (vi) sind *Distributivgesetze*, (vii) und (viii) heißen *De Morgan'sche Gesetze*, (x) ist eine wichtige Charakterisierung der Implikation ((x) hätte man – anstelle einer Wertetafel – als Definition der Implikation verwenden können), (xi) wird manchmal als das

Prinzip der *Kontraposition* bezeichnet, (xviii)-(xix) sind *Idempotenzgesetze*. Die obigen Äquivalenzen sind so zu verstehen, dass sie für *beliebige* Aussagen A, B, C Gültigkeit haben.

Quantoren. Um mathematische Aussagen knapp und präzise und ohne Verwendung von Wörtern (vgl. Anfang des Kapitels) notieren zu können, braucht man *Quantoren*. Es gibt zwei Arten, den *Allquantor* und den *Existenzquantor*:

\forall : "für alle", "für jedes"

\exists : "es existiert", "es gibt" (im Sinne von: es gibt *mindestens* ein)

(Manchmal findet man auch: " $\exists!$ " für: "es gibt genau ein", "es gibt ein eindeutig bestimmtes")

Beispiele: Die beiden Aussagen zu Beginn dieses Kapitels in Quantorschreibweise lauten:

$$\forall n \in \mathbb{N} : n \geq 1$$

$$\exists t \in \mathbb{Z} : 5 = 2t$$

Quantoren können auch kombiniert werden, z.B.:

$$\forall n \in \mathbb{N} \exists m \in \mathbb{N} : m > n$$

Wie lautet diese Aussage in Worten? Ist sie wahr?

Die dritte Aussage zu Beginn dieses Kapitels lautet in Quantorenschreibweise:

$$\forall z \in \mathbb{Z} : (\exists t \in \mathbb{Z} : z = 8t \implies \exists u \in \mathbb{Z} : z = 2u)$$

Bei gleichartigen Quantoren ($\forall \dots \forall \dots$, $\exists \dots \exists \dots$) ist die Reihenfolge unerheblich; bei verschiedenartigen Quantoren ($\forall \dots \exists \dots$, $\exists \dots \forall \dots$) darf die Reihenfolge i.a. nicht verändert werden (s. Übung). Beim Hinein- oder Herausziehen eines Negationszeichens ändert sich immer die Art des Quantors (s. Übung), d.h.

$$\neg(\forall x \in M : A(x)) \iff \exists x \in M : \neg A(x)$$

$$\neg(\exists x \in M : A(x)) \iff \forall x \in M : \neg A(x)$$

1.2 Mengen

Def. (Mengendefinition nach Cantor)². Eine *Menge* ist eine Zusammenfassung von wohlbestimmten und wohlunterschiedenen Objekten zu einem Ganzen. Die Objekte heißen *Elemente* der Menge.

Ist a ein Element der Menge M , so schreiben wir $a \in M$, andernfalls $a \notin M$. (Genau eine von beiden Aussagen ist immer wahr, Bivalenzprinzip). Mengen können durch Aufzählung der Elemente beschrieben werden, z.B. $M = \{1, 2, 3\}$,

²Georg Cantor, 1845-1913, 'Vater' der Mengenlehre

$M = \{0, 2, 4, 6, 8, \dots\}$; Mengen können endlich oder unendlich viele Elemente besitzen. Mit $\emptyset := \{\}$ wird die leere Menge bezeichnet; es gilt $\forall a : a \notin \emptyset$.

Nach Cantor bezeichnet $M = \{1, 2, 2, 3\}$ keine sinnvolle Menge ('wohlunterschiedene Objekte').

Mengen können auch durch eine charakterisierende Eigenschaft definiert werden, z.B. $M = \{n \in \mathbb{N} \mid n \geq 5\} = \{n \mid n \in \mathbb{N} \wedge n \geq 5\}$ ³.

Wir definieren *Teilmengen* (Inklusion von Mengen):

$$M \subseteq N \iff \forall a \in M : a \in N \iff \forall a : (a \in M \Rightarrow a \in N)$$

Statt ' \subseteq ' wird von vielen Autoren auch ' \subset ' geschrieben.

Wir definieren die Gleichheit von Mengen:

$$M = N \iff M \subseteq N \wedge N \subseteq M$$

Zwei Mengen sind also gleich, wenn alle Elemente der ersten Menge auch Elemente der zweiten Menge sind, und alle Elemente der zweiten Menge Elemente der ersten Menge sind. Kurz: Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.

Die Elemente von Mengen können durchaus auch wiederum Mengen sein, ein skuriles Beispiel dazu wäre $M = \{0, 1, \{1, 2, 3\}, \emptyset\}$, dies ist nach Cantor in der Tat eine sinnvolle Menge. Wichtigstes Beispiel ist jedoch die *Potenzmenge* $P(M)$ einer Menge M :

Für eine Menge M heißt $P(M) := \{U \mid U \subseteq M\}$, also die Menge aller Teilmengen von M , die *Potenzmenge* von M .

Bsp.: $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Nach obiger Definition gilt $U \in P(M)$ genau dann wenn $U \subseteq M$.

Zur Übung: wie viele Elemente hat die Potenzmenge einer n -elementigen Menge?

Die Verknüpfung von Mengen liefert neue Mengen:

Vereinigung: $A \cup B := \{a \mid a \in A \vee a \in B\}$

Schnitt: $A \cap B := \{a \mid a \in A \wedge a \in B\}$

Differenz: $A \setminus B := \{a \mid a \in A \wedge a \notin B\}$ (sprich: A ohne B)

Paarmenge (Cartesisches Produkt)⁴:

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$$

³Wie Sie bemerken gehen wir hier einfach mal davon aus, wir wüssten schon, was Zahlen sind, um konkrete Beispiele für Mengen zur Verfügung zu haben. Wir werden auf diese Fragestellung, was Zahlen sind, noch einmal genauer in Kap. 2 eingehen

⁴René Descartes, 1596-1650

Beispiele: $\mathbb{R} \times \mathbb{R} [=: \mathbb{R}^2]$ (anschaulich: die Menge der Punkte in einer Ebene);
für $A = \{1\}$, $B = \{2, 3\}$ ist $A \times B = \{(1, 2), (1, 3)\}$.

Das Komplement einer Menge:

Sei Ω eine gegebene nichtleere Menge ('Grundmenge') und $A \subseteq \Omega$. Dann ist

$$\mathcal{C}A := \Omega \setminus A$$

das *Komplement von A (bzgl. der Grundmenge Ω)*. (Oft wird auch \bar{A} für $\mathcal{C}A$ geschrieben.)

Einige Verknüpfungsregeln für Mengen:

$$\begin{aligned} A \cap B &= B \cap A \\ A \cup B &= B \cup A \\ (A \cap B) \cap C &= A \cap (B \cap C) \\ (A \cup B) \cup C &= A \cup (B \cup C) \\ (A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \\ \mathcal{C}(A \cup B) &= \mathcal{C}(A) \cap \mathcal{C}(B) \\ \mathcal{C}(A \cap B) &= \mathcal{C}(A) \cup \mathcal{C}(B) \\ \mathcal{C}\mathcal{C}A &= A \\ A \cup \mathcal{C}A &= \Omega \\ A \cap \mathcal{C}A &= \emptyset \\ A \cup \Omega &= \Omega \\ A \cup \emptyset &= A \\ A \cap \Omega &= A \\ A \cap \emptyset &= \emptyset \\ A \cup A &= A \\ A \cap A &= A \end{aligned}$$

Es fällt die große strukturelle Ähnlichkeit dieser Verknüpfungsregeln für *Mengen* mit den entsprechenden Gesetzen für *Aussagen* aus Kap. 1.1 auf. Diese Ähnlichkeit wird verständlich, wenn man sich klar macht, wie man obige Mengengleichheiten beweist: Gemäß der Gleichheitsdefinition von Mengen muss man dazu zeigen, dass jedes Element der einen Menge auch Element der anderen Menge, sowie umgekehrt, ist. Und um dies zu tun, werden gerade die entsprechenden Regeln für *Aussagen* verwendet (siehe auch Übung).

Bemerkung: Die Mengenlehre, die auf die Cantor'sche Mengendefinition zurückgreift, wird auch als *Naive Mengenlehre* bezeichnet. Demgegenüber steht die sog. *Axiomatische Mengenlehre*, die im 20.

Jahrhundert entwickelt wurde (die für unsere Zwecke jedoch unnötig ist).

Die Notwendigkeit, die recht 'diffuse' Cantor'sche Mengendefinition müsse eigentlich durch etwas Präziseres ersetzt werden, kann man wie folgt einsehen:

Sei $\mathcal{M} := \{M \mid M \notin M\}$ (die Menge aller Mengen, die sich nicht selbst enthalten). Nach Cantor scheint dies eine sinnvolle Menge zu sein. Frage: Ist die Aussage $\mathcal{M} \in \mathcal{M}$ wahr oder falsch? Falls $\mathcal{M} \in \mathcal{M}$ falsch ist, also $\mathcal{M} \notin \mathcal{M}$ gilt, so ist nach Definition der Menge $\mathcal{M} \in \mathcal{M}$. Und falls $\mathcal{M} \notin \mathcal{M}$, so ist nach Definition $\mathcal{M} \in \mathcal{M}$. Die Aussage ist weder wahr noch falsch; Widerspruch zum Bivalenzprinzip! Es gibt, also, wenn man die recht 'diffuse' Mengendefinition von Cantor verwendet, in der Mathematik Aussagen, denen kein Wahrheitswert zugewiesen kann (so wie 'Dieser Satz ist falsch' in Kap. 1.1)!!

Als Konsequenz dieser als *Russel'sche Antinomie*⁵ (1902) bekannt gewordenen Schwierigkeit muss man strenger regeln, welche 'Gebilde' Mengen sind und welche nicht. Ein sehr rabiater Ansatz wäre, zu verbieten, dass die Elemente von Mengen wiederum Mengen sind; dann löst sich die Russel'sche Antinomie auf, jedoch könnten wir dann u.a. keine Potenzmengen bilden. Stattdessen werden Axiomatische Ansätze favorisiert. Diese gehen so vor, dass über rund ein halbes Dutzend Axiome geregelt wird, was Mengen sind, z.B. ein Axiom sagt, dass \emptyset eine Menge ist, ein weiteres besagt, dass wenn M eine Menge ist, auch $\{M\}$ eine Menge ist, ein Axiom sagt, dass wenn A und B Mengen sind, auch $A \cap B$ und $A \cup B$ Mengen sind, und so weiter⁶. Mit diesen Axiomen könnten wir, ganz ohne Zahlen zu verwenden, aus der leeren Menge weitere Mengen *konstruieren*: $\{\emptyset\}$ ist eine Menge, $\{\{\emptyset\}\}$ ist eine Menge; die Vereinigung der beiden Mengen, $\{\emptyset, \{\emptyset\}\}$ ist ebenfalls eine Menge; etc. Wir wollen das nicht weiter vertiefen, wie diese Axiome im Detail aussehen; im 'Normalfall' treten solche Antinomien nicht an jeder Ecke auf; es hat Jahrhunderte gedauert, bis man auf die Russel'sche stieß.

1.3 Relationen

Def. (Relation). Sei $M \neq \emptyset$ eine Menge und $R \subseteq M \times M$. Dann heißt R eine *Relation auf M* . also: Eine Relation auf einer Menge M ist nichts weiter als eine Menge von Paaren, also eine Teilmenge von $M \times M$.

Statt $(a, b) \in R$ schreibt man oft auch: aRb . Um die Übersichtlichkeit zu erhöhen schreibt man oft " \sim " statt " R ", also $a \sim b$ (dann auch: $(a, b) \in \sim$).

Beispiele:

- Auf der Menge \mathbb{N} ist durch $R := \sim := \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a < b\}$ offensichtlich eine Relation erklärt. Es ist also $R = \{(1, 2), (1, 3), (1, 4), \dots, (2, 3), (2, 4), \dots\}$; es ist $1 \sim 2$, aber $3 \not\sim 3$.
- Ist $M \neq \emptyset$, so ist $R := \{(a, a) \mid a \in M\}$ eine Relation auf M (Die Menge R wird auch *Diagonale* von $M \times M$ genannt). Bei der Relation handelt es sich offenbar um die Gleichheitsrelation $a \sim b \Leftrightarrow a = b$.

Bei Grundmengen der Art \mathbb{N} , \mathbb{Z} , \mathbb{R} kann man Relationen mittels eines Koordinatensystems veranschaulichen.

⁵Bertrand Russel, 1872-1970

⁶Das bekannteste Axiomensystem der Mengenlehre ist das von Zermelo-Fraenkel

Def. (Eigenschaften von Relationen). Eine Relation \sim auf einer Menge $M \neq \emptyset$ heißt

- (i) *reflexiv*, falls $\forall x \in M : x \sim x$
- (ii) *symmetrisch*, falls $\forall x, y \in M : (x \sim y \Rightarrow y \sim x)$
- (iii) *transitiv*, falls $\forall x, y, z \in M : (x \sim y \wedge y \sim z \Rightarrow x \sim z)$
- (iv) *antisymmetrisch*, falls $\forall x, y \in M : (x \sim y \wedge y \sim x \Rightarrow x = y)$
- (v) *alternativ*, falls $\forall x, y \in M : (x \sim y \vee y \sim x)$

z.Ü.: Welche dieser Eigenschaften haben die Relationen " \leq ", " $<$ ", " $=$ " (auf der Menge \mathbb{N} z.B.)?

Def. Eine Relation R auf einer Menge M heißt

- (i) *Äquivalenzrelation* genau dann wenn R reflexiv, symmetrisch und transitiv ist,
- (ii) *Ordnungsrelation* genau dann, wenn R reflexiv, antisymmetrisch und transitiv ist.

Falls eine Ordnungsrelation zusätzlich alternativ ist, heißt sie *vollständig*. Die Menge M heißt dann vollständig geordnet.

Ein Beispiel für eine (vollständige) Ordnungsrelation ist " \leq " (auf \mathbb{N} oder \mathbb{R}); " $<$ " ist jedoch nach obiger Definition *keine* Ordnungsrelation auf \mathbb{N} oder \mathbb{R} ! (Warum?)

\mathbb{N} und \mathbb{R} sind also durch " \leq " (oder auch " \geq ") vollständig geordnet. Ein Beispiel für eine Ordnung, die nicht vollständig ist, ist die Relation " \subseteq " auf einer Potenzmenge $P(M)$:

Wir zeigen

- (i) Reflexivität: Sei $A \in P(M)$, also $A \subseteq M$. Dann gilt offensichtlich $A \subseteq A$.
- (ii) Antisymmetrie: Seien $A, B \in P(M)$, also $A, B \subseteq M$, und es sei $A \subseteq B$ und $B \subseteq A$. Dann ist nach Definition der Gleichheit von Mengen $A = B$.
- (iii) Transitivität: Seien $A, B, C \subseteq M$ mit $A \subseteq B$ und $B \subseteq C$. Dann folgt $A \subseteq C$.
- (iv) Alternativität ist i.a. nicht erfüllt. Dazu geben wir ein Gegenbeispiel an:
 $M := \{1, 2, 3\}$, $A := \{1, 2\} [\in P(M)]$, $B := \{2, 3\} [\in P(M)]$. Es gilt weder $A \subseteq B$ noch $B \subseteq A$.

Äquivalenzrelationen und Partitionen

Def. (Partition). Sei $M \neq \emptyset$ eine Menge und seien $A_i, i \in I$, ein System von Teilmengen von M ⁷. (I ="Indexmenge"). Es seien die beiden folgenden Eigenschaften erfüllt:

⁷Soll heißen: eine *Menge* von Teilmengen von M

(i) Die A_i sind paarweise disjunkt, d.h. $\forall i, j \in I : i \neq j \Rightarrow A_i \cap A_j = \emptyset$.

(ii) Die A_i füllen ganz M auf, d.h. $\bigcup_{i \in I} A_i = M$.

Dann heißt das System der A_i eine *Partition* vom M .

Beispiele: Für $M = \{1, 2, 3, 4, 5\}$ ist das System $A_1 = \{1, 2\}, A_2 = \{4\}, A_3 = \{3, 5\}$ eine Partition. Für $M = \mathbb{N}$ ist z.B. $A_1 = \{1, 3, 5, 7, \dots\}$ und $A_2 = \{2, 4, 6, 8, 10, \dots\}$ eine Partition, aber auch $A_1 = \{1, 2, 3\}, A_2 = \{4, 5, 6\}, A_3 = \{7, 8, 9\}, \dots$

Bemerkung: Die Eigenschaft (i) lässt sich auch wie folgt formulieren: ein A_i und ein A_j sind entweder gleich (nämlich wenn $i = j$) oder disjunkt (nämlich wenn $i \neq j$).

Die folgenden beiden Sätze klären den Zusammenhang zwischen Äquivalenzrelationen und Partitionen auf:

Satz. Sei eine Partition $A_i, i \in I$, einer Menge M gegeben. Dann ist durch

$$x \sim y :\iff \exists i \in I : x, y \in A_i$$

eine Äquivalenzrelation \sim auf M erklärt.

Beweis. Wir müssen die drei Eigenschaften einer Äquivalenzrelation nachprüfen:

(i) Reflexivität: Sei $x \in M$ beliebig. Nach Eigenschaft (ii) der Partition gibt es ein $i \in I$ so dass $x \in A_i$. Es folgt nach Definition von \sim , dass $x \sim x$.

(ii) Symmetrie: Seien $x, y \in M$ und $x \sim y$. Also gibt es ein $i \in I$ so dass $x, y \in A_i$. Trivialerweise können wir das als $y, x \in A_i$ schreiben, woraus $y \sim x$ folgt.

(iii) Transitivität: Seien $x, y, z \in M$ und $x \sim y$ und $y \sim z$. Dann gibt es ein $i \in I$ mit $x, y \in A_i$, und es gibt ein $j \in I$ mit $y, z \in A_j$. Es ist also insbesondere $y \in A_i$ und $y \in A_j$, also $y \in A_i \cap A_j$, was $A_i \cap A_j \neq \emptyset$ zur Folge hat. Nach obiger Bemerkung muss also $A_i = A_j$, d.h. $i = j$ sein, und somit ist $x, z \in A_i = A_j$, also $x \sim z$. \square

Satz. Sei \sim eine Äquivalenzrelation auf $M \neq \emptyset$. Wir definieren für jedes $x \in M$ die Menge (Teilmenge von M)

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

Dann bilden die Mengen $[x]_{\sim}$ eine Partition von M .

Die beiden obigen Sätze besagen also, dass es zu jeder Partition einer Menge M eine 'zugehörige' Äquivalenzrelation auf M gibt, und umgekehrt, dass es zu jeder Äquivalenzrelation eine zugehörige Partition gibt.

Definition 1.1 . Die obigen Mengen $[x]_{\sim}$ heißen *Äquivalenzklassen* (von x bzgl. \sim). Ein Element von einer Klasse heißt auch *Repräsentant* der Klasse (so ist z.B. x immer ein Repräsentant der Klasse $[x]_{\sim}$). Beachten Sie, dass obige Definition einer Klasse $[x]_{\sim}$ bedeutet:

$$y \in [x]_{\sim} \Leftrightarrow y \sim x$$

Beweis des Satzes. Wir müssen zeigen, dass die beiden Eigenschaften (i) und (ii) von Partitionen erfüllt werden.

Zur Eigenschaft (i) ('Disjunktheit'). Seien $[x]_{\sim}$ und $[y]_{\sim}$ zwei Äquivalenzklassen. Es ist zu zeigen, dass $[x]_{\sim} = [y]_{\sim}$ oder $[x]_{\sim} \cap [y]_{\sim} = \emptyset$ gilt. Dazu nehmen wir an, dass $[x]_{\sim} \cap [y]_{\sim} \neq \emptyset$ gelte; es ist zu zeigen, dass dann $[x]_{\sim} = [y]_{\sim}$ gilt.

Sei also $z \in [x]_{\sim} \cap [y]_{\sim}$. Es ist also $z \in [x]_{\sim}$ und $z \in [y]_{\sim}$. Es folgt $z \sim x$ und $z \sim y$. Es folgt $x \sim y$ (Transitivität) sowie $y \sim x$ (Symmetrie). Nach Definition der Klassen bedeutet dies dass $x \in [y]_{\sim}$ und $y \in [x]_{\sim}$. Es folgt⁸ $[x]_{\sim} \subseteq [y]_{\sim}$ und $[y]_{\sim} \subseteq [x]_{\sim}$. Nach Definition der Gleichheit von Mengen also $[x]_{\sim} = [y]_{\sim}$

Zur Eigenschaft (ii): Sei $x \in M$ beliebig. Es ist zu zeigen, dass x zu einer der Klassen gehört. Dies ist trivial, denn $x \sim x$ (Reflexivität), d.h. $x \in [x]_{\sim}$. \square

Beispiele für Äquivalenzrelationen und -klassen.

- Die auf \mathbb{R} definierte Relation $x \sim y \iff |x| = |y|$ ist eine Äquivalenzrelation. Zugehörige Äquivalenzklassen sind $[5]_{\sim} = \{5, -5\}$, $[0]_{\sim} = \{0\}, \dots$ (Es gibt unendlich viele Klassen.)
- Die auf \mathbb{N}_0 definierte Relation $x \sim y \iff \exists t \in \mathbb{Z} : x - y = 5t$ ist eine Äquivalenzrelation. Zugehörige Klassen sind z.B. $[2]_{\sim} = \{2, 7, 12, 17, 22, \dots\}, \dots$ Es gibt genau 5 Klassen, und zwar $[0]_{\sim}, [1]_{\sim}, [2]_{\sim}, [3]_{\sim}, [4]_{\sim}$; es ist z.B. $[5]_{\sim} = [0]_{\sim}$ keine neue Klasse (s.Ü.).
- Die auf $\mathbb{R} \times \mathbb{R}$ definierte Relation $(x_1, x_2) \sim (y_1, y_2) \iff x_1^2 + x_2^2 = y_1^2 + y_2^2$ ist eine Äquivalenzrelation. Die Äquivalenzklassen sind konzentrische Kreise um $(0, 0)$.

Anwendungen. Relationen können verwendet werden, um 'Ordnung zu schaffen' in Mengen (z.B. ' \leq ' in \mathbb{N} oder \mathbb{R} , oder ' \subseteq ' in $P(M)$); denken Sie auch an die Relationen 'ist Elternteil von', 'ist Nachkomme von', definiert auf der Menge der Menschen (s.Ü.). Als (innermathematische) Anwendung des Konzeptes der Relation (genauer: der Äquivalenzrelation) werden wir in Kap. 2.2 die Konstruktion der Menge der rationalen Zahlen \mathbb{Q} kennenlernen. Weitere (außermathematische) Anwendungen finden sich z.B. in der Informatik im Bereich von Datenbanken ('relationale Datenbanken'); hier wird der Begriff der Relation etwas weiter gefasst als $R \subseteq M \times N$ statt wie bei uns $R \subseteq M \times M$. (Z.B. könnte eine Datenbank für eine Bibliotheksverwaltung eine Tabelle (=Menge) M von Büchern sowie eine Tabelle (=Menge) N von Nutzern beinhalten, und das Ausleihen von Büchern als Relation aufgefasst werden: $m \sim n \iff$ Nutzer n hat Buch m ausgeliehen.)

⁸denn alle Elemente, die mit x in Relation stehen (also die Klasse von x), stehen dann auch (Transitivität) mit y in Relation

1.4 Abbildungen (Funktionen)

Def. (Abbildung/Funktion, Definitionsbereich, Wertevorrat, Graph) Seien $M, N \neq \emptyset$ Mengen, und sei f eine Menge mit $f \subseteq M \times N$. Das Tripel (M, N, f) heißt *Funktion* (oder auch *Abbildung*), wenn es zu jedem $x \in M$ genau ein $y \in N$ gibt mit $(x, y) \in f$.

$f \subseteq M \times N$ schreibt man auch $f : M \rightarrow N$.

M heißt *Definitionsbereich* der Funktion (M, N, f) , N heißt *Wertevorrat* von (M, N, f) , und f heißt *Graph* von (M, N, f) .

Schreibweise: Es ist üblich, das zu einem $x \in M$ eindeutig bestimmte $y \in N$ mit der Eigenschaft $(x, y) \in f$ als $y = f(x)$ zu bezeichnen. Statt z.B. $(\mathbb{R}, \mathbb{R}, \{(x, y) \mid x \in \mathbb{R}, y = x^2\})$ schreibt man üblicherweise $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ oder $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$.

Eine Funktion ordnet also jedem Element des Definitionsbereichs genau ein Element des Wertevorrats zu.

Def. (Bildmenge) Die Menge

$$\text{Bild}(f) := f(M) := \{f(x) \mid x \in M\}$$

heißt *Bild* von f (oder auch *Bild der Menge M unter der Abbildung f*).

Die Bildmenge einer Abbildung muss also nicht mit dem Wertevorrat N übereinstimmen; sie ist i.a. nur eine Teilmenge.

Als Anwendung in der Informatik kann man z.B. Computerprogramme (oder Prozeduren) als Abbildungen betrachten; die eine Eingabe (entspricht dem x) einer Ausgabe $f(x)$ (berechnen und) zuordnen. Teamarbeit beim Programmieren erfordert, dass alle Teammitglieder sich über Definitionsmenge und Wertevorrat ("Schnittstellen") dieser Funktionen einig sind.

Def. (wichtige charakterisierende Eigenschaften von Funktionen) Sei $f : M \rightarrow N$ eine Funktion.

- a) Für $U \subseteq M$ sei $f(U) := \{f(x) \mid x \in U\}$.
(Insbesondere, für $U := M, f(M) = \{f(x) \mid x \in M\} = \text{Bild}(f)$).
- b) Für $y \in N$ sei $f^{-1}(y) := \{x \in M \mid f(x) = y\}$ die *Urbildmenge* von y .
(Vorsicht: Dies hat nichts mit Existenz einer Umkehrfunktion, die ebenfalls mit f^{-1} bezeichnet werden wird, zu tun!)
- c) f heißt *injektiv*, wenn für alle $x_1, x_2 \in M$ mit $x_1 \neq x_2$ gilt: $f(x_1) \neq f(x_2)$ (also: wenn verschiedene Urbilder immer verschiedene Bilder haben); kurz, wenn **jedes $y \in N$ höchstens ein Urbild hat**.
Zum Nachweis der Injektivität verwendet man am besten die äquivalente⁹ Cha-

⁹Die Äquivalenz der Aussagen ergibt sich aus dem Prinzip $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

rakterisierung: f ist genau dann injektiv, wenn für alle $x_1, x_2 \in M$ mit $f(x_1) = f(x_2)$ gilt dass $x_1 = x_2$.

d) f heißt *surjektiv*, wenn $f(M) = N$, d.h. wenn **jedes** $y \in N$ **mindestens ein Urbild hat**.

e) f heißt *bijektiv* (auch: *eineindeutig*), wenn f injektiv und surjektiv ist, wenn also **jedes** $y \in N$ **genau ein Urbild hat**.

Eine bijektive Abbildung wird auch *Bijektion* genannt.

Bemerkung. Um die Begriffe injektiv, surjektiv, bijektiv sinnvoll verwenden zu können ist es also wichtig, unter einer Funktion nicht einfach nur eine Zuordnungsvorschrift zu verstehen, sondern ein Tripel bestehend aus Zuordnungsvorschrift, Definitionsbereich und Wertevorrat.¹⁰

Beispiel. Betrachte die Abbildung $f : M \rightarrow N$, $f(x) = x^2$, wobei

a) $M = \mathbb{R}$, $N = \mathbb{R}$,

b) $M = \mathbb{R}$, $N = \mathbb{R}_0^+$,

c) $M = \mathbb{R}_0^+$, $N = \mathbb{R}_0^+$.

Im Fall (a) ist f nicht injektiv, denn z.B. zu $x_1 = 1$ und $x_2 = -1$ ist $f(x_1) = f(x_2)$. f ist nicht surjektiv, denn z.B. zu $y = -1 \in N$ gibt es kein Urbild, da $f(x) = x^2$ immer nicht-negativ ist.

Im Fall (b) ist f weiterhin nicht injektiv, aber surjektiv, denn zu jedem $y \geq 0$ kann man (mindestens) ein Urbild x finden (d.h. $f(x) = y$), und zwar $x := \sqrt{y}$.

Im Fall (c) ist f injektiv, denn: Seien $x_1, x_2 \geq 0$. "Ohne Beschränkung der Allgemeinheit" (kurz: o.B.d.A.)¹¹ können wir davon ausgehen, dass $x_1 < x_2$. Wegen der strengen Monotonie von f ist dann $f(x_1) < f(x_2)$, also insbesondere $f(x_1) \neq f(x_2)$, woraus die Injektivität folgt.¹²

f ist (nur) im Fall (c) bijektiv.

Beispiel. Im Einwohnermeldeamt einer Stadt liegt vor: Eine Liste (Datei) aller Einwohner der Stadt und eine Liste (Datei) aller Adressen in der Stadt. Außerdem ist zu jedem Einwohner ein Link auf seine Adresse gelegt. Die Zuordnung eines Einwohners x zu seiner Adresse $f(x)$, wobei Definitionsbereich und Wertevorrat die beiden genannten Listen sind, definiert eine Funktion (wir verwenden dabei: kein Einwohner hat mehr als einen (Haupt-)Wohnsitz). Ist diese Funktion injektiv/surjektiv?

¹⁰Beachte, dass im Finckenstein ein hiervon abweichender Funktionsbegriff verwendet wird.

¹¹Manche Autoren schreiben stattdessen auch "o.E." ("ohne Einschränkung")

¹²Wenn man sich speziell für Funktionen von \mathbb{R} nach \mathbb{R} interessiert (die zudem noch 'hinreichend glatt' sein müssen), so kann die sog. *Ableitung* f' der Funktion (\rightarrow 2. Semester oder Schulmathematik) berechnet werden, um Aussagen über das Monotonieverhalten und damit auch über die Injektivität zu treffen.

Vermutlich ist die Funktion nicht injektiv, denn es wird z.B. Mehrpersonenhaushalte geben. Vermutlich ist die Funktion nicht surjektiv, denn es wird leerstehende Wohnungen oder Bürogebäude geben.

Verkettung von Funktionen. Seien $f : A \rightarrow B$ und $g : C \rightarrow D$ zwei Funktionen und es gelte $B \subseteq C$ (oft: $B = C$). Dann ist offensichtlich durch $x \mapsto g(f(x))$ eine Abbildung von A nach D definiert; diese wird mit $g \circ f$ bezeichnet:

$$g \circ f : A \rightarrow D, \quad x \mapsto (g \circ f)(x) := g(f(x))$$

Die identische Abbildung. Sei $M \neq \emptyset$ eine Menge und $f : M \rightarrow M$ die Abbildung mit $f(x) = x$ für alle $x \in M$. f heißt dann *Identische Abbildung* oder die *Identität* auf M und wird mit Id_M (oder id_M oder I_M oder 1_M) bezeichnet.

Die Umkehrabbildung. Sei $f : M \rightarrow N$ eine Abbildung. Eine Abbildung $g : N \rightarrow M$ heißt *Umkehrabbildung zu f* , wenn

$$\forall x \in M : g(f(x)) = x \quad \wedge \quad \forall y \in N : f(g(y)) = y,$$

also kurz, wenn $g \circ f = \text{Id}_M$ und $f \circ g = \text{Id}_N$. Die Umkehrabbildung wird mit f^{-1} bezeichnet.

Satz. Eine Abbildung f besitzt genau dann eine Umkehrabbildung, wenn f bijektiv ist. In diesem Fall ist dann auch die Umkehrabbildung bijektiv. Existiert eine Umkehrabbildung, so ist sie eindeutig bestimmt, und sie ist ebenfalls bijektiv.

Wir wollen diesen Satz hier nicht streng formal beweisen, sondern nur veranschaulichen:

Die Bijektivität von f bedeutet, dass es zu jedem $y \in N$ genau ein Urbild $x \in M$ gehört. Die Zuordnung $y \mapsto x$, $N \rightarrow M$, definiert gerade die Umkehrabbildung.

Bemerkung. Manchmal liest man, dass schon die Injektivität hinreichend sei für die Existenz einer Umkehrfunktion. Das ist, wenn man Funktionen und Umkehrfunktionen wie oben definiert, nicht korrekt. Lediglich in folgendem Sinne wird daraus eine korrekte Aussage: Ist $f : M \rightarrow N$ injektiv, so hat die Abbildung $f : M \rightarrow \text{Bild}(M)$, die also durch Einschränkung des Wertevorrats entsteht (und die ja trivialerweise dann bijektiv ist) eine Umkehrabbildung (von $\text{Bild}(M)$ nach M).

Neben der Existenz der Umkehrfunktion ist ein weiterer wichtiger Punkt, bei dem die Bijektivität eine Rolle spielt:

Man kann die "Größe" (Mächtigkeit, Kardinalität) von Mengen vergleichen mit Hilfe bijektiver Funktionen:

Def. (Gleichmächtigkeit) Zwei Mengen A und B heißen *gleich mächtig*, wenn es

eine Bijektion von A nach B gibt.¹³

Eine Menge, die gleich mächtig zu \mathbb{N} ist, heißt *abzählbar unendlich*. Eine unendliche Menge, die nicht gleich mächtig zu \mathbb{N} ist, heißt *überabzählbar*.

Beispiele.

- Im Fall einer endlichen Menge A mit, sagen wir, $n \in \mathbb{N}_0$ Elementen, muss dann auch B n Elemente haben, d.h. die Gleichmächtigkeit bedeutet 'gleich viele Elemente'.
- Im Fall unendlicher Mengen betrachten wir folgendes Beispiel:
Die Mengen \mathbb{N} und \mathbb{N}_0 sind, obwohl $\mathbb{N} \subsetneq \mathbb{N}_0$, gleich mächtig: als Bijektion von \mathbb{N}_0 nach \mathbb{N} nehmen wir die Abbildung $n \mapsto n+1$.
Es schließen sich spannende Fragen an: Sind \mathbb{N} und \mathbb{Z} gleich mächtig? \mathbb{Z} und \mathbb{Q} ? \mathbb{Q} und \mathbb{R} ? Dazu mehr in Kapitel 2.

1.5 Kurzer Einblick in die Kombinatorik

Definition (Permutation). Sei $n \in \mathbb{N}$. Eine bijektive Abbildung

$$f : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$$

heißt Permutation (auf der Menge $\{1, 2, \dots, n\}$).

Sei S_n die Menge aller Permutationen auf $\{1, 2, \dots, n\}$. Wie viele solche Permutationen gibt es? Um $f(1)$ festzulegen gibt es n Möglichkeiten. Um danach $f(2)$ festzulegen, gibt es nur noch $n-1$ Möglichkeiten, da die Injektivität von f erfordert, dass $f(2) \neq f(1)$. Für $f(3)$ gibt es $n-2$ Möglichkeiten, usw. Insgesamt kommen wir auf

$$|S_n| = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n =: n! \quad (\text{sprich: } n\text{-Fakultät})$$

Möglichkeiten.¹⁴ Beachte: Man definiert $0! := 1$

Die Anzahl der Permutationen beschreibt die Anzahl der Möglichkeiten, n Objekte anzuordnen/zu sortieren: Die Zahlen 1,2,3 kann man anordnen zu 123, 132, 213, 231, 312, 321; das sind genau $3! = 1 \cdot 2 \cdot 3 = 6$ Möglichkeiten. Diese 6 Anordnungen entsprechen 6 bijektiven Abbildungen (also Permutationen) von $\{1, 2, 3\}$ nach $\{1, 2, 3\}$: "123" entspricht der Permutation f mit $f(1) = 1, f(2) = 2, f(3) = 3$; "132" entspricht der Permutation f mit $f(1) = 1, f(2) = 3, f(3) = 2$, usw.

Es gibt neben der mühsamen Darstellung $f(1) = \dots, f(2) = \dots$ kürzere Notationen für Permutationen, so zum Beispiel die Notation (entspricht einer 'Wertetabelle')

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

¹³Bemerkung: Die 'Gleichmächtigkeit' kann man als Relation zwischen Mengen auffassen. Sie ist reflexiv, symmetrisch und transitiv, hat also die Eigenschaften einer Äquivalenzrelation.

¹⁴die Surjektivität der oben konstruierten Abbildungen f ergibt sich 'von selbst', da Definitionsbereich und Wertevorrat die gleiche Anzahl von Elementen haben.

Definition (Transposition) Eine Permutation, die nur zwei Objekte vertauscht und alle anderen fix (=fest) lässt, heißt *Transposition* (=Vertauschung).

Bsp.: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$ ist eine Transposition.

Man kann zeigen, dass sich jede Permutation f als Verkettung von Transpositionen f_1, \dots, f_m darstellen lässt: $f = f_m \circ \dots \circ f_2 \circ f_1$. Praktische Konsequenz: Man kann eine Liste von n Objekten sortieren (bzw. in eine beliebige Reihenfolge bringen), indem man nur nacheinander jeweils zwei Objekte der Liste vertauscht.

Dies ist interessant für Sortieralgorithmen in der Informatik. Beispiel: Vor mir liegen nebeneinander 750 Klausuren, die ich alphabetisch sortieren will; ich habe nur 2 Hände. Doch diese reichen, denn ich kann die immer wieder Liste durchgehen, und wann immer ich Paare von Klausuren finde, die in der 'falschen' Reihenfolge liegen, vertausche ich diese.¹⁵ Der Begriff des Paares, das in der falschen Reihenfolge liegt, führt auf den Begriff der 'Inversion':

Def. (Inversion, Signum) Sei f eine Permutation auf $\{1, 2, \dots, n\}$. Man nennt ein Paar (i, j) eine Inversion, falls $i < j$ und $f(i) > f(j)$. Das Signum einer Permutation ist definiert als

$$\text{sgn}(f) := (-1)^{N(f)},$$

wobei $N(f)$ die Anzahl der Inversionen von f ist.

Es folgt sofort: Transpositionen haben immer das Signum '-1'.

Nun folgen einige Aufgabenstellungen der Kombinatorik.

Frage 1: Wie viele k -elementige Teilmengen kann man aus einer n -elementigen Menge ($k \leq n$) bilden? Gleichbedeutend: Auf wie viele Arten kann man k Objekte aus einer Menge von n Objekten auswählen (ohne Zurücklegen, ohne Beachtung der Reihenfolge)?

Für das erste der k Objekte hat man n Wahlmöglichkeiten, für das zweite nur noch $n-1$ viele, für das k -te noch $n-k+1$ viele Möglichkeiten. Das ergibt $n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$ viele Möglichkeiten. Jedoch soll es nicht auf die Reihenfolge der gezogenen Objekte ankommen (die Mengen $\{1, 2, 3\}$ und $\{1, 3, 2\}$ sind gleich!) Deshalb müssen wir die obige Anzahl durch die Anzahl aller Anordnungen (Permutationen) von k Elementen, also $k!$, teilen. Wir erhalten als Anzahl

$$\frac{n!}{k! (n-k)!} =: \binom{n}{k} \quad (\text{sprich: } n \text{ über } k)$$

Dieser Ausdruck wird auch *Binomialkoeffizient* genannt (Grund dafür: später, Übung).

Bsp.: Wie viele Möglichkeiten gibt es, 2-elementige Teilmengen aus einer 4-elementigen Menge zu bilden? $\binom{4}{2} = \frac{4!}{2!2!} = \frac{4 \cdot 3 \cdot 2}{2 \cdot 2} = 6$. In der Tat:

¹⁵dies ist nicht unbedingt die effizienteste Sortiermethode

$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$.

Frage 2: Wie viele k -Tupel (das ist die Verallgemeinerung von Paar=2-Tupel, Tripel=3-Tupel) kann man aus einer n -elementigen Menge auswählen? (Entspricht: Ziehen mit Zurücklegen mit Beachtung der Reihenfolge)

Antwort: Für jede der k Komponenten des k -Tupels hat man offenbar n Möglichkeiten, also insgesamt n^k viele.

Frage 3: Wie viele k -Tupel kann man aus einer n -elementigen Menge auswählen, wenn die Komponenten des k -Tupels paarweise verschieden sein sollen? (Entspricht: Ziehen ohne Zurücklegen mit Beachtung der Reihenfolge)

Die Antwort hatten wir uns oben unter Frage bereits als Zwischenergebnis überlegt: Es gibt $\frac{n!}{(n-k)!}$ viele Möglichkeiten.

Zur Übung: wie viele injektive Abbildungen aus einer k -elementigen Menge in eine n -elementige Menge gibt es?

2 Zahlensysteme

2.1 Die natürlichen und die ganzen Zahlen; Gruppen, Ringe, Körper

Der bekannteste Zugang zu den natürlichen Zahlen ist der axiomatische Zugang nach Peano aus dem 19. Jahrhundert:

Def. (Die Peano-Axiome der Natürlichen Zahlen)¹⁶ Eine Menge \mathbb{N} heißt Menge der natürlichen Zahlen, falls gilt:

1. Jedem Element der Menge $n \in \mathbb{N}$ ist genau ein Element $f(n) \in \mathbb{N}$ dieser Menge zugeordnet; der sogenannte *Nachfolger* von n .
(Kurz: Es gibt eine Abbildung $f : \mathbb{N} \rightarrow \mathbb{N}$.)
2. Es gibt ein Element von \mathbb{N} , genannt "1", welches kein Nachfolger irgendeines Elementes von \mathbb{N} ist.
(Kurz: $\exists 1 \in \mathbb{N} : 1 \notin f(\mathbb{N})$.)
3. Sind $n, m \in \mathbb{N}$ mit $n \neq m$, so ist $f(n) \neq f(m)$.
Kurz: Verschiedene Zahlen haben verschiedene Nachfolger, d.h.: f ist injektiv.
4. Ist $M \subseteq \mathbb{N}$ mit den Eigenschaften
 - (a) $n \in M \Rightarrow f(n) \in M$ (mit jedem Element von M ist auch dessen Nachfolger in M) und

¹⁶Giuseppe Peano: 1858-1932

(b) $1 \in M$,

so gilt $M = \mathbb{N}$.

Mit den Peano-Axiomen kann man folgern, dass

$$\mathbb{N} = \{1, f(1), f(f(1)), f(f(f(1))), \dots\}$$

gilt, dass die so aufgeführten Elemente tatsächlich (was unsere Definition von Mengen ja erfordert) wohlunterschieden sind, und dass die Menge unendlich viele Elemente enthält.

Die obige Schreibweise ist natürlich ziemlich unpraktisch, weswegen wir in Zukunft $2 := f(1)$, $3 := f(2) = f(f(1))$ usw. verwenden wollen.

z.Ü.: Das vierte Peano-Axiom klingt deutlich komplizierter als die übrigen drei. Ist es wirklich nötig, um die Menge der natürlichen Zahlen zu charakterisieren? Dazu die folgende Aufgabe: Geben Sie eine Zahlenmenge an, die die Axiome 1.-3. erfüllt, nicht aber 4. Analog kann man sich fragen, weshalb es notwendig ist, 2. oder 3. zu fordern (d.h. welche Mengen man bekommen könnte, wenn man eines der Axiome weglässt).

Die Konstruktion der natürlichen Zahlen aus Sicht der axiomatischen Mengenlehre.

Nach Peano verzichtet man also auf eine *Konstruktion* der natürlichen Zahlen aus Bekanntem; man nimmt einfach an, dass eine Menge mit den oben genannten Eigenschaften existiert, und betreibt Mathematik unter dieser Annahme. Das bedeutet letztendlich, dass man die Existenz einer Menge \mathbb{N} mit obigen Eigenschaften als zusätzliches Axiom den Axiomen der Mengenlehre hinzufügt. Eine *Konstruktion* der natürlichen Zahlen unter Verwendung der (axiomatischen) Mengenlehre erfolgte historisch gesehen erst später (20. Jhdt.). Man kann dazu wie folgt vorgehen: Wir haben Axiome der Mengenlehre zur Verfügung, die uns sagen, dass die leere Menge \emptyset existiert, sowie dass, wenn M eine Menge ist, auch $M \cup \{M\}$ eine Menge ist. Somit existieren also die Mengen $M_0 = \emptyset$, $M_1 = M_0 \cup \{M_0\} = \{\emptyset\}$, $M_2 = M_1 \cup \{M_1\} = \{\emptyset, \{\emptyset\}\}$, $M_3 = M_2 \cup \{M_2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots$ Man erkennt, dass all diese so konstruierten Mengen paarweise verschieden sind (dies erkennt man an ihrer Elementzahl; M_n hat genau n Elemente). Jede dieser Mengen M hat eine 'Nachfolgemenge' $M \cup \{M\}$, und alle weiteren Peano-Axiome sind ebenfalls erfüllt. Man führt nun neue Symbole ein: $0 := \emptyset$, $1 := \{\emptyset\}$, $2 := \{\emptyset, \{\emptyset\}\}$ usw.

Auf diese Art und Weise kann man aus Axiomen der axiomatischen Mengenlehre also beweisen, dass es eine Menge gibt mit den Eigenschaften, die Peano gefordert hat, und muss die Existenz einer solchen Menge \mathbb{N} nicht als zusätzliches Axiom fordern.

Kurzer Einschub zur Notation: Für Summationen gibt es die Kurzschreibweise

$$\sum_{k=m}^n a_k := a_m + a_{m+1} + \dots + a_n \quad (\text{für } n \geq m).$$

Analog für Produkte

$$\prod_{k=m}^n a_k := a_m \cdot a_{m+1} \cdot \dots \cdot a_n \quad (\text{für } n \geq m).$$

Beispiel: $\sum_{k=1}^n k^2 = 1^2 + 2^2 + \dots + n^2$

Folgerungen aus dem letzten Peano-Axiom.

Aus dem Axiom 4. folgt das sogenannte **(Beweis-)Prinzip der Vollständigen Induktion**:

Gesetzt den Fall es ist eine Aussage gegeben, die von einem Parameter $n \in \mathbb{N}$ abhängt.

Diese bezeichnen wir mit $A(n)$. [Beispiel: $A(n) := \left(\sum_{k=0}^n k = \frac{n(n+1)}{2} \right)$.]

Aufgabe sei es, zu zeigen, dass diese Aussage für alle $n \in \mathbb{N}$ wahr ist. Wir könnten anfangen zu zeigen, dass die Aussage $A(1)$ wahr ist, anschließend, dass die Aussage $A(2)$ wahr ist, usw. Jedoch würde diese Vorgehensweise unendlich viele Beweise erfordern, und soviel Zeit haben wir nicht. Stattdessen verwenden wir das letzte Peano-Axiom. Wir setzen M als die Menge aller Zahlen n , für die $A(n)$ wahr ist. Wir müssen zeigen, dass $M = \mathbb{N}$ ist; dann sind wir fertig. Das 4. Peano-Axiom besagt, dass wir dazu zeigen müssen:

(I.) $1 \in M$, also: $A(1)$ ist wahr.

(II.) wenn $n \in M$, dann ist auch $f(n) = n+1 \in M$, also: Unter der Voraussetzung, dass $A(n)$ wahr ist, ist auch $A(n+1)$ wahr.

Den ersten Schritt, zu zeigen, dass $A(1)$ wahr ist, nennt man *Induktionsanfang* oder *Induktionsverankerung*. Den zweiten Schritt, dass unter der Voraussetzung $A(n)$ auch $A(n+1)$ gilt, nennt man den *Induktionsschritt*. Innerhalb des Induktionsschritts wird $A(n)$ als *Induktionsvoraussetzung* bezeichnet.

Formelmäßig lautet das Prinzip der Vollständigen Induktion:

$$\underbrace{A(1)}_{\text{Ind.-anfang}} \quad \wedge \quad \underbrace{(\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1))}_{\text{Induktionsschritt}} \quad \Longrightarrow \quad \underbrace{\forall n \in \mathbb{N} : A(n)}_{\text{zu beweisende Aussage}}$$

Anwendungsbeispiel. Beweise, dass für alle $n \in \mathbb{N}$ gilt: $\sum_{k=1}^n k = \frac{n(n+1)}{2}$.¹⁷

Induktionsanfang ($n=1$): Es ist $\sum_{k=1}^1 k = 1$ und $\frac{1(1+1)}{2} = 1$; die Aussage ist also für $n=1$

¹⁷Der Legende nach hat Carl Friedrich Gauß als Grundschüler diese Formel sich überlegt, als sein Lehrer, der die Schüler still beschäftigen wollte, die Aufgabe stellte, alle Zahlen von 1 bis 100 zu addieren. Der kleine Gauß erkannte: Durch Umordnung der Summe müssen wir 1 und n , sowie 2 und $n-1$, sowie 3 und $n-2$ usw. addieren, also jeweils $k + (n-k+1) = n+1$, und zwar $\frac{n}{2}$ mal (denn so viele Paare gibt es), also $\frac{n}{2}(n+1)$. Man kann die Formel also auch *ohne* vollständige Induktion beweisen.

wahr.

Induktionsschritt ($n \rightarrow n+1$): Es gelte $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ (Dies ist die Induktionsvoraussetzung (I.V.).)

Es ist zu zeigen, dass $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$ gilt (dies ist die Aussage $A(n+1)$).

Dazu rechnen wir:

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^n k + (n+1) \stackrel{\text{I.V.}}{=} \frac{n(n+1)}{2} + n+1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+2)(n+1)}{2}$$

An der mit "I.V." gekennzeichneten Stelle ging die Induktionsvoraussetzung ein. \square

Rechenoperationen auf \mathbb{N} . Auf der Menge \mathbb{N} wollen wir natürlich, wie wir es gewohnt sind, auch rechnen, d.h. zunächst einmal addieren und multiplizieren können. Addition und Multiplikation können wir als Abbildungen

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad \cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

auffassen (d.h. die Summe bzw. das Produkt zweier natürlicher Zahlen soll wieder eine natürliche Zahl sein). Wie können wir diese beiden Abbildungen *definieren*? Dazu können wir uns wieder des Prinzips der Vollständigen Induktion bedienen. Um $m+n$ für beliebige $m, n \in \mathbb{N}$ zu definieren können wir zunächst $m+n$ nur für den Fall $n=1$ (und $m \in \mathbb{N}$ beliebig) definieren, und zwar, mit der Schreibweise von Peano, als

$$m+1 := f(m) \quad (*)$$

für alle $m \in \mathbb{N}$. Anschließend legen wir fest: Falls die Addition von $m+n$ bereits definiert ist, so sei die Addition von $m+(n+1)$ (also $m+f(n)$) ("rekursiv") definiert als

$$m+f(n) := f(m+n) \quad (**)$$

für alle $m \in \mathbb{N}$. Also, wir wollen mal unter ausschließlicher Verwendung unserer Definitionen $4+3$ berechnen:

$4+3 = 4+f(2) \stackrel{(**)}{=} f(4+2) = f(4+f(1)) \stackrel{(**)}{=} f(f(4+1)) \stackrel{(*)}{=} f(f(f(4))) = f(f(5)) = f(6) = 7$, wobei an den gekennzeichneten Stellen (*) und (**) sowie an den übrigen Stellen die Definition von $3 := f(2)$ usw verwendet wurde.

Ähnlich kann man vorgehen zur Definition der Multiplikation. Wir definieren

$$\forall m \in \mathbb{N} : m \cdot 1 := m$$

sowie rekursiv

$$\forall m \in \mathbb{N} : m \cdot f(n) := m \cdot n + m.$$

Wir wollen uns nun mit **Eigenschaften von Verknüpfungen** beschäftigen:

Def. Sei $M \neq \emptyset$ eine Menge und $* : M \times M \longrightarrow M$ eine Abbildung ('Verknüpfung auf M '). ' $*$ ' heißt

- *kommutativ*, falls $\forall a, b \in M : a * b = b * a$
- *assoziativ*, falls $\forall a, b, c \in M : (a * b) * c = a * (b * c)$

Bemerkung: Ist eine Verknüpfung assoziativ, so können wir die Klammern auch weglassen: $a * b * c := (a * b) * c = a * (b * c)$.

Wir können nun *beweisen*:

Satz: Addition und Multiplikation auf \mathbb{N} sind kommutativ und assoziativ.

Wir überspringen aus Zeitgründen den Beweis der Kommutativität und wollen uns darauf beschränken, die Assoziativität von $+$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ zu zeigen.

Beweis per Induktion. Wir setzen $A(c) := [\forall a, b \in \mathbb{N} : (a + b) + c = a + (b + c)]$:

Induktionsanfang ($c=1$):

Für beliebiges $a, b \in \mathbb{N}$ gilt $(a + b) + 1 = f(a + b) \stackrel{(**)}{=} a + f(b) = a + (b + 1)$

Induktionsschritt ($c \rightarrow c+1$):

Es gelte $(a + b) + c = a + (b + c)$ für ein $c \in \mathbb{N}$ und alle $a, b \in \mathbb{N}$. Zu zeigen: Dann gilt auch $(a + b) + f(c) = a + (b + f(c))$. Beweis:

$$(a + b) + f(c) \stackrel{(**)}{=} f((a + b) + c) \stackrel{\text{I.V.}}{=} f(a + (b + c)) \stackrel{(**)}{=} a + f(b + c) \stackrel{(**)}{=} a + (b + f(c)) \quad \square$$

Bemerkung. Offensichtlich können wir leicht die auf \mathbb{N} definierten Verknüpfungen $'+'$ und $'\cdot'$ auf $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ erweitern durch Setzung von

$$n + 0 := 0 + n := n, \quad n \cdot 0 := 0 \cdot n := 0$$

für alle $n \in \mathbb{N}_0$; $f(0) := 1$. Die Abbildungen

$$+, \cdot : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

sind dann ebenfalls kommutativ und assoziativ.

Def. (neutrales Element, inverses Element) Sei M eine nichtleere Menge und $*$: $M \times M \rightarrow M$ eine Abbildung.

- (a) Ein Element $e \in M$ heißt *neutrales Element* von M bezüglich $'*'$ (kurz: neutrales Element in $(M, *)$), wenn

$$\forall x \in M : e * x = x * e = x.$$

- (b) Sei e neutrales Element von $(M, *)$ und sei $x \in M$. $y \in M$ heißt *inverses Element* von x in $(M, *)$, wenn

$$x * y = y * x = e.$$

Schreibweise: Ein Inverses zu x wird mit x^{-1} oder mit $-x$ bezeichnet.

Beispiele. $(\mathbb{N}_0, +)$ hat offensichtlich als neutrales Element 0; (\mathbb{N}_0, \cdot) hat als neutrales Element 1; $(\mathbb{N}, +)$ hat kein neutrales Element.

0 hat in $(\mathbb{N}_0, +)$ ein inverses Element 0; die übrigen Elemente von \mathbb{N}_0 haben kein Inverses in \mathbb{N}_0 ! In (\mathbb{N}, \cdot) hat lediglich das Element 1 ein Inverses. Um inverse Elemente zu bekommen, werden wir zu \mathbb{N}_0 weitere Zahlen hinzunehmen müssen: Die negativen ganzen Zahlen, um Inverse bzgl. '+' zu bekommen, und Brüche (rationale Zahlen), um Inverse bzgl. '\cdot' zu bekommen; siehe später.

Frage: Sind neutrale und inverse Elemente immer eindeutig bestimmt? Dazu der folgende

Satz. Sei M eine nichtleere Menge und $* : M \times M \rightarrow M$ eine Abbildung.

- (a) Dann gibt es in M höchstens ein neutrales Element bzgl. '*'.
- (b) Wenn '*' assoziativ ist und ein neutrales Element hat, dann hat jedes $x \in M$ höchstens ein inverses Element.

Beweis.

- (a) Seien sowohl e als auch \tilde{e} neutrale Elemente in $(M, *)$. (z.z.: $e = \tilde{e}$)
Da \tilde{e} neutrales Element, gilt $e = e * \tilde{e}$. Da e neutrales Element ist, gilt $\tilde{e} = e * \tilde{e}$.
Insgesamt also $e = e * \tilde{e} = \tilde{e}$.
- (b) Sei $x \in M$ und seien sowohl y als auch \tilde{y} inverse Elemente von x . Dann gilt:

$$y = y * e = y * (x * \tilde{y}) = (y * x) * \tilde{y} = e * \tilde{y} = \tilde{y}$$

□

Def. (Gruppe) Sei M eine Menge und $* : M \times M \rightarrow M$ eine Abbildung. $(M, *)$ heißt *Gruppe*, wenn

- (i) $(M, *)$ assoziativ ist,
- (ii) $(M, *)$ ein neutrales Element hat, und
- (iii) in $(M, *)$ jedes Element ein Inverses hat.

Falls $(M, *)$ zusätzlich kommutativ ist, heißt $(M, *)$ *kommutative* oder *Abelsche Gruppe*¹⁸.

Bemerkung. Nach obigem Satz wissen wir, dass in Gruppen neutrales und inverse Elemente immer eindeutig sind.

¹⁸Niels Henrik Abel, Norwegischer Algebraiker, 1802-1829. U.a. bewies er im Alter von nur 22 Jahren, dass es keine allgemeine Formel für Nullstellen von Polynomen fünften Grades geben kann.

Beispiel. Endliche Gruppen (d.h. Gruppen mit endlich vielen Elementen) kann man mit Hilfe einer *Verknüpfungstabelle* darstellen. Z.B. ist die Menge $G = \{e, b, c\}$ mit der durch die folgende Tabelle beschriebene Verknüpfung eine Gruppe:

$*$	e	b	c
e	e	b	c
b	b	c	e
c	c	e	b

Man sieht, dass e das neutrale Element ist (s. 1. Zeile u. 1. Spalte) und dass $b^{-1} = c$ und $c^{-1} = b$ ist. Man kann diese Gruppe übrigens auch durch Umbenennen der Elemente als $G = \{0, 1, 2\}$ mit der Verknüpfungstabelle

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

darstellen; die Verknüpfung entspricht gerade der Addition ganzer Zahlen 'modulo 3'! z.Ü.: Wie viele mögliche Verknüpfungstabellen gibt es für eine 4-elementige Gruppe $G = \{e, b, c, d\}$, wobei o.B.d.A. e das neutrale Element sei?

Zurück zu \mathbb{N} :

Wie wir uns bereits überlegt haben (fehlende Inverse!) sind $(\mathbb{N}_0, +)$ und (\mathbb{N}_0, \cdot) keine Gruppen; um Gruppenstrukturen zu erhalten, müssen wir unsere Zahlenmenge erweitern: Wir nehmen zusätzliche Objekte $-1, -2, -3, \dots$ hinzu¹⁹ und bekommen so die Menge

$$\mathbb{Z} := \mathbb{N}_0 \cup \mathbb{N}^- := \{0, 1, 2, 3, 4, \dots\} \cup \{-1, -2, -3, \dots\},$$

wobei wir fordern, dass $-n$ das Additiv-Inverse (d.h. das Inverse bzgl. '+') von $n \in \mathbb{N}$ ist. Die Addition und die Multiplikation, die wir auf \mathbb{N}_0 kennen, lässt sich auf \mathbb{Z} erweitern, so dass die erweiterten Verknüpfungen $+, \cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ebenfalls assoziativ und kommutativ sind. Da, anders als in \mathbb{N} , jedes Element n in $(\mathbb{Z}, +)$ ein Inverses $-n$ hat, **ist $(\mathbb{Z}, +)$ eine (Abelsche) Gruppe.**

Zur Schreibweise: Anstelle von $m + (-n)$ schreiben wir auch kurz $m - n$.

Die Existenz von additiv-inversen Elementen hat zur Folge, dass wir in \mathbb{Z} (anders als in \mathbb{N}) Gleichungen der Art

$$a + x = b \quad (a, b \text{ gegeben})$$

immer lösen können. Wir addieren dazu auf beiden Seiten der Gleichung das Additiv-Inverse von a und erhalten

$$(-a) + a + x = (-a) + b$$

¹⁹Falls es Sie interessiert, "wo diese neuen Elemente herkommen", d.h. ob man die Menge \mathbb{Z} oder $(\mathbb{Z}, +)$ auch formal *konstruieren* kann (z.B. aus $(\mathbb{N}_0, +)$): Eine Möglichkeit der Konstruktion zeigt Aufgabe P-6-b.

also $x = b + (-a) = b - a$.

Def. (Primzahl) Eine Zahl $n \in \mathbb{N}$ heißt Primzahl, wenn n genau zwei Teiler in \mathbb{N} hat (nämlich n und 1).

Äquivalent: Wenn aus $n = k_1 k_2$ mit $k_1, k_2 \in \mathbb{N}$ folgt: Entweder $k_1 = 1$ oder $k_2 = 1$.

Bemerkung: 1 ist keine Primzahl.

Satz. Jede Zahl $n \in \mathbb{N} \setminus \{1\}$ lässt sich als Produkt $n = p_1 \cdot \dots \cdot p_m$ von $m \in \mathbb{N}$ Primzahlen schreiben, und diese Darstellung ist – bis auf Reihenfolge der Faktoren – eindeutig.

Beweis: Erfolgt mit vollständiger Induktion nach n .

Satz. Es gibt unendlich viele Primzahlen.²⁰

Der Beweis erfolgt als sog. Widerspruchsbeweis: Die Annahme, dass es nur endlich viele Primzahlen $p_1 < \dots < p_n$ gibt, führt auf einen Widerspruch: Die Zahl $z := p_1 \cdot \dots \cdot p_n + 1$ ist 'offensichtlich' nicht durch p_1, \dots, p_n teilbar. Da außerdem $z > p_n$ ist, ist aber z auch keine Primzahl. Nach dem Satz über die Primfaktorzerlegung muss, da z nicht prim ist, z als Produkt von (mindestens zwei) Primzahlen darzustellen sein. Diese beiden Primzahlen können, da z nicht durch p_1, \dots, p_n teilbar ist, nicht in der Liste der Primzahlen p_1, \dots, p_n vorkommen. Widerspruch. \square

(\mathbb{Z}, \cdot) ist zwar keine Gruppe (fehlende Inverse!), jedoch hat $\mathbb{Z}, +, \cdot$ Eigenschaften, die mit dem Begriff 'Ring' belegt sind:

Def. (Ring)²¹ Sei M eine Menge und seien $+, \cdot : M \times M \rightarrow M$ zwei Verknüpfungen. $(M, +, \cdot)$ heißt *Ring*, falls

- (i) $(M, +)$ eine Abelsche Gruppe ist, und
- (ii) (M, \cdot) assoziativ ist, und
- (iii) falls die Distributivgesetze

$$\forall a, b, c \in M : a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

gelten.

Der Ring heißt *kommutativ*, falls \cdot kommutativ ist.

Hat der Ring ein neutrales Element bzgl. \cdot , so wird er *Ring mit Eins(element)* genannt.

Beispiele.

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement.
2. Auf $M := \{0\}$ definieren wir $0+0 := 0$ und $0 \cdot 0 := 0$. Dann ist $(M, +, \cdot)$ ein kommutativer Ring mit Einselement.

²⁰Dieser Satz und sein Beweis waren schon in der Antike bekannt.

²¹Das Konzept des Rings wurde eingeführt von Richard Dedekind und David Hilbert.

3. Die Menge aller Polynome mit Koeffizienten in \mathbb{Z} ist bezüglich der üblichen Addition und Multiplikation von Funktionen ein kommutativer Ring mit Eins.

Schreibweise: Selbst wenn wir andere Ringe als \mathbb{Z} betrachten, so wird doch oft das additiv-neutrale Element mit dem Symbol '0' und das multiplikativ-neutrale Element mit dem Symbol '1' bezeichnet.

Beachte: In Ringen haben die Elemente also i.a. keine multiplikativ-Inversen. Haben jedoch in einem kommutativen Ring mit Einselement alle Elemente mit Ausnahme des additiv-neutralen Elementes ein multiplikativ-inverses Element, so sprechen wir von einem 'Körper':

Def. (Körper) Ein Ring $(M, +, \cdot)$, bei dem $(M \setminus \{0\}, \cdot)$ eine Abelsche Gruppe ist, heißt *Körper*.

$(M, +, \cdot)$ ist also genau dann ein Körper, wenn $(M, +)$ und $(M \setminus \{0\}, \cdot)$ Abelsche Gruppen sind und zwischen '+' und '.' Distributivgesetze gelten.

Beispiel. \mathbb{Q} , die Menge der rationalen Zahlen (die Menge der Brüche), ist mit der 'üblichen' Addition und Multiplikation ein Körper. Dagegen ist $(\mathbb{Z}, +, \cdot)$ kein Körper. Was \mathbb{Q} eigentlich ist, wollen wir im folgenden Kapitel klären:

2.2 Die rationalen Zahlen

Die Menge der rationalen Zahlen ist die Menge aller 'Brüche' und wird mit \mathbb{Q} bezeichnet. Wir wollen versuchen, diese Menge zu *konstruieren* unter Verwendung der ganzen Zahlen. Ein erster Versuch könnte sein:

Da Brüche offenbar aus zwei Zahlen, Zähler und Nenner, 'zusammengesetzt' sind, könnte man versuchen, die Menge der Brüche als *Menge von Paaren von ganzen Zahlen* aufzufassen, also

$$\frac{p}{q} \stackrel{???}{:=} (p, q), \quad \text{wobei } p \in \mathbb{Z}, q \in \mathbb{N}; \quad \mathbb{Q} \stackrel{???}{:=} \{(p, q) \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$$

zu setzen. (Man könnte genau so gut auch $q \in \mathbb{Z} \setminus \{0\}$ statt $q \in \mathbb{N}$ nehmen.)

Leider ist dies unbefriedigend, denn z.B. für Paare gilt $(3, 4) \neq (6, 8)$, d.h. wir bekämen für unsere Brüche $\frac{3}{4} \neq \frac{6}{8}$! Wir müssen dafür sorgen, dass alle Paare, deren zugehöriger Bruch den gleichen Wert ergeben soll, miteinander 'identifiziert' werden. Wie kann das geschehen? Die grundlegende Idee ist: Wir fassen alle Zahlenpaare, die den gleichen Bruch repräsentieren sollen, zu *Klassen* zusammen. Das bedeutet: Wir definieren auf der Menge der Paare $\mathbb{Z} \times \mathbb{N}$ eine Äquivalenzrelation, so dass Paare genau dann in Relation stehen, wenn sie den gleichen Bruch repräsentieren. Die zugehörigen Klassen sind dann gerade die gesuchten. Die Menge der Klassen 'ist' dann \mathbb{Q} (per Definition). Zunächst einmal wollen wir die Eigenschaft, dass zwei Brüche gleich sind, formulieren ohne Verwendung von Bruchstrichen, d.h. ohne Division. Das ist ganz einfach:

$$\frac{p}{q} = \frac{r}{s} \iff p \cdot s = r \cdot q$$

Nun definieren wir dementsprechend eine *Relation* \sim auf der Menge der Paare $\mathbb{Z} \times \mathbb{N}$:
Für alle $(p, q), (r, s) \in \mathbb{Z} \times \mathbb{N}$ sei

$$(p, q) \sim (r, s) \quad :\iff \quad p \cdot s = r \cdot q$$

Man kann leicht zeigen, dass die Relation eine *Äquivalenzrelation* ist, d.h. nach dem betreffenden Satz aus Kap.1.3 wird von dieser Relation die Menge $\mathbb{Z} \times \mathbb{N}$ in *Äquivalenzklassen* eingeteilt.

Diese Menge von Äquivalenzklassen bezeichnen wir mit \mathbb{Q} :

$$\mathbb{Q} := \{[(p, q)]_{\sim} \mid (p, q) \in \mathbb{Z} \times \mathbb{N}\}$$

Für die Elemente dieser Menge führen wir die Schreibweise als 'Bruch' ein:

$$\frac{p}{q} := [(p, q)]_{\sim}$$

Die Gleichheit von Brüchen wie z.B. $\frac{3}{4}$ und $\frac{6}{8}$ haben wir somit erreicht, denn:

$$\frac{p}{q} = \frac{r}{s} \quad \Leftrightarrow \quad [(p, q)]_{\sim} = [(r, s)]_{\sim} \quad \Leftrightarrow \quad (p, q) \sim (r, s) \quad \Leftrightarrow \quad ps = rq$$

Zur Veranschaulichung: z.B. stehen zu $(3, 4)$ die Elemente $(6, 8), (9, 12), \dots$, in Relation, d.h. diese Paare sind in der Klasse von $(3, 4)$, d.h. $\frac{3}{4} = [(3, 4)]_{\sim} = \{(3, 4), (6, 8), (9, 12), \dots\}$

Auf dieser zunächst noch recht abstrakten Menge \mathbb{Q} wollen wir auch rechnen, d.h. wir wollen eine Addition und eine Multiplikation erklären, und zwar so, dass wir genau so rechnen können, wie wir es gewohnt sind. Wir definieren also $+, \cdot : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ mittels²²

$$[(p, q)]_{\sim} + [(r, s)]_{\sim} := [(ps + rq, qs)]_{\sim} \quad \text{und} \quad [(p, q)]_{\sim} \cdot [(r, s)]_{\sim} := [(pr, qs)]_{\sim},$$

d.h. also in unserer Bruch-Schreibweise

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

Man kann nun zeigen, dass die so definierte Struktur $(\mathbb{Q}, +, \cdot)$ in der Tat ein Körper ist. So ist z.B. $\frac{0}{1} = \frac{0}{2} = \dots$ das additiv-neutrale Element, $\frac{1}{1} = \frac{2}{2} = \dots$ ist das multiplikativ-neutrale Element, $\frac{-p}{q} = \frac{p}{-q}$ ist das additiv-inverse von $\frac{p}{q}$, und $\frac{q}{p}$ ist das multiplikativ-inverse von $\frac{p}{q}$. Wenn wir von \mathbb{Q} die Teilmenge $\{[(p, 1)]_{\sim} \mid p \in \mathbb{Z}\}$, also alle Brüche mit Nenner=1, betrachten, und die oben auf \mathbb{Q} definierte Addition und Multiplikation auf diese Teilmenge einschränken, so erhalten wir eine Menge, die, inklusive Additions- und Multiplikationsverknüpfung, genau die Eigenschaften von $(\mathbb{Z}, +, \cdot)$ aus Kapitel 2.1 hat; in diesem Sinne können wir \mathbb{Z} als Teilmenge von \mathbb{Q} betrachten.

²²Strenggenommen müssten wir hier prüfen, dass diese Definition 'wohldefiniert' ist, d.h. dass wenn wir auf der linken Seite andere Repräsentanten der selben Klassen wählen, auf der rechten Seite unverändert die gleiche Klasse herauskommt.

Auf der Menge \mathbb{Q} können wir eine Relation \leq definieren mittels²³

$$\frac{p}{q} \leq \frac{r}{s} \quad :\iff \quad ps \leq rq$$

(wobei rechts die ' \leq '-Relation auf \mathbb{Z} gemeint ist). Man kann zeigen, dass ' \leq ' eine totale Ordnungsrelation auf \mathbb{Q} darstellt:

$(\mathbb{Q}, +, \cdot, \leq)$ ist ein total geordneter Körper.

In \mathbb{Q} (allgemein in beliebigen Körpern) können wir, insbesondere Dank der Existenz von multiplikativ-inversen Elementen, Gleichungen der Art

$$a \cdot x = b \quad (a, b \text{ gegeben}),$$

sofern $a \neq 0$, immer lösen: Multiplikation obiger Gleichung mit dem multiplikativ-inversen a^{-1} von a liefert $a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b$, also $(a^{-1} \cdot a) \cdot x = a^{-1} \cdot b$, also $x = a^{-1} \cdot b$.

2.3 Die reellen Zahlen

Wir haben die Menge der rationalen Zahlen konstruiert um Gleichungen der Art $a+x = b$ sowie $a \cdot x = b$ (für $a \neq 0$) lösen zu können. Reicht das? Oder gibt es Gleichungen, die wir nach wie vor nicht lösen können? Können wir die Gleichung

$$x \cdot x = a \quad (a \in \mathbb{Q} \text{ gegeben})$$

immer lösen? Wir wollen uns zunächst mal auf den Fall $a \geq 0$ beschränken.

Dazu gibt es folgenden wichtigen Sachverhalt, der (inkl. eines Beweises) bereits in der Antike entdeckt wurde:

Satz. Es gibt kein $x \in \mathbb{Q}$, so dass $x \cdot x = 2$ ist.

Bemerkung. Das bedeutet, dass die Länge der Diagonale eines Quadrates, dessen Kantenlänge 1 ist, keine rationale Zahl ist.

Beweis des Satzes. Beweis durch Widerspruch. Angenommen, es gibt ein $x \in \mathbb{Q}$ mit $x^2 = 2$. O.B.d.A. können wir annehmen, dass $x > 0$. (denn wenn $x < 0$ eine Lösung ist, so ist auch $-x > 0$ eine Lösung). Wir können dann $x = \frac{p}{q}$ schreiben, wobei $p \in \mathbb{Z}$ und $q \in \mathbb{N}$. (Es ist also $x \cdot q = p$, und da x und q positiv ist, muss auch p positiv sein.)

Wir wollen nun außerdem voraussetzen, dass p und q teilerfremd sind, d.h. falls p und q einen gemeinsamen Teiler $p = \tilde{p}t$, $q = \tilde{q}t$ haben, teilen wir durch diesen, und das wird

²³Dies ist die einzige Stelle, in der es von Nutzen ist, dass wir uns bei den Nennern auf *positive* ganze Zahlen beschränkt haben.

so oft wiederholt, bis kein gemeinsamer Teiler mehr vorhanden ist.²⁴ Die Gleichung $x^2 = 2$ schreiben wir als $\frac{p^2}{q^2} = 2$, also

$$p^2 = 2q^2.$$

Auf der rechten Seite der Gleichung steht offensichtlich eine gerade Zahl, also, muss auch p^2 ein Vielfaches von 2 sein. Also muss auch p ein Vielfaches von 2 sein. Wir können also p als $p = 2\tilde{p}$ schreiben, wobei $\tilde{p} \in \mathbb{N}$. Wir setzen dies ein und erhalten $4\tilde{p}^2 = 2q^2$, also

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

Hieraus folgt wiederum, dass zunächst q^2 und somit auch q durch 2 teilbar ist, also sich schreiben lässt als $q = 2\tilde{q}$ mit $\tilde{q} \in \mathbb{N}$. Dies ist ein Widerspruch zu unserer Voraussetzung, dass p, q das kleinste Zahlenpaar mit $\frac{p}{q} = x$ ist. Also muss die Annahme, es gebe ein $x \in \mathbb{Q}$ mit $x^2 = 2$, falsch sein. \square

Offenbar war in der antiken Gemeinschaft der Pythagoreer die Ansicht weit vertreten, dass sich alle Phänomene und Erscheinungen der Welt mit ganzen Zahlen und den Verhältnissen ganzer Zahlen (Brüche) beschreiben lässt; die obige Erkenntnis soll der Legende nach eine Grundlagenkrise ausgelöst haben; angeblich war man über den Tod durch Ertrinken des angeblichen Entdeckers dieser Tatsache, Hippasos von Metapont, während einer Schiffsreise, eher erfreut als betrübt.

Eng mit dem Problem der Nichtexistenz von Lösungen der Gleichung $x^2 = 2$ in \mathbb{Q} ist auch das antike Problem der sog. (*In-*)*Kommensurabilität* verknüpft. Die Frage lautet (in geometrischer Form): Kann man für zwei beliebige Strecken immer ein "gemeinsames Maß" finden, in dem sich beide Strecken messen lassen, d.h. gibt es für zwei Strecken der Länge x und y immer eine Größe L_0 (das gemeinsame Maß), so dass sich beide Streckenlängen als ganzzahlige Vielfache von L_0 darstellen lassen: $x = m \cdot L_0$ und $y = n \cdot L_0$ mit $m, n \in \mathbb{N}$? Nehmen wir für die Strecken x und y die Kantenlänge und die Diagonale eines Quadrates, so sehen wir ein, dass die Antwort negativ ausfallen muss: Wir haben oben bewiesen, dass dieses Verhältnis $\frac{y}{x}$ keine rationale Zahl ist; gäbe es jedoch ein gemeinsames Maß L_0 , so wäre $\frac{x}{y} = \frac{m \cdot L_0}{n \cdot L_0} = \frac{m}{n} \in \mathbb{Q}$, Widerspruch.

Wir haben zu recht den Eindruck, dass Diagonalen von Quadraten zu wichtig sind, als dass wir auf ihre mathematische Beschreibung verzichten können. In einer Welt, in der wir mathematisch die Diagonalen von Quadraten nicht 'fassen' können, wollen wir nicht leben. Daher wollen wir die 'Lücken', die die Menge \mathbb{Q} offensichtlich aufweist, wenn wir sie uns als Zahlenstrahl vorstellen, auffüllen; die 'vervollständigte' Menge soll anschaulich gesprochen alle Punkte des Zahlenstrahls umfassen (insbesondere also \mathbb{Q} als Teilmenge enthalten). Wir wollen sie \mathbb{R} , *Menge der reellen Zahlen*, nennen. Auf \mathbb{R} sollen Addition und Multiplikation so definiert sein, dass $(\mathbb{R}, +, \cdot)$ ein Körper ist (so wie \mathbb{Q}), und \mathbb{R} soll bezüglich einer Ordnungsrelation ' \leq ' vollständig angeordnet sein (so wie \mathbb{Q}). Der entscheidende Unterschied zwischen \mathbb{Q} und \mathbb{R} ist die geforderte 'Lückenlosigkeit' von \mathbb{R} . Wie können wir diese mathematisch fassen? Dazu betrachten wir nochmal die Stelle x des Zahlenstrahls, die durch $x^2 = 2$ (und $x \geq 0$) charakterisiert

²⁴Da p und q dabei jedesmal echt kleiner werden, kommt dieser Prozess nach endlich vielen Schritten zu einem Ende.

ist und die üblicherweise mit $x = \sqrt{2}$ bezeichnet wird. Wir wissen, dass $x \notin \mathbb{Q}$ (s.o.). Wir betrachten die folgende, $\sqrt{2}$ entsprechende 'Zerlegung' des Zahlenstrahls in eine 'untere' und eine 'obere' Menge

$$U := \{x \in \mathbb{Q} \mid x^2 \leq 2 \vee x < 0\}, \quad O := \{x \in \mathbb{Q} \mid x^2 > 2 \wedge x \geq 0\}$$

In gewisser Weise 'repräsentiert' diese Zerlegung, dieser 'Schnitt', unseren gesuchten, nicht in \mathbb{Q} enthaltenen Punkt x des Zahlenstrahls, nämlich in dem Sinne, dass \mathbb{Q} in Mengen U und O zerlegt wurde (Partition von \mathbb{Q}) so dass alle rationalen Zahlen, die kleiner als x sind, in U , und alle rationalen Zahlen, die größer als x sind, in O enthalten sind. Dies motiviert folgende Vorgehensweise: Wir betrachten alle 'Schnitte' der obigen Art. Die Menge aller solchen Schnitte wird unsere Menge \mathbb{R} werden. Natürlich hat auch jede *rationale* Zahl einen eigenen Schnitt, nämlich für jedes $x \in \mathbb{Q}$ nehmen wir den Schnitt

$$U = \{q \in \mathbb{Q} \mid q \leq x\}, \quad O = \{q \in \mathbb{Q} \mid q > x\}.$$

In diesem Sinne ist die Menge aller Schnitte mindestens so groß wie die Menge aller rationalen Zahlen, aber, was erstaunlich ist, ist die Menge aller Schnitte echt größer (d.h. eine echte Obermenge) der Menge aller rationalen Zahlen! Wir wollen noch formal definieren, was ein Schnitt ist:

Def. (Dedekind'scher Schnitt)

eine Zerlegung $\mathbb{Q} = U \cup O$, $U \cap O = \emptyset$ heißt *Dedekind'scher Schnitt*²⁵, wenn

- a) $U, O \neq \emptyset$
- b) $x \in U \wedge y \in O \Rightarrow x < y$
- c) Falls es ein $q \in \mathbb{Q}$ gibt, so dass $\forall x \in U : x \leq q$ und $\forall x \in O : x \geq q$, so sei $q \in U$.

Wenn es ein $q \in \mathbb{Q}$ gibt, das die Bedingung aus c) erfüllt, dass

$$\forall x \in U : x \leq q \quad \wedge \quad \forall x \in O : x \geq q,$$

so sagt man auch *der Schnitt* (U, O) "trifft" $q \in \mathbb{Q}$ und spricht dann von einem *rationalen Schnitt*.

Bemerkungen.

- Die Bedingung c) dient lediglich dazu, dass es zu rationalen Zahlen q nicht zwei Schnitte $U = \{q \in \mathbb{Q} \mid q \leq x\}, O = \{q \in \mathbb{Q} \mid q > x\}$ und $U = \{q \in \mathbb{Q} \mid q < x\}, O = \{q \in \mathbb{Q} \mid q \geq x\}$ gibt.
- Es gibt Schnitte, die keine rationale Zahl treffen (Beispiel dafür ist der oben zu $\sqrt{2}$ gehörende Schnitt: die Annahme, er treffe eine rationale Zahl q , hätte $q^2 = 2$ zur Folge, Widerspruch); die Menge der Schnitte ist – entgegen aller Anschauung(!) – also echt größer als die Menge der rationalen Zahlen.

²⁵Richard Dedekind, 1831 - 1916

Man kann auf der Menge der Schnitte eine (totale) Ordnungsrelation definieren durch $(U_1, O_1) \leq (U_2, O_2) :\iff U_1 \subseteq U_2$. Man kann Dedekind'sche Schnitte addieren und multiplizieren, und zwar sei die Addition $(U_1, O_1) + (U_2, O_2)$ definiert als der Schnitt (U_3, O_3) , der sich ergibt als $U_3 = \{x_1+x_2 \mid x_1 \in U_1, x_2 \in U_2\}$, $O_3 = \{x_1+x_2 \mid x_1 \in O_1, x_2 \in O_2\}$.²⁶

Wir definieren: **\mathbb{R} ist die Menge aller Dedekind'schen Schnitte.** Indem wir \mathbb{Q} mit der Menge der rationalen Schnitte identifizieren, können wir \mathbb{Q} als Teilmenge von \mathbb{R} auffassen. Die Elemente aus $\mathbb{R} \setminus \mathbb{Q}$ heißen *irrationale Zahlen*. Auf \mathbb{R} gibt es eine totale Ordnung ' \leq ' (s.o.), die für Elemente aus \mathbb{Q} mit der Ordnung auf \mathbb{Q} übereinstimmt. Die auf \mathbb{R} oben definierten Addition und Multiplikation, eingeschränkt auf \mathbb{Q} , ergeben die bekannte Addition/Multiplikation in \mathbb{Q} . Man kann zeigen, dass \mathbb{R} bezüglich dieser Verknüpfungen ein *Körper* ist.

\mathbb{R} ist also, so wie \mathbb{Q} , ein vollständig angeordneter Körper, d.h. ein Körper mit einer vollständigen Ordnungsrelation. Eine reelle Zahl mit " (U, O) " zu bezeichnen, und dann damit zu rechnen, ist auf Dauer recht mühsam. Wir wollen stattdessen in Zukunft wieder einfach " x " (oder " y ", " z ", ...) schreiben. Wir hatten den Umweg über Dedekind'sche Schnitte nur deshalb gewählt, um uns davon zu überzeugen, dass es eine Menge \mathbb{R} (genauer: eine Menge, die genau die Eigenschaften hat, die \mathbb{R} haben soll) wirklich 'gibt'. Genauer: Wir konnten eine solche Menge *konstruieren* unter Verwendung der Menge \mathbb{Q} . Wir halten hier einige Eigenschaften fest, die für alle Zahlen in \mathbb{R} (insbesondere also auch für alle Zahlen in \mathbb{Q}) gelten:

- (1) $x < y \Rightarrow x + z < y + z$
- (2) $x < y \wedge z > 0 \Rightarrow xz < yz$
- (3) $x < y \wedge z < 0 \Rightarrow xz > yz$
- (4) $xy > 0 \Leftrightarrow (x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)$
- (5) $x > 0 \wedge y > 0 \Rightarrow x + y > 0$
- (6) $x > 0 \Leftrightarrow -x < 0$
- (7) $x < y \wedge xy > 0 \Rightarrow y^{-1} < x^{-1}$
- (8) $x \neq 0 \Rightarrow x^2 = x \cdot x > 0$
- (9) $x > 0 \Leftrightarrow x^{-1} > 0$

Die Aussagen (1)-(6) gelten auch, wenn man die Relationen ' $<$ ', ' $>$ ' durch ' \leq ', ' \geq ' ersetzt. Die Ungleichung $xy > 0$ (siehe (7)) drückt in knapper Form aus: x und y haben das gleiche Vorzeichen (heißt: sind beide größer null oder beide kleiner null (siehe (4))).

²⁶Die Multiplikation ist etwas mühsamer zu definieren, da man Fälle unterscheiden muss, je nach dem, ob die einzelnen Schnitte links oder rechts des Null-Schnitts liegen.

Potenzen können für $a \in \mathbb{R}$, $n \in \mathbb{N}_0$ rekursiv durch $a^0 := 1$, $a^{n+1} := a \cdot a^n$ definiert werden. Die n -te Wurzel $\sqrt[n]{a}$ ist für $n \in \mathbb{N}$ und $a \in \mathbb{R}_0^+$ definiert als die Lösung von $x^n = a$ (im Falle von ungeradem n kann hier auch negatives a zugelassen werden). Es sei $a^{\frac{m}{n}} := \sqrt[n]{a^m}$ für $a \geq 0$.²⁷ Es gelten die Potenzrechenregeln $(ab)^c = a^c b^c$, $a^b a^c = a^{b+c}$, $(a^b)^c = a^{bc}$, und wir vereinbaren, dass $a^{b^c} := a^{(b^c)}$ heißen soll.

Ferner definiert man auf \mathbb{R} (und somit auch auf \mathbb{Q}) den *Absolutbetrag* oder kurz *Betrag*

$$|x| := \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}$$

und das *Signum* (Vorzeichen)

$$\operatorname{sgn}(x) := \begin{cases} 1, & \text{falls } x > 0 \\ 0, & \text{falls } x = 0 \\ -1, & \text{falls } x < 0 \end{cases}$$

Es gilt dann $x = \operatorname{sgn}(x) |x|$ für alle $x \in \mathbb{R}$.

Vergleich von \mathbb{R} und \mathbb{Q} . Sowohl \mathbb{R} als auch \mathbb{Q} sind Körper und sind vollständig angeordnet, und auch obige Rechenregeln gelten in beiden Mengen. Doch wodurch unterscheiden sich \mathbb{R} und \mathbb{Q} ? Wir haben gesehen: \mathbb{Q} hat gewisse 'Lücken'; wir wissen, dass $\mathbb{Q} \subsetneq \mathbb{R}$, denn $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. (Ähnlich kann man zeigen, dass auch $\sqrt[3]{2} \in \mathbb{R} \setminus \mathbb{Q}$. (Wie lautet der zu $\sqrt[3]{2}$ gehörende Dedekind'sche Schnitt?) Nicht ganz so einfach ist es zu zeigen, dass auch $\pi \in \mathbb{R} \setminus \mathbb{Q}$.) Diesen wesentlichen Unterschied, der anschaulich mit 'Lückenlosigkeit' beschrieben werden kann, wird auch als (*topologische*) *Vollständigkeit* von \mathbb{R} bezeichnet²⁸; diesen Unterschied präzise zu fassen ist mit unserem aktuellen Kenntnisstand nicht ganz leicht. Er wird in der Analysis-Vorlesung noch einmal thematisiert werden im Kapitel 'Konvergenz von Folgen'. Eine etwas leichter greifbare Charakterisierung, wann eine reelle Zahl rational und wann irrational ist, liefert die sogenannte Dezimaldarstellung von reellen Zahlen, siehe folgendes Kapitel.

2.4 Dezimaldarstellung rationaler und reeller Zahlen

Mit der Schreibweise

$$x = a_0, a_1 a_2 a_3 \dots, \quad \text{mit } a_0 \in \mathbb{Z}, a_1, a_2, a_3, \dots \in \{0, 1, \dots, 9\}$$

ist, wie wir wissen, der Zahlenwert

$$a_0 + 10^{-1}a_1 + 10^{-2}a_2 + 10^{-3}a_3 + \dots = \sum_{i=0}^{\infty} 10^{-i}a_i$$

²⁷Die Potenz für *irrationale* Exponenten kann man definieren über Grenzwertprozesse oder über $x^y := \exp(y \ln x)$, siehe Analysis-Teil der Vorlesung.

²⁸nicht zu verwechseln mit dem Begriff der vollständigen Ordnung, d.h. vollständig angeordneten Mengen

gemeint.²⁹ Wie wandelt man einen gegebenen Bruch in die Dezimaldarstellung um? Dazu die folgenden

Beispiele.

1. $x = \frac{221}{80}$

Wir spalten den ganzzahligen Anteil ab: $\frac{221}{80} = 2 + \frac{61}{80}$. (Wir haben hier 'Division mit Rest' durchgeführt: $221 = 2 \cdot 80 + 61$, d.h. 221 durch 80 ist 2 Rest 61)

Der Bruch $\frac{61}{80}$ ergibt den Nachkommaanteil. Um die erste Nachkommastelle zu finden, multiplizieren wir den Bruch mit 10 und spalten davon wieder den ganzzahligen Anteil ab³⁰:

$\frac{61}{80} \cdot 10 = \frac{610}{80} = 7 + \frac{50}{80}$ (wir haben hier wieder Division mit Rest durchgeführt: $610 = 7 \cdot 80 + 50$). Wir erhalten die Ziffer 7.

Und so weiter:

$$\frac{50}{80} \cdot 10 = \frac{500}{80} = 6 + \frac{20}{80}$$

$$\frac{20}{80} \cdot 10 = \frac{200}{80} = 2 + \frac{40}{80}$$

$$\frac{40}{80} \cdot 10 = \frac{400}{80} = 5 + \frac{0}{80}$$

Hier bricht die Rechnung ab, da kein gebrochener Anteil mehr übrig ist bzw. da die Division mit Rest den Rest 0 ergeben hat ('aufgegangen ist').

Ergebnis: $\frac{221}{80} = 2,7625$

2. $x = \frac{8}{990}$:

$$\frac{8}{990} = 0 + \frac{8}{990}$$

$$\frac{8}{990} \cdot 10 = \frac{80}{990} = 0 + \frac{80}{990}$$

$$\frac{80}{990} \cdot 10 = \frac{800}{990} \stackrel{(*)}{=} 0 + \frac{800}{990}$$

$$\frac{800}{990} \cdot 10 = \frac{8000}{990} = 8 + \frac{80}{990}$$

$$\frac{80}{990} \cdot 10 = \frac{800}{990} = \dots$$

Hier brauchen wir nicht weiterzurechnen, denn dieses Zwischenergebnis hatten wir schonmal an der Stelle (*): Es kommt nun die Ziffer 0 und der Rest $\frac{800}{990}$, danach die Ziffer 8, usw., es wiederholt sich zyklisch. Wir erhalten $\frac{8}{990} = 0,008080808\dots = 0,0\overline{08}$ Also: Sobald ein Rest zum zweiten mal vorkommt, können wir die Rechnung abbrechen; die Folge der Dezimalziffern wird ab dieser Stelle zyklisch.

Da für den Rest nur endlich viele verschiedene Werte (maximal so viele, wie der Nenner von $x = \frac{m}{n}$ angibt) vorkommen können, muss sich irgendwann ein Rest wiederholen, also ein periodisches Verhalten der Ziffernfolge einsetzt. (Falls man abbrechende Dezimalzahlen als 'Periode null' auffasst, kann man den Fall einer abbrechenden Dezimalentwicklung auch als Spezialfall einer periodischen Dezimalentwicklung auffassen: $2,7625 = 2,7625000000\dots = 2,7625\overline{0}$.)

So sehen wir ein: **Jeder Bruch**, d.h. jede rationale Zahl, lässt sich **in eine abbre-**

²⁹ ∞ := "unendlich". Später im Analysis-Teil der Vorlesung werden wir noch genauer erklären, was wir unter einer solchen "Summation von unendlich vielen Zahlen" verstehen wollen.

³⁰Wer will kann zwischendurch auch kürzen.

chende oder eine periodische Dezimalzahl umwandeln.

Auf analoge Weise kann man Brüche auch in andere Stellensysteme umwandeln, z.B. ins Binärsystem. Dazu multipliziert man mit 2 statt 10.

Nun zur Umkehrung der Aufgabenstellung:

Gegeben sei eine Dezimalzahl, gesucht ist eine Darstellung als Bruch.

Für abbrechende Dezimalzahlen ist dies sehr einfach: Z.B. ist

$$2,7625 = 2 + \frac{7}{10} + \frac{6}{100} + \frac{2}{1000} + \frac{5}{10\,000} = \frac{27\,625}{10\,000}.$$

Für periodische Dezimalzahlen wie z.B. $0,12\bar{4}$ gehen wir wie folgt vor:

$$\begin{aligned} 0,12\bar{4} &= \frac{1}{10} + \frac{2}{100} + \frac{4}{1000} + \frac{4}{10\,000} + \dots \\ &= \frac{1}{10} + \frac{2}{100} + \frac{4}{1000} \cdot \left(1 + \frac{1}{10} + \frac{1}{100} + \dots\right) \end{aligned}$$

Die Klammer berechnen wir mit der Summenformel der geometrischen Reihe (Aufgabenblatt 3):

Es ist $\sum_{i=0}^n q^i = \frac{1-q^{n+1}}{1-q}$ für $q \neq 1$, lassen wir n gegen unendlich gehen, erhalten wir

$\sum_{i=0}^{\infty} q^i = \frac{1}{1-q}$, sofern $|q| < 1$. Die Klammer ergibt, mit $q := \frac{1}{10}$, $\frac{1}{1-\frac{1}{10}} = \frac{10}{9}$. Wir erhalten also

$$0,12\bar{4} = \frac{12}{100} + \frac{4}{1000} \cdot \frac{10}{9} = \frac{12}{100} + \frac{4}{900} = \frac{112}{900} = \frac{28}{225}.$$

Noch ein Beispiel:

$$\begin{aligned} 1,3\bar{26} &= 1 + \frac{3}{10} + \frac{2}{100} + \frac{6}{1000} + \frac{2}{10\,000} + \frac{6}{100\,000} + \dots \\ &= 1 + \frac{3}{10} + \frac{26}{10^3} + \frac{26}{10^5} + \frac{26}{10^7} + \dots \\ &= 1 + \frac{3}{10} + \frac{26}{10^3} \cdot \left(1 + \frac{1}{10^2} + \frac{1}{10^4} + \frac{1}{10^6} + \dots\right) \\ &= 1 + \frac{3}{10} + \frac{26}{10^3} \cdot \frac{1}{1-\frac{1}{100}} = 1 + \frac{3}{10} + \frac{26}{10^3} \cdot \frac{100}{99} \\ &= \frac{13}{10} + \frac{26}{990} = \frac{1313}{990} \end{aligned}$$

wobei wieder die geometrische Summenformel (mit $q = \frac{1}{100}$) verwendet wurde.

Wir sehen, dass diese Methode allgemein auf jede periodische oder abbrechende Dezimalzahl anwendbar ist und erkennen, dass sich jede abbrechende oder periodische

Dezimalzahl in einen Bruch umwandeln lässt. Insgesamt haben wir damit gezeigt:

Eine reelle Zahl ist *genau dann* rational, wenn sie sich als periodische oder abbrechende Dezimalzahl schreiben lässt.

Die Dezimaldarstellung von $\sqrt{2}$ und von $\sqrt[3]{2}$ ist also weder periodisch noch abbrechend.

Noch ein Aspekt der Dezimaldarstellung:

Mit der Summenformel der geometrischen Reihe ist

$$0,\bar{9} = \frac{9}{10} + \frac{9}{100} + \dots = \frac{9}{10} \cdot \left(1 + \frac{1}{10} + \frac{1}{100} + \dots\right) = \frac{9}{10} \cdot \frac{1}{1 - \frac{1}{10}} = 1,$$

also $0,99999\dots = 1,00000\dots$!

Wenn wir wollen, dass die Dezimaldarstellung einer Zahl *eindeutig* ist, so müssen wir alle 'Perioden-Neun' verbieten. Mathematisch präzise: Für beliebig großes $n \in \mathbb{N}$ muss es einen Index $i \geq n$ geben, so dass in der Dezimalentwicklung $a_i \neq 9$ ist.

Eine Folgerung aus der Dezimaldarstellung ist:

Jede reelle Zahl lässt sich beliebig genau durch eine rationale Zahl approximieren: Denn als rationale Approximation $q \in \mathbb{Q}$ an eine Zahl $x \in \mathbb{R}$ kann man z.B. die abgeschnittene Dezimalentwicklung von x nehmen. So kann z.B. $x = \sqrt{2} = 1,41421356237\dots$ durch $q := 1,414213$ mit einem Fehler $|x - q| \leq 10^{-6}$ von höchstens 10^{-6} approximiert werden.

Man sagt dazu auch: Die rationalen Zahlen liegen *dicht* in \mathbb{R} .

Zur (näherungsweise, beliebig genauen) Berechnung von Wurzeln gibt es das *Heron-Verfahren* (siehe Übung).

Mächtigkeit von \mathbb{Q} und von \mathbb{R} .

Man kann zeigen ("Cantor'sches Diagonalargument", siehe Vorlesung): Die Menge \mathbb{Q} ist abzählbar. Die Menge \mathbb{R} ist nicht abzählbar (ist überabzählbar).

2.5 Die komplexen Zahlen

Die reellen Zahlen ermöglichten uns das Finden von Lösungen der Gleichung

$$x^2 = a,$$

wobei $a \geq 0$ gegeben war. Falls jedoch $a < 0$, so finden wir keine Lösung $x \in \mathbb{R}$, denn sowohl für negatives als auch für positives x ist x^2 immer ≥ 0 .

Diese Problematik der Nichtexistenz von reellen Lösungen finden wir auch bei allgemeineren quadratischen Gleichungen:

Wir wollen Lösungen der quadratischen Gleichung

$$x^2 + px + q = 0$$

berechnen. Mit quadratischer Ergänzung bekommen wir

$$0 = x^2 + 2 \cdot \frac{p}{2} x + \left(\frac{p}{2}\right)^2 + q - \frac{p^2}{4} = \left(x + \frac{p}{2}\right)^2 + q - \frac{p^2}{4}$$
$$\iff \left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q$$

Falls die rechte Seite (auch *Diskriminante* genannt) nichtnegativ ist, können wir die Wurzel auf beiden Seiten der Gleichung ziehen und bekommen

$$x + \frac{p}{2} = \pm \sqrt{\frac{p^2}{4} - q}$$

also

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Im Fall dass $\frac{p^2}{4} - q < 0$ finden wir jedoch keine reelle Lösung. Wenn wir auch in diesem Fall Lösungen wünschen, müssen wir unseren Zahlenbereich weiter vergrößern. Dies führt auf die Zahlenmenge der *Komplexen Zahlen*, bezeichnet mit \mathbb{C} .

Sofern man rein praktisch orientiert den Körper der komplexen Zahlen einführen möchte, so kann man \mathbb{C} 'definieren' als:

$(\mathbb{C}, +, \cdot)$ ist der Körper

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\},$$

wobei $i^2 = -1$ gilt.

Also z.B. rechnet man $(2+3i) \cdot (7+4i) = 2 \cdot 7 + 2 \cdot 4i + 3i \cdot 7 + 3i \cdot 4i = 14 + 8i + 21i + 12i^2 = 2 + 29i$.

Die Visualisierung von Elementen von \mathbb{C} kann in einem Koordinatensystem, der sog. *Komplexen Ebene*, erfolgen, mit a auf der horizontalen und b auf der vertikalen Achse.

An dieser 'Definition' von \mathbb{C} ist jedoch ein wenig unbefriedigend, dass nicht erklärt wird, was 'i' ist und warum $i^2 = -1$ gilt.³¹

Die mathematisch präzise Definition/Konstruktion von \mathbb{C} ist jedoch gar nicht schwer: Wir setzen

$$\mathbb{C} := \mathbb{R} \times \mathbb{R},$$

d.h. \mathbb{C} ist die Menge aller Paare von reellen Zahlen. Wir müssen auf \mathbb{C} nun noch Rechenoperationen '+' und '.' definieren, und zwar ist es zweckmäßig, dies so zu tun, dass $(\mathbb{C}, +, \cdot)$ ein Körper ist, und zwar:

³¹Manchmal liest man auch ' $i = \sqrt{-1}$ ', was allerdings etwas ungenau und nicht ganz ungefährlich ist. Dazu später mehr.

Die Addition $+$: $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ definieren wir auf die naheliegendste Art, nämlich *komponentenweise* (d.h. wie bei 'Vektoren' im \mathbb{R}^2):

$$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$$

Die Multiplikation \cdot : $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ muss jedoch, um die Körpereigenschaften zu erhalten (hier ohne Beweis), wie folgt definiert werden:

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$$

Wenn wir für den Moment nur komplexe Zahlen, deren zweite Komponente null ist, betrachten, finden wir $(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0)$ und $(a_1, 0) \cdot (a_2, 0) = (a_1 a_2, 0)$. Die auf \mathbb{C} definierten Rechenoperationen '+', ' \cdot ' führen aus dieser Menge $\mathbb{R} \times \{0\} \subset \mathbb{C}$ also nicht heraus, und die auf \mathbb{C} definierten Verknüpfungen liefern die entsprechenden Ergebnisse wie die uns wohlbekannteren Verknüpfungen in \mathbb{R} . Wir können somit die reellen Zahlen als Teilmenge von \mathbb{C} identifizieren: \mathbb{R} kann identifiziert werden mit $\mathbb{R} \times \{0\} = \{(a, 0) \mid a \in \mathbb{R}\} \subset \mathbb{C}$, d.h. wir können $(a, 0) \in \mathbb{C}$ mit $a \in \mathbb{R}$ 'identifizieren'.

Unter anderem weil man sich obige Multiplikationsformel nur schwer merken kann, ist es zweckmäßig, eine neue Schreibweise einzuführen: Die Zahl $(0, 1) \in \mathbb{C}$ bezeichnen wir von nun an mit i , der sogenannten *Imaginären Einheit*, und die Zahl $(1, 0)$ bezeichnen wir gemäß obiger Identifizierung von nun an nur noch mit '1'. Wir können nun jede komplexe Zahl schreiben als

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + b \cdot i = a + bi$$

Mit dieser Schreibweise können wir Addition und Multiplikation sehr intuitiv behandeln:

$$(a + bi) + (c + di) = (a + b) + (c + d)i,$$

und, wegen $i^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 0 \cdot 1) = (-1, 0) = -(1, 0) = -1$, also

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i.$$

Es ist (anders als auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$) i.a. nicht sinnvoll, auf \mathbb{C} Ordnungsrelationen zu betrachten.³²

Einige besondere Bezeichnungen im Zusammenhang mit komplexen Zahlen:

Def. (Real-, Imaginärteil, Betrag, Argument, konjugiert-komplexes einer komplexen Zahl)

³²Grund: wie auch immer man eine solche Ordnungsrelation definieren würde, man würde nie erreichen, dass so nützliche Rechenregeln wie für die reellen Zahlen (S. 30) gelten, d.h. eine Ordnungsrelation auf \mathbb{C} würde sich nicht mit der dortigen Addition und Multiplikation 'vertragen' und wäre somit recht nutzlos.

- (a) Sei $z = a + bi$, mit $a, b \in \mathbb{R}$, eine komplexe Zahl. Dann heißt a der *Realteil* von z und b der *Imaginärteil* von z :

$$a = \operatorname{Re}(z), \quad b = \operatorname{Im}(z)$$

Jede komplexe Zahl lässt sich also schreiben als $z = \operatorname{Re}(z) + i \operatorname{Im}(z)$.

- (b) $\bar{z} := a - bi$ heißt die zu $z = a + bi$ *konjugiert-komplexe* Zahl.
- (c) Der Betrag einer komplexen Zahl $z = a + bi$ wird definiert als
 $|z| := \sqrt{a^2 + b^2} = \sqrt{\operatorname{Re}(z)^2 + \operatorname{Im}(z)^2}$.

- (d) Das sog. *Argument* $\varphi = \arg(z)$ einer komplexen Zahl $z \neq 0$ ist der Winkel zwischen der positiven horizontalen Achse und dem Ursprungsvektor von 0 nach z .³³ Das Argument wird im Bogenmaß gemessen und ist eigentlich nur 'modulo 2π ' bestimmt. Derjenige Wert des Arguments, der im Intervall $[0, 2\pi)$ liegt, wird als *Hauptwert* des Arguments bezeichnet, also z.B. $\arg(-i) = 3\pi/2$ (=Hauptwert des Arguments).

Polarkoordinaten. Offenbar kann man durch Angabe von Betrag und Argument einer komplexen Zahl diese eindeutig beschreiben. Gibt man eine komplexe Zahl durch Angabe ihres Betrags und ihres Arguments, so spricht man von *Polarkoordinaten*.

Beispiele: Die komplexe Zahl mit Betrag $|z| = 1$ und Argument $\arg(z) = \pi/4$ ist $z = \sqrt{1/2} + i\sqrt{1/2}$. Die komplexe Zahl mit Argument $\arg(z) = 2\pi/3$ und Betrag $|z| = 12$ ist $z = 12 \cdot (-\frac{1}{2} + \frac{1}{2}\sqrt{3}i) = -6 + 6\sqrt{3}i$.

Ist $\alpha \in \mathbb{R}$ und $z = a+ib \in \mathbb{C}$, $a, b \in \mathbb{R}$, so ist $\alpha z = \alpha(a+ib) = \alpha a + i\alpha b$, d.h. bei Multiplikation einer komplexen Zahl mit einem reellen Faktor werden Real- und Imaginärteil um diesen Faktor vergrößert; geometrisch wird der 'Vektor' z also um den Faktor α gestreckt. Wir können daher auch umgekehrt jede komplexe Zahl $z \neq 0$ als Produkt ihres Betrages $\alpha = |z| \in \mathbb{R}_0^+$ und eines Punktes $z_0 \in \mathbb{C}$, der auf dem Einheitskreis liegt, darstellen:

$$z = |z| z_0, \quad \text{wobei } |z_0| = 1, \quad \arg(z_0) = \arg(z).$$

Eine Zahl auf dem Einheitskreis kann mittels Sinus und Kosinus des Argumentes dargestellt werden³⁴:

$$z_0 = \cos(\arg(z_0)) + i \sin(\arg(z_0)) = \cos(\arg(z)) + i \sin(\arg(z))$$

Wir bekommen also die Darstellung

$$z = |z| (\cos(\arg(z)) + i \sin(\arg(z)))$$

³³Für z aus dem ersten Quadranten (d.h. Real- u. Imaginärteil positiv) ist $\arg(z) = \arctan(\operatorname{Im}(z)/\operatorname{Re}(z))$.

³⁴Dies stellt einen hier leider unvermeidlichen Vorgriff auf trigonometrische Funktionen dar, die erst in späteren Kapiteln *exakt* definiert werden werden.

bzw.

$$z = r(\cos \varphi + i \sin \varphi), \quad \text{wobei } r = |z|, \quad \varphi = \arg(z).$$

Rechenregeln. Sei $z = a + bi$ mit $a, b \in \mathbb{R}$. Es ist

$$|\bar{z}| = |a - bi| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$$

sowie

$$\arg(\bar{z}) = 2\pi - \arg(z).$$

Es ist

$$z\bar{z} = (a + bi) \cdot (a - bi) = a^2 + abi - abi - i^2b^2 = a^2 + b^2 = |z|^2.$$

Es ist

$$z^2 = (a + bi)^2 = a^2 + 2abi + b^2i^2 = a^2 - b^2 + 2abi,$$

also $\operatorname{Re}(z^2) = a^2 - b^2$, $\operatorname{Im}(z^2) = 2ab$.

Berechnung von Inversen: Es ist (für $z \neq 0$)

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i$$

oder kurz

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2},$$

was nichts anderes ist als $z\bar{z} = |z|^2$, s.o..

Lösen von Gleichungen mittels Ansatz $z = a + bi$, $a, b \in \mathbb{R}$:

Beispiel. Bestimme alle $z \in \mathbb{C}$ mit $|1 - z|^2 = (1 - |z|)^2$:

Mit obigem Ansatz ist

$$\begin{aligned} |1 - z|^2 &= (1 - |z|)^2 \\ \Leftrightarrow |1 - a - bi|^2 &= (1 - \sqrt{a^2 + b^2})^2 \\ \Leftrightarrow (1 - a)^2 + (-b)^2 &= 1 - 2\sqrt{a^2 + b^2} + a^2 + b^2 \\ \Leftrightarrow -2a &= -2\sqrt{a^2 + b^2} \quad | \cdot (-1/2), \quad \text{quadr.} \\ \stackrel{(*)}{\Leftrightarrow} a^2 &= a^2 + b^2 \quad \wedge \quad a \geq 0 \\ \Leftrightarrow b &= 0 \quad \wedge \quad a \geq 0 \end{aligned}$$

Wir bekommen also die Lösungsmenge $L = \mathbb{R}_0^+ \subset \mathbb{C}$.

Beachte die Stelle (*): Wurzelziehen ist nicht unbedingt eine Äquivalenzumformung. Ließe man " $a \geq 0$ " in obiger Rechnung weg, so würde bei (*) nur " \Rightarrow " anstelle von " \Leftrightarrow " gelten.

Beispiel. Bestimme alle $z \in \mathbb{C}$ mit $z^2 = \bar{z} + 2z$:

Mit obigem Ansatz ist

$$\begin{aligned} z^2 &= \bar{z} + 2z \\ \Leftrightarrow a^2 - b^2 + 2abi &= 3a + bi \\ \stackrel{(*)}{\Leftrightarrow} a^2 - b^2 &= 3a \quad \wedge \quad 2ab = b \end{aligned}$$

An der Stelle (*) haben wir benutzt, dass zwei komplexe Zahlen genau dann gleich sind, wenn sowohl ihre Realteile als auch ihre Imaginärteile gleich sind.

Die zweite Gleichung darf nur durch b geteilt werden, wenn $b \neq 0$. Wir machen daher eine *Fallunterscheidung*:

Fall 1: $b \neq 0$. Division durch b ergibt $a = \frac{1}{2}$. Dies in die erste Gleichung eingesetzt ergibt $b^2 = \frac{1}{4} - \frac{3}{2} = -\frac{5}{4}$. Da wir *reelle* b suchen, hat diese Gleichung keine Lösung.

Fall 2: $b = 0$. Dies in die erste Gleichung eingesetzt ergibt $a^2 = 3a$, also $a^2 - 3a = 0$, was zu $a(a - 3) = 0$ faktorisiert werden kann, also $a = 0$ oder $a = 3$.

Wir erhalten somit die Lösungsmenge $L = \{0, 3\} \subset \mathbb{C}$.

Geometrische Deutung von Addition und Multiplikation.

- Anhand einer Skizze wird schnell klar:
Geometrische Addition zweier komplexer Zahlen: Fasse beide Zahlen als Ursprungsvektoren auf, verschiebe den zweiten Vektor, so dass sein Anfangspunkt am Endpunkt des ersten zu liegen kommt; der Endpunkt des zweiten Vektors ist dann die Summe (vgl. 'Kräfteparallelogramm').
- Um die Multiplikation komplexer Zahlen grafisch zu deuten, ist es sinnvoll beide Zahlen in Polarkoordinaten zu betrachten: Seien $z_1 = r_1 (\cos \varphi_1 + i \sin \varphi_1)$, $z_2 = r_2 (\cos \varphi_2 + i \sin \varphi_2)$ ($r_1, r_2 > 0$) zu multiplizieren:

$$\begin{aligned} \Rightarrow z_1 z_2 &= r_1 r_2 [\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2 \\ &\quad + i \cos \varphi_1 \sin \varphi_2 + i \sin \varphi_1 \cos \varphi_2] \end{aligned}$$

Mittels der Additionstheoreme für trigonometrische Funktionen³⁵ folgt

$$z_1 z_2 = r_1 r_2 [\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)]$$

Dies ist die Polardarstellung von $z_1 z_2$, und wir können ablesen:

$$|z_1 z_2| = r_1 r_2, \quad \arg(z_1 z_2) = \varphi_1 + \varphi_2 \pmod{2\pi}$$

Fazit:

Beim Multiplizieren komplexer Zahlen multiplizieren sich die Beträge und addieren sich die Argumente.

Aus dieser Tatsache folgt sofort: Beim Erheben einer Komplexen Zahl $z = r (\cos(\varphi) + i \sin(\varphi))$ in die n -te Potenz ($n \in \mathbb{Z}$) wird der Betrag mit n potenziert und das Argument mit n multipliziert:

$$z^n = r^n (\cos(n\varphi) + i \sin(n\varphi))$$

(de Moivre'sche Formel)

³⁵...welche wir später in der Analysis beweisen werden...

Bsp.: $z = 1+i$ hat $r = \sqrt{2}$ und $\varphi = \frac{\pi}{4}$. Also $(1+i)^4$ hat Betrag $(\sqrt{2})^4 = 4$ und Argument $4 \cdot \frac{\pi}{4} = \pi$. Also ist $(1+i)^4 = -4$. (Alternativ kann man $(1+i)^4$ mit der Binomischen Formel ausrechnen.)

Das Problem der n -ten Wurzeln. Gegeben sei eine Zahl $z \in \mathbb{C}$ und ein $n \in \mathbb{N}$, und gesucht sind Zahlen $w \in \mathbb{C}$ so dass

$$w^n = z.$$

Solche Zahlen w heißen n -te Wurzeln von z . Zur praktischen Berechnung erinnern wir uns an obige Regel zur Multiplikation komplexer Zahlen und halten fest:

$$\begin{aligned} \arg(w^n) &= \underbrace{\arg(w) \cdot \dots \cdot \arg(w)}_{n \text{ mal}} = n \cdot \arg(w) \\ |w^n| &= \underbrace{|w| \cdot \dots \cdot |w|}_{n \text{ mal}} = |w|^n \end{aligned}$$

Wir wollen erreichen, dass $w^n = z$ gilt, also dass $|w^n| = |z|$ und dass $\arg(w^n) \equiv \arg(z) \pmod{2\pi}$. Dies liefert die Bedingungen

$$|w|^n = |z|, \quad n \cdot \arg(w) \equiv \arg(z) \pmod{2\pi}$$

Aus der ersten Bedingung folgt

$$|w| = \sqrt[n]{|z|}$$

(beachte, dass wir hier die n -te Wurzel aus *reellen* nichtnegativen Zahlen ziehen, was wir als bekannt voraussetzen).

Bei der Deutung der Beziehung der Argumente ist Vorsicht angebracht: Zunächst ist offensichtlich $\arg(w) = \frac{1}{n} \arg(z)$ eine Lösung, jedoch nicht die einzige, denn addieren wir den n -ten Teil des Vollkreises, oder allgemeiner, ein ganzzahliges Vielfaches des n -ten Einheitskreises zu $\arg(w)$, so erhalten wir ebenfalls $n \cdot (\arg(w) + k \cdot \frac{2\pi}{n}) = n \arg(w) + 2\pi k = \arg(z) + 2\pi k \equiv \arg(z) \pmod{2\pi}$. Wir können in diese Rechnung $k = 0, 1, \dots, n-1$ einsetzen (alle weiteren ganzzahligen k liefern keine weiteren Lösungen) und erhalten also n viele Lösungen w_0, \dots, w_{n-1} mit

$$|w_0| = |w_1| = \dots = |w_{n-1}| = \sqrt[n]{|z|}$$

und

$$\arg(w_k) = \frac{1}{n} \arg(z) + k \frac{2\pi}{n}, \quad k = 0, 1, \dots, n-1.$$

Bemerkungen.

- Die n -ten Wurzeln einer komplexen Zahl liegen also immer symmetrisch um den Nullpunkt verteilt auf den Ecken eines regelmäßigen n -Ecks. Im Fall $n=2$ erhalten wir zwei 'gegenüberliegende' Lösungen, d.h. $w_1 = -w_0$.
- Im Fall $z=1$ spricht man von den n -ten *Einheitswurzeln*. Da $\arg(1)=0$ und $|1|=1$ haben die n -ten Einheitswurzeln w_j , $j=0, \dots, n-1$, $|w_j|=1$ und $\arg(w_j) = \frac{2\pi j}{n}$

- Mit der Schreibweise $\sqrt[n]{z}$ kann, je nach Autor, die *Menge* aller n -ten Wurzeln von z oder diejenige Wurzel mit dem kleinsten Argument gemeint sein, oder man vermeidet diese Schreibweise grundsätzlich.

Im Spezialfall $z = -1$, $n = 2$ erhalten wir übrigens die Wurzeln $\pm i$, also sollte die weiter oben kritisierte unpräzise Schreibweise " $i = \sqrt{-1}$ " genauer lauten: $\sqrt{-1} = \{i, -i\}$ oder kurz $\sqrt{-1} = \pm i$.

Beispiel. Finde alle komplexen vierten Wurzeln von $z = -2$:

z hat Betrag 2 und Argument π . Die 4 Lösungen haben also Betrag $\sqrt[4]{2}$ und die Argumente $\frac{\pi}{4} + \frac{k\pi}{2}$, $k = 0, 1, 2, 3$. In Polarkoordinaten, sowie umgerechnet in die Darstellung mit Real- und Imaginärteil, lauten die Wurzeln:

$$\begin{aligned} w_0 &= \sqrt[4]{2} \left[\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right] = \sqrt[4]{2} \left(\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \right) = 2^{1/4} (2^{-1/2} + i 2^{-1/2}) = 2^{-1/4} + i 2^{-1/4} \\ w_1 &= \sqrt[4]{2} \left[\cos \left(\frac{\pi}{4} + \frac{\pi}{2} \right) + i \sin \left(\frac{\pi}{4} + \frac{\pi}{2} \right) \right] = \sqrt[4]{2} \left(-\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \right) = -2^{-1/4} + i 2^{-1/4} \\ w_2 &= \sqrt[4]{2} \left[\cos \left(\frac{\pi}{4} + \frac{2\pi}{2} \right) + i \sin \left(\frac{\pi}{4} + \frac{2\pi}{2} \right) \right] = \sqrt[4]{2} \left(-\frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}} \right) = -2^{-1/4} - i 2^{-1/4} \\ w_3 &= \sqrt[4]{2} \left[\cos \left(\frac{\pi}{4} + \frac{3\pi}{2} \right) + i \sin \left(\frac{\pi}{4} + \frac{3\pi}{2} \right) \right] = \sqrt[4]{2} \left(\frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}} \right) = 2^{-1/4} - i 2^{-1/4} \end{aligned}$$

Bemerkung. Im Prinzip kann man das Lösen von Gleichungen der Art $w^n = z$ auch mittels Ansatz $w = a + bi$ angehen, jedoch ist das dann entstehende Gleichungssystem für die Unbekannten a und b nur in seltenen Fällen leicht zu lösen (siehe Übung).

Das Lösen quadratischer Gleichungen in \mathbb{C} .

Gesucht werden alle $z \in \mathbb{C}$ mit $z^2 + pz + q = 0$, wobei $p, q \in \mathbb{C}$:

Die Rechnung zu Anfang dieses Kapitels ist auch für komplexe p, q korrekt bis zur Stelle

$$\left(z + \frac{p}{2} \right)^2 = \frac{p^2}{4} - q.$$

Im allgemeinen muss man nun von der komplexen Zahl $\frac{p^2}{4} - q$ die beiden komplexen Wurzeln, nennen wir sie $\pm w$, bestimmen (s.o.). Die beiden komplexen Lösungen der Gleichung lauten dann $z_{1,2} = -\frac{p}{2} \pm w$.

Den Spezialfall, dass $p, q \in \mathbb{R}$, können wir genauer betrachten:

Im Spezialfall, dass $\frac{p^2}{4} - q \in \mathbb{R}_0^+$ ergeben sich die bereits bekannten *reellen* Lösungen.

Im Spezialfall, dass $d := \frac{p^2}{4} - q \in \mathbb{R}^-$ ist $\arg(\frac{p^2}{4} - q) = \pi$, die Hilfsgröße d hat also zweite

Wurzeln, die 'rein imaginär' (d.h. reelle Vielfache von i) sind, und zwar $\pm i \sqrt{\left| \frac{p^2}{4} - q \right|}$.

Wir bekommen die Lösungen

$$z_{1,2} = \begin{cases} -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} & , \text{ falls } \frac{p^2}{4} - q > 0 \\ -\frac{p}{2} \pm i \sqrt{\left| \frac{p^2}{4} - q \right|} & , \text{ falls } \frac{p^2}{4} - q < 0 \end{cases}$$

im Fall $p, q \in \mathbb{R}$.

Polynome über \mathbb{C} und über \mathbb{R} ; Polynomgleichungen.

Man kann zeigen:

Satz (Fundamentalsatz/Hauptsatz der Algebra). Jedes Polynom $P(z) = a_0 + a_1z + \dots + a_nz^n$ mit Koeffizienten in \mathbb{C} (also insbesondere auch, wenn die Koeffizienten in \mathbb{R}), $n \in \mathbb{N}$, $a_n \neq 0$ (n heißt dann *Grad* von P), hat eine Darstellung (*Linearfaktorzerlegung*) $P(z) = a_n \prod_{j=1}^n (z - z_j)$, wobei $z_1, \dots, z_n \in \mathbb{C}$.

Die z_j sind offensichtlich die Nullstellen von P (nicht notwendigerweise verschieden); es folgt also:

Jedes Polynom vom Grad ≥ 1 mit Koeffizienten in \mathbb{C} (insbesondere: mit Koeffizienten in \mathbb{R}) hat mindestens eine Nullstelle in \mathbb{C} . Anders ausgedrückt: Jede Polynomgleichung $a_0 + a_1z + \dots + a_nz^n = 0$ mit $n \geq 1$, $a_n \neq 0$ hat mindestens eine Lösung in \mathbb{C} .

Beachte: In \mathbb{R} gilt ein analoger Satz nicht: Es gibt Polynome mit Koeffizienten in \mathbb{R} , die keine Nullstelle in \mathbb{R} haben, z.B. $P(x) = 1 + x^2 > 0 \forall x \in \mathbb{R}$ (hat *komplexe* Nullstellen $\pm i$).

Dreiecksungleichung in \mathbb{C} .

Die aus dem Reellen bekannte Dreiecksungleichung $|z_1 + z_2| \leq |z_1| + |z_2|$ gilt auch für komplexe Zahlen, jedoch lässt sich der Beweis (siehe Übung) nicht übertragen sondern muss anders erfolgen:

Zur Vorbereitung des Beweises der Dreiecksungleichung stellen wir zunächst fest:

1. $z + \bar{z} = 2 \operatorname{Re}(z)$
2. $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$
3. $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$

Beweis:

1. $z + \bar{z} = (a + bi) + (a - bi) = 2a = 2 \operatorname{Re}(z)$
2. $\overline{z_1 + z_2} = \overline{a_1 + ib_1 + a_2 + ib_2} = a_1 - ib_1 + a_2 - ib_2 = \bar{z}_1 + \bar{z}_2$
3. $\overline{z_1 z_2} = \overline{(a_1 + b_1 i)(a_2 + b_2 i)} = \overline{a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)} = a_1 a_2 - b_1 b_2 - i(a_1 b_2 + a_2 b_1) = (a_1 - b_1 i)(a_2 - b_2 i) = \bar{z}_1 \bar{z}_2.$

Nun zum Beweis der Dreiecksungleichung im Komplexen:

$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2) \overline{(z_1 + z_2)} = (z_1 + z_2)(\bar{z}_1 + \bar{z}_2) \\ &= z_1 \bar{z}_1 + z_1 \bar{z}_2 + \bar{z}_1 z_2 + z_2 \bar{z}_2 = |z_1|^2 + z_1 \bar{z}_2 + \overline{z_1 \bar{z}_2} + |z_2|^2 \\ &= |z_1|^2 + 2 \operatorname{Re}(z_1 \bar{z}_2) + |z_2|^2 \leq |z_1|^2 + 2|z_1| |\bar{z}_2| + |z_2|^2 = |z_1|^2 + 2|z_1| |\bar{z}_2| + |z_2|^2 \\ &= |z_1|^2 + 2|z_1| |z_2| + |z_2|^2 = (|z_1| + |z_2|)^2 \end{aligned}$$

Mit Wurzelziehen folgt die Behauptung.

Historisches. 'Wurzeln aus negativen Zahlen' wurden offenbar erstmalig von Cardano (1545) und Descartes (1637) verwendet, aber damals offenbar eher als 'Rechentrick' angesehen. Eine systematische Untersuchung komplexer Zahlen sowie auch die allgemeine Akzeptanz des Rechnens mit komplexen Zahlen unter den Mathematikern setzte erst um die Jahrhundertwende vom 18. zum 19. Jhd. ein.

Komplexe Exponentialfunktion. An Stelle des Terms $\cos \varphi + i \sin \varphi$ finden Sie in Büchern oft den Ausdruck $\exp(i\varphi)$ oder $e^{i\varphi}$. Dazu die Bemerkung: Man kann in der Tat z.B. einfach als abkürzende Schreibweise, $\exp(i\varphi) := \cos \varphi + i \sin \varphi$ vereinbaren für $\varphi \in \mathbb{R}$. Aus der Tatsache, dass sich die Argumente bei der Multiplikation komplexer Zahlen addieren, folgt dann, dass $\exp(i(\varphi_1 + \varphi_2)) = \exp(i\varphi_1) \cdot \exp(i\varphi_2)$ (analog wie bei der 'klassischen' reellen Exponentialfunktion). Weiter kann man die Definition von 'exp' von rein imaginären auf beliebige komplexe Zahlen $\exp : \mathbb{C} \rightarrow \mathbb{C}$ ausdehnen per $\exp(a+bi) := \exp(a) \cdot \exp(bi) = e^a \cdot (\cos b + i \sin b)$. Problematisch ist bei diesem Zugang zur komplexen Exponentialfunktion, dass man mit unserem aktuellen Wissensstand nur schwer präzise erklären kann, was 'e' ist (die sog. Euler'sche Zahl). Im Kapitel 'Reihen' werden wir definieren, dass $\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!}$ und $e := \exp(1)$ ist, sowie – ganz ohne auf Begriffe der Geometrie (rechtwinklige Dreiecke) zurückgreifen zu müssen), werden wir dort die Sinus- und die Kosinus-Funktion definieren als 'Grenzwert' $\sin(z) := \sum_{n=0}^{\infty} \frac{z^{2n+1}}{(2n+1)!}$, $\cos(z) := \sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!}$ für alle $z \in \mathbb{C}$ (also insbesondere auch für $z \in \mathbb{R}$). Die Eigenschaften $\exp(i\varphi) = \cos \varphi + i \sin \varphi$ sowie $\exp(a+bi) = e^a (\cos b + i \sin b) \forall \varphi, a, b \in \mathbb{R}$ folgen dann als *Satz*.

Anwendungen des Rechnens mit komplexen Zahlen. Das Rechnen mit komplexen Zahlen hat sich als überaus fruchtbar erwiesen, auch und gerade für Probleme, die aus Anwendungen erwachsen. So ist es beispielsweise bei Schwingungsvorgängen in der Physik (Mechanik, Elektrotechnik), man denke an den sog. Federschwinger, oder an einen elektrischen Schwingkreis) möglich, die Gleichungen, nach denen sich das System verhält, (sogenannte Differentialgleichungen, siehe 2. oder 3. Semester) im Reellen aufzustellen, jedoch während des Lösens dann u.U. auch im Komplexen weiterzurechnen und gegen Ende der Rechnung rein reelle, also physikalisch sinnvolle Lösungen zu erhalten; ohne Kenntnis des Körpers der komplexen Zahlen wären solche Rechnungen viel mühsamer und weniger elegant.

Ein kleines Anwendungsbeispiel, wie es auch im Physik-Leistungskurs der Schule gerechnet werden kann: Ein Federschwinger (Masse befestigt an einer elastischen Feder) wird ausgelenkt und losgelassen und schwingt; es sei $x(t)$ der Ort zur Zeit t und $x=0$ die Ruhelage. Es wird angenommen, dass die Rückstellkraft=Federkraft proportional zur Auslenkung ist $F_{rueck} = -k_1 x$ (Hooke'sches Gesetz) und dass eine Reibungskraft proportional zur Geschwindigkeit $x'(t) = \frac{dx}{dt}$ vorliegt: $F_{reib} = -k_2 x'$. Die beschleunigende Kraft ist also $F = F_{rueck} + F_{reib}$. Nach dem Newton'schen Gesetz "Kraft gleich Masse mal Beschleunigung" ($F = m x''$) bekommen wir eine sog. Differentialgleichung $m x''(t) = -k_1 x(t) - k_2 x'(t)$, also $x''(t) + \frac{k_2}{m} x'(t) + \frac{k_1}{m} x(t) = 0$. Man kann diese Differentialgleichung z.B. lösen mit einem *Exponentialansatz*: Man setzt den Ansatz $x(t) := \alpha e^{\lambda t}$ in die Differentialgleichung ein. Man bekommt dann eine algebraische Gleichung für λ : $\lambda^2 + \frac{k_2}{m} \lambda + \frac{k_1}{m} = 0$. Je nach vorliegenden Werten für k_1 und k_2 kann diese quadratische Gleichung reelle oder aber auch komplexe Lösungen haben. Falls die Lösungen λ_1, λ_2 reell sind (sie sind dann insbesondere negativ) sind die Lösungen der Dgl $x(t) = e^{\lambda_1 t}$ und $x(t) = e^{\lambda_2 t}$ monoton fallend gegen null. Doch was ist die physikalische Bedeutung *komplexer nicht-reeller* Lösungen? Gibt es überhaupt eine Bedeutung? In der Tat: Man kann mit dem Gesetz

$e^{a+bi} = e^b(\cos b + i \sin b)$ die beiden komplexen Lösungen umschreiben. Anschließend überlegt man sich, dass, wenn man zwei Lösungen der Differentialgleichungen $e^{\lambda_1 t}$ und $e^{\lambda_2 t}$ hat, auch deren Summe sowie deren Differenz Lösungen der Dgl sein müssen. Die Summe (sowie, nach Division durch i auch die Differenz) beider Lösungen ist, wie man leicht nachrechnen kann, eine *rein reelle* Funktion, und zwar eine Schwingung, deren Amplitude im Laufe der Zeit abklingt. Und dies ist tatsächlich eine physikalisch sinnvolle Lösung des Problems. Man sieht: Man kann Anwendungsprobleme, die rein mit reellen Zahlen/Funktionen formuliert sind, unter Ausdehnung des Zahlenraums/Lösungsraums auf komplexe Zahlen lösen, und dann aus diesen komplexen Lösungen auch wieder rein reelle, somit physikalisch sinnvolle Lösungen des Anwendungsproblems finden.

Ein Schwingkreis (\rightarrow Elektrotechnik; ggf. Physik in der Schule), d.h. ein Stromkreis mit Kondensator, Spule und Ohm'schem Widerstand) wird durch eine Differentialgleichung beschrieben, die genau die gleiche Struktur hat wie die des Federschwingers. Komplexe Zahlen spielen daher in der Elektrotechnik eine große Rolle.

Im 3. Semester werden wir systematisch solche und andere Differenzialgleichungen lösen.

3 Lineare Algebra

3.1 Lineare Gleichungssysteme: Das Gauß-Verfahren

Beispiel: Gesucht sind zwei Zahlen, deren Summe 10 und deren Differenz $1/2$ ist:

$$\begin{aligned} \text{(I): } x + y &= 10 \\ \text{(II): } x - y &= \frac{1}{2} \end{aligned}$$

Lösen: Addiere z.B. die erste zur zweiten Gleichung, dies ergibt eine Gleichung, die nur eine Unbekannte enthält:

$$\begin{aligned} \text{(I): } x + y &= 10 \\ \text{(I)+(II): } 2x &= 10\frac{1}{2} \end{aligned}$$

Dies war in der Tat eine Äquivalenzumformung, denn man kann ja von der unteren Gleichung nun wieder die obere abziehen, um das Ausgangssystem wieder zu erhalten. Das umgeformte System hat somit die gleiche Lösungsmenge, es hat aber den Vorteil, dass es leichter zu lösen ist, denn in der unteren Gleichung haben wir eine der Unbekannten *eliminiert*. Die Gleichung mit nur einer Unbekannten kann man lösen: $x = 21/4$. Dies kann man in die andere Gleichung einsetzen:

$$\frac{21}{4} + y = 10$$

Es folgt $y = \frac{19}{4} = 4\frac{3}{4}$.

Variante: Man hätte auch eine der beiden Gleichungen durch die *Differenz* der beiden Gleichungen ersetzen können, was das x eliminiert hätte:

$$\begin{aligned} \text{(I): } x + y &= 10 \\ \text{(I)-(II): } 2y &= 9\frac{1}{2} \end{aligned}$$

also $y = 4\frac{3}{4}$; dies einsetzen ergibt wieder $x = \frac{21}{4}$.

Ein Gleichungssystem mit 3 Gleichungen und 3 Unbekannten x_1, x_2, x_3 :³⁶

$$\begin{aligned} x_1 - 2x_2 - 2x_3 &= 2 \\ x_1 + 3x_2 + 2x_3 &= 22 \\ -5x_1 + 20x_2 + 15x_3 &= 30 \end{aligned}$$

³⁶Geometrische Interpretation: Jede Gleichung mit zwei Unbekannten beschreibt (wenn nicht alle Koeffizienten gleich null sind) eine *Gerade* im \mathbb{R}^2 . Die Lösungsmenge eines LGS mit zwei Gleichungen und zwei Unbekannten ist also der Schnitt der zwei Geraden. (Dieses ist 'meistens' ein einzelner Punkt im \mathbb{R}^2 , kann aber auch leer sein oder eine komplette Gerade, wenn die beiden Geraden parallel sind.) Eine Gleichung mit drei Unbekannten beschreibt (wenn nicht alle Koeffizienten gleich null sind) eine *Ebene* im \mathbb{R}^3 . Die Lösungsmenge eines LGS mit drei Gleichungen und drei Unbekannten ist also der Schnitt dreier Ebenen im \mathbb{R}^3 . (Dieser ist 'meistens' ein einzelner Punkt.)

Allgemein: Ein *Lineares Gleichungssystem* (LGS) mit $n \in \mathbb{N}$ Unbekannten x_1, x_2, \dots, x_n und $m \in \mathbb{N}$ Gleichungen hat die Form³⁷

$$\begin{array}{rcl} a_{11}x_1 + \dots + a_{1n}x_n & = & b_1 \\ \vdots & & \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n & = & b_m \end{array}$$

Dabei heißen die b_1, \dots, b_m die *rechten Seiten* und die a_{ij} , $i = 1, \dots, m$, $j = 1, \dots, n$, die *Koeffizienten* des LGS. (Beide sind gegeben.)

Zur kürzeren Schreibweise führt man auch ein:

$$\vec{x} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \quad \text{Vektor der Unbekannten}$$

$$\vec{b} := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^m \quad \text{Vektor der rechten Seite}$$

$$A := \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in \mathbb{R}^{m \times n} \quad \text{Koeffizientenmatrix, Systemmatrix}$$

Merke:

m = Anzahl Zeilen = Anzahl Gleichungen,

n = Anzahl Spalten = Anzahl Unbekannte,

Der Zeilenindex kommt immer vor dem Spaltenindex: a_{ij}

$(A|\vec{b}) \in \mathbb{R}^{m \times (n+1)}$ bezeichnet man als *erweiterte Koeffizientenmatrix*.

In obigem Beispiel:

$$A = \begin{pmatrix} 1 & -2 & -2 \\ 1 & 3 & 2 \\ -5 & 20 & 15 \end{pmatrix}, \quad (A|b) = \left(\begin{array}{ccc|c} 1 & -2 & -2 & 2 \\ 1 & 3 & 2 & 22 \\ -5 & 20 & 15 & 30 \end{array} \right)$$

Die erweiterte Koeffizientenmatrix enthält offensichtlich alle gegebenen Daten eines LGS.

Ziele/Fragestellungen:³⁸

³⁷Anwendungen: Gleichungssysteme mit (deutlich) mehr als 3 Gleichungen/Unbekannten kommen in vielen Gebieten vor, z.B. bei der Berechnung von Stabwerken in der Mechanik (die Unbekannten sind die Spannungen und die Verschiebungen), bei der Berechnung von elektrischen Netzwerken (die Unbekannten sind Spannungen, Stromstärken und el. Potenziale), und auch, nach einer sog. Diskretisierung, bei der Berechnung von Strömungsvorgängen; dort geht die Anzahl der Gleichungen/Unbekannten oft in die Millionen.

³⁸Die evtl. auch aus der Schule bekannten Verfahren haben Nachteile: Die Cramer'sche Regel funktioniert nur, wenn $n = m$ und $\det(A) \neq 0$ und ist außerdem für $n > 3$ viel zu aufwändig, da $n+1$

- Suche allgemeine Lösungsverfahren für LGS
 - für allgemeine $m \times n$ -Matrizen,
 - mit akzeptablem Aufwand
- Eindeutigkeit der Lösung? Existenz einer Lösung? (allg.: Lösungsmenge?)

Vorgehensweise:

Umformung des LGS in ein leichter zu lösendes LGS

- 1. Welche Typen von LGS sind leicht zu lösen?
- 2. Wie formen wir die gegebenen LGS um?

Systeme, die leicht zu lösen sind: Systeme mit *Stufenform*:

Typ I: Alle Stufen haben Höhe und Breite 1, unterhalb der Stufen (der Diagonale der Systemmatrix) stehen nur Nullen, auf der Diagonalen stehen von Null verschiedene Einträge $a_{ii} \neq 0$, insbesondere sei $m \geq n$ vorausgesetzt; im Fall $m > n$ sind unten $m - n$ viele Nullzeilen enthalten:

$$(A|b) = \left(\begin{array}{cccc|c} \boxed{*} & & & & * \\ & \boxed{*} & & & \\ & & * & & \\ & & & \boxed{*} & \\ & 0 & & & \boxed{*} \\ & & & & 0 \end{array} \right) \left. \vphantom{\begin{array}{c} \\ \\ \\ \\ \\ \end{array}} \right\} m$$

$*$ = beliebiger Wert
 $\boxed{*}$ = Wert, der sicher $\neq 0$ ist

Bsp.: $\left(\begin{array}{ccc|c} \underline{3} & 4 & 1 & -1 \\ 0 & \underline{2} & 5 & 8 \\ 0 & 0 & \underline{3} & 6 \end{array} \right)$ d.h. $\begin{cases} 3x_1 + 4x_2 + x_3 = -1 \\ 2x_2 + 5x_3 = 8 \\ 3x_3 = 6 \end{cases} \iff \begin{cases} x_1 = \frac{1}{3}(-1 - 4x_2 - x_3) = \frac{1}{3} \\ x_2 = \frac{1}{2}(8 - 5x_3) = -1 \\ x_3 = \frac{6}{3} = 2 \end{cases}$

Dieses Bestimmen der Unbekannten von unten nach oben heißt *Rückwärtseinsetzen*.
Für Stufenform vom Typ I existiert genau eine Lösung.

Typ I heißt **eindeutiger Typ**.

Algorithmus Rückwärtseinsetzen für Stufenformen vom Typ I:

```

Fuer i von n rueckwaerts bis 1 (Zeilenindex)
{ x(i):=b(i)
  Fuer j von i+1 bis n (Spaltenindex)
    x(i):=x(i)-A(i,j)*x(j)
  x(i):=x(i)/A(i,i)
}
  
```

Determinanten berechnet werden müssen. (Und die Sarrus-Regel zur effizienten Berechnung von Determinanten gilt nur für $n=m=3$.) Die Methode, sukzessive eine Gleichung nach einer Unbekannten aufzulösen und diese in den verbleibenden Gleichungen zu eliminieren, ist für große n, m ebenfalls zu aufwändig.

Typ II: Es gibt mindestens eine Stufe der Breite > 1 ; in der b -Spalte fängt keine neue Stufe an:

$$(A|b) = \begin{matrix} 1 \{ \\ 1 \{ \\ 1 \{ \\ 1 \{ \end{matrix} \left(\begin{array}{cccc|c} \boxed{*} & * & & * & * \\ & \boxed{*} & & & \\ & & \boxed{*} & * & * \\ 0 & & & \boxed{*} & 0 \end{array} \right)$$

$\underbrace{\hspace{10em}}_{>1}$

Bsp.:

$$\left(\begin{array}{ccccc|c} \underline{4} & -3 & 4 & 0 & -1 & -8 \\ 0 & 0 & \underline{2} & \underline{2} & 1 & 14 \\ 0 & 0 & 0 & 0 & \underline{2} & \underline{4} \end{array} \right) \text{ d.h. } \begin{array}{l} 4x_1 - 3x_2 + 4x_3 - x_5 = -8 \\ 2x_3 + 2x_4 + x_5 = 14 \\ 2x_5 = 4 \end{array} \iff \begin{array}{l} x_1 = \frac{1}{4}(-8 + 3x_2 - 4x_3 + x_5) \\ x_3 = \frac{1}{2}(14 - 2x_4 - x_5) \\ x_5 = 2 \end{array}$$

$\begin{matrix} \uparrow & \uparrow & \uparrow \\ 1. & 3. & 5. \end{matrix}$

$x_2, x_4 \in \mathbb{R}$ können frei gewählt werden.

Die Komponenten x_1, x_3, x_5 ergeben sich dann wie oben.

→ **Es existieren unendlich viele Lösungen.**

Typ II heißt *mehrdeutiger Typ*.

Bestimmung der Lösungsmenge (von unten nach oben vorgehend):

$$x_1 = -2 + \frac{3}{4}x_2 - x_3 + \frac{1}{4}x_5 = -2 + \frac{3}{4}\lambda_2 - 6 + \lambda_1 + \frac{1}{2} = -\frac{15}{2} + \frac{3}{4}\lambda_2 + \lambda_1$$

$$x_2 = \lambda_2$$

$$x_3 = 7 - x_4 - \frac{1}{2}x_5 = 7 - \lambda_1 - 1 = 6 - \lambda_1$$

$$x_4 = \lambda_1$$

$$x_5 = 2$$

wobei $\lambda_1, \lambda_2 \in \mathbb{R}$ beliebig

$$\implies L = \left\{ \left(\begin{array}{c} -\frac{15}{2} + \lambda_1 + \frac{3}{4}\lambda_2 \\ \lambda_2 \\ 6 - \lambda_1 \\ \lambda_1 \\ 2 \end{array} \right) \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\}$$

Typ III:

$$(A|b) = \begin{matrix} \rightarrow & \left(\begin{array}{cccc|c} \boxed{*} & * & & * & * \\ & \boxed{*} & & & \\ & & \boxed{*} & * & * \\ 0 & & & \boxed{*} & 0 \end{array} \right) & \leftarrow \end{matrix}$$

Stufenform, bei der sich in der Spalte der rechten Seite eine Stufe befindet, d.h. es gibt eine Gleichung der Form

$$\underbrace{0 \cdot x_1 + 0 \cdot x_2 + \dots + 0 \cdot x_n}_{=0} = b_r \quad \text{mit} \quad b_r \neq 0$$

\implies **Es existiert keine Lösung.**

Typ III heißt **nicht lösbarer Typ**.

- Fazit soweit: Wir können für die 3 Stufenformen (Typ I,II,III) die Lösungsmenge leicht bestimmen.
- Nun: Transformiere *beliebiges* gegebenes LGS auf Stufenform unter Verwendung von *Äquivalenzumformungen*. Diese ändern die Lösungsmenge nicht.
- Einige einfache Äquivalenzumformungen für LGS sind:
 1. Vertauschen von Zeilen
 2. Multiplikation einer Zeile mit einem Faktor $\alpha \neq 0$
 3. Addition des α -fachen ($\alpha \in \mathbb{R}$) der i -ten Zeile zur j -ten Zeile ($i \neq j$)

Die Transformationen (1)-(3) heißen *elementare Zeilenumformungen*.

Dass 1. und 2. *Äquivalenzumformungen* sind, ist offensichtlich. 3. ist ebenfalls Äquivalenzumformung, denn man kann die Operation durch Subtraktion des α -fachen der i -ten Zeile von der j -ten Zeile rückgängig machen.

\implies Bringe also ein gegebenes (ggf. voll besetztes) LGS auf Stufenform durch elementare Zeilenumformungen.

Erzeuge dazu Nullen im linken unteren Bereich des Schemas.

Wir bringen ein LGS mit Hilfe von elementaren Zeilenumformungen auf Stufenform:

$$\begin{aligned} & \left(\begin{array}{ccc|c} 0 & 0 & -3 & 2 & 4 \\ 1 & 2 & 3 & -1 & 5 \\ 2 & 4 & -9 & 3 & 10 \end{array} \right) \xrightarrow{(I) \leftrightarrow (II)} \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 2 & 4 & -9 & 3 & 10 \end{array} \right) \xrightarrow{(III) \leftarrow (III) - 2 \cdot (I)} \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 0 & 0 & -15 & 5 & 0 \end{array} \right) \\ & \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 0 & 0 & -15 & 5 & 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 0 & 0 & -15 & 5 & 0 \end{array} \right) \\ & \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 0 & 0 & -15 & 5 & 0 \end{array} \right) \xrightarrow{(III) \leftarrow (III) - 5 \cdot (II)} \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 0 & 0 & 0 & -5 & -20 \end{array} \right) \\ & \implies \left(\begin{array}{ccc|c} 1 & 2 & 3 & -1 & 5 \\ 0 & 0 & -3 & 2 & 4 \\ 0 & 0 & 0 & -5 & -20 \end{array} \right) \text{ Stufenform Typ II} \end{aligned}$$

Der Gauß-Algorithmus (Gauß'sches Eliminationsverfahren, Gauß-Elimination):

Mit Worten, als rekursiver Algorithmus:

Gauss($A|b$):

Solange das Schema aus ≥ 1 Spalten besteht:

- Falls die erste Spalte von (A, b) aus lauter Nullen besteht:
 - Wende Gauss auf das Schema an, das bei Streichen der ersten Spalte entsteht.
- Andernfalls (es ist also mindestens ein Eintrag der 1. Spalte $\neq 0$):
 - Falls der linke obere Eintrag des Schemas $= 0$ ist, tausche die erste Zeile mit einer weiter unter stehenden Zeile, deren erster Eintrag $\neq 0$ ist (danach ist sicher der linke obere Eintrag des Schemas $\neq 0$)
 - Für alle Zeilen i unterhalb der ersten: Subtrahiere das a_{i1}/a_{11} -fache der ersten Zeile von der j -ten Zeile (unterhalb des linken oberen Eintrags sind jetzt Nullen)
 - Wende den Algorithmus nun auf das Schema an, das entsteht, wenn man die erste Zeile und die erste Spalte weglässt

Als Code (setzen voraus, dass b als $n+1$ -te Spalte der Matrix A gespeichert ist):

```
i0:=1 (Zeile der aktuellen Stufe)
Fuer j0 von 1 bis n+1 (Spalte, in der Stufe gebildet und Nullen erzeugt werden)
{ (suche Element  $\neq 0$  in der j0-ten Spalte:)
  i1:=i0
  Solange A(i1,j0)=0 und i1<=m: i1:=i1+1
  Wenn i0<i1<=m (Element  $\neq 0$  gefunden, tausche Zeilen i1 und i0:)
  { Fuer j von j0 bis n+1:
    { tmp:=A(i1,j); A(i1,j):=A(i0,j); A(i0,j)=tmp }
  }
  Wenn i0<=m: (andernfalls wurde kein von null verschiedener Eintrag gefunden,
  { Spalte j0 bekommt keine Stufe, und man geht weiter zu Spalte j0+1)
  (nun ist A(i0,j0) ungleich 0, erzeuge nun Nullen unterhalb durch
  Subtraktion eines Vielfachen der i0-ten von der i-ten Zeile:)
  Fuer i von i0+1 bis m: (Zeile)
  { faktor:=A(i,j0)/A(i0,j0)
    Fuer j von j0 bis n+1: (Spalte)
      A(i,j):=A(i,j)-faktor*A(i,j0)
    }
  }
  i0:=i0+1 (naechste Stufe muss um 1 tiefer liegen)
  Falls i0>m dann fertig.
}
```

}

Algorithmus im Spezialfall, dass die Matrix quadratisch ist ($m = n$) und keine Zeilenvertauschungen nötig werden:

```
Fuer i0 von 1 bis n (Spalte, in der Nullen erzeugt werden sollen)
{ Wenn A(i0,i0)=0 dann
  { schreibe('Ich will nicht durch null dividieren!'); exit; }
  Fuer i von i0+1 bis n (Zeile)
  { faktor:=A(i,i0)/A(i0,i0)
    Fuer j von i0 bis n+1
      A(i,j):=A(i,j)-faktor*A(i0,j) (subtr. Vielfaches von Zeile i0 von Zeile i)
  }
}
```

Aufwand. In der innersten Schleife werden $n+2-i_0$ Multiplikationen und Subtraktionen durchgeführt. Insgesamt jeweils

$$\begin{aligned} \sum_{i_0=1}^n \sum_{i=i_0+1}^n n+2-i_0 &= \sum_{i_0=1}^n (n-i_0)(n+2-i_0) = \sum_{\tilde{i}_0=0}^{n-1} \tilde{i}_0 (2+\tilde{i}_0) \\ &= 2 \sum_{\tilde{i}_0=0}^{n-1} \tilde{i}_0 + \sum_{\tilde{i}_0=0}^{n-1} \tilde{i}_0^2 = n(n-1) + \frac{n-1}{6}n(2n-1) \approx \frac{1}{3}n^3 \end{aligned}$$

Multiplikationen und Subtraktionen für großes n (die Berechnung von 'faktor' fällt nicht weiter ins Gewicht für großes n). Das Rückwärtseinsetzen anschließend benötigt nur ca. $\frac{1}{2}n^2$ Additionen und Multiplikationen jeweils, d.h. es ist gegenüber dem Aufwand $\frac{1}{3}n^3$ zu vernachlässigen für großes n .

Verallgemeinerung. Die Koeffizienten und die rechten Seiten des LGS müssen nicht unbedingt reelle Zahlen sein, es reicht, wenn die $a_{ij} \in \mathbb{K}$, $b_j \in \mathbb{K}$ gegeben sind, wobei \mathbb{K} ein beliebiger Körper ist, und die Unbekannten x_i ebenfalls in \mathbb{K} gesucht werden.

Hinsichtlich von Anwendungen von Linearen Gleichungssystemen über Körpern $\mathbb{K} \neq \mathbb{R}$ lassen sich *Wechselstromnetzwerke* nennen (Netzwerke von Leitern, in denen Spulen, Kondensatoren, Ohmsche Widerstände und Wechselstromspannungsquellen eingebaut sind); diese führen auf Lineare Gleichungssysteme über dem Körper $\mathbb{K} = \mathbb{C}$. (Wechselstrom kann mittels einer Amplitude und einer 'Phase' beschrieben werden, also mit einer komplexen Zahl (Amplitude=Betrag, Phase=Argument)).

Spaltenvertauschungen. In vielen Büchern und Skripten ist im Zusammenhang mit dem Gauß-Verfahren nicht nur von Zeilen-, sondern auch von Spaltenvertauschungen die Rede. Dabei ist folgendes zu beachten: Jede Spalte eines LGS enthält die Koeffizienten, die zu einer bestimmten Unbekannten gehören. So ohne weiteres ist demnach das Vertauschen von Spalten *nicht* erlaubt, da es die Lösungsmenge verändert. (Ist z.B. $\vec{x} = (1, 2, 3)^T$ eine Lösung eines LGS, so hat dasjenige LGS, das durch Vertauschung der ersten beiden Spalten entsteht, die Lösung $\vec{x} = (2, 1, 3)^T$.) Wenn man also Spalten

vertauschen möchte, so muss man dies "mitprotokollieren", z.B. indem man sich merkt, welche Unbekannte zu welcher Spalte der Systemmatrix gehört. So kann man z.B. durch zwei Spaltentausche folgendes System auf Stufenform bringen und die Lösung berechnen:³⁹

$$\begin{array}{cccc|c}
 x_1 & x_2 & x_3 & x_4 & \\
 \hline
 1 & 0 & 0 & 1 & 2 \\
 2 & 1 & 3 & 0 & 8 \\
 1 & 0 & 4 & 0 & 9 \\
 0 & 0 & 5 & 0 & 10
 \end{array}
 \xrightarrow{S1 \leftrightarrow S4}
 \begin{array}{cccc|c}
 x_4 & x_2 & x_3 & x_1 & \\
 \hline
 1 & 0 & 0 & 1 & 2 \\
 0 & 1 & 3 & 2 & 8 \\
 0 & 0 & 4 & 1 & 9 \\
 0 & 0 & 5 & 0 & 10
 \end{array}
 \xrightarrow{S3 \leftrightarrow S4}
 \begin{array}{cccc|c}
 x_4 & x_2 & x_1 & x_3 & \\
 \hline
 1 & 0 & 1 & 0 & 2 \\
 0 & 1 & 2 & 3 & 8 \\
 0 & 0 & 1 & 4 & 9 \\
 0 & 0 & 0 & 5 & 10
 \end{array}$$

Rücksubstitution liefert die Unbekannten nun in dieser Reihenfolge: $x_3 = 2$, $x_1 = 9 - 4x_3 = 1$, $x_2 = 8 - 2x_1 - 3x_3 = 0$, $x_4 = 2 - x_1 = 1$.

Jedoch kann man beliebige Lineare Gleichungssysteme auch immer ohne Spaltenvertauschungen auf Stufenform bringen. Das Einbeziehen von Spaltenvertauschungen ermöglicht es lediglich, dass man immer eine spezielle Stufenform, die sogenannte Trapezform,

$$(A|\vec{b}) = \left(\begin{array}{cccc|c}
 \mathbb{K} & & & & * \\
 & \mathbb{K} & & & * \\
 & & \mathbb{K} & * & * \\
 & & & \mathbb{K} & * \\
 0 & & & & \frac{*}{0} \\
 & & & & 0
 \end{array} \right)$$

erreichen kann.

3.2 Vektorräume

3.2.1 Definition und Beispiele

Def. (Vektorraum). Sei \mathbb{K} ein Körper und V eine Menge mit einer Verknüpfung $+$: $V \times V \rightarrow V$ ('Vektoraddition'). Außerdem sei eine Verknüpfung \cdot : $\mathbb{K} \times V \rightarrow V$ ('Skalarmultiplikation') gegeben, und es gelte:

1. $(V, +)$ ist eine kommutative Gruppe.
2. Es gelten die Distributivgesetze

$$(\lambda + \mu) \vec{x} = \lambda \vec{x} + \mu \vec{x},$$

$$\lambda(\vec{x} + \vec{y}) = \lambda \vec{x} + \lambda \vec{y},$$

sowie das Assoziativgesetz

$$(\lambda \mu) \vec{x} = \lambda(\mu \vec{x})$$

sowie

$$1 \cdot \vec{x} = \vec{x},$$

für alle $\lambda, \mu \in \mathbb{K}$, $\vec{x}, \vec{y} \in V$.

Dann heißt V ein \mathbb{K} -Vektorraum (oder Vektorraum über dem Körper \mathbb{K}).

Die Elemente eines Vektorraums heißen *Vektoren*, die Elemente des zugrunde liegenden Körpers heißen *Skalare*.

³⁹Bemerkung: Auf das n -Tupel der Spalten werden *Transpositionen* angewendet; eine Hintereinanderschaltung von Transpositionen ergibt eine *Permutation* der Spalten, vgl. Kap. 1.5.

Bemerkung: Man kann aus den obigen 'Vektorraumaxiomen' herleiten, dass in jedem Vektorraum

$$0 \cdot \vec{x} = \vec{0}, \quad \lambda \cdot \vec{0} = \vec{0}, \quad -\vec{x} = (-1) \cdot \vec{x}$$

gilt für alle $\vec{x} \in V$, $\lambda \in \mathbb{K}$. Übrigens gilt $x \cdot 0 = 0 \cdot x = 0 \forall x \in \mathbb{K}$ auch in Körpern, ja sogar in Ringen.

Von nun an sei grundsätzlich immer $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$.

Zur Notation: In den Ingenieurwissenschaften ist es üblich, Vektoren mit einem 'Pfeil' zu kennzeichnen, also z.B. \vec{x} ; in Büchern auch manchmal ersetzt durch Fettdruck; in der Mathematik sind solche Schreibweisen eigentlich nicht üblich.

(Wichtigstes) Beispiel. Sei $n \in \mathbb{N}$. Die Menge aller n -Tupel

$$V := \mathbb{K}^n = \mathbb{K} \times \dots \times \mathbb{K} = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \dots, x_n \in \mathbb{K} \right\}$$

ist mit der komponentenweisen Addition

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

und der Skalarmultiplikation

$$\lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

ein \mathbb{K} -Vektorraum. Um Platz zu sparen schreibt man auch $(x_1, \dots, x_n)^T$ statt $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Bemerkung. Man kann soweit gehen zu sagen, dass die Menge aller n -Tupel mit den oben angegebenen Addition und Skalarmultiplikation als Prototyp/Vorlage bei der Festlegung des Begriffs 'Vektorraum' diene: Man frage sich, was sind die Eigenschaften/Rechenregeln bei der Addition und der Skalarmultiplikation von Tupeln, und in welchen anderen Mengen lässt sich ähnlich rechnen. Und all die Mengen, in denen man analog rechnen kann, fasst man unter dem Begriff 'Vektorräume' zusammen.

Weiteres Beispiel: Sei $M \neq \emptyset$ eine Menge und \mathbb{K} ein Körper und $\text{Abb}(M, \mathbb{K})$ die Menge aller Abbildungen von M nach \mathbb{K} . Dann ist $\text{Abb}(M, \mathbb{K})$ mit der Addition $(f + g)(x) := f(x) + g(x)$ und der Skalarmultiplikation $(\lambda \cdot f)(x) := \lambda \cdot f(x)$ ein \mathbb{K} -Vektorraum; also beispielsweise $\text{Abb}(\mathbb{R}, \mathbb{R})$.

Teilmengen von Vektorräumen sind oft ebenfalls Vektorräume:

3.2.2 Unterräume und affine Unterräume

Def. (Unterraum) Sei V ein \mathbb{K} -Vektorraum und $U \subseteq V$ eine nichtleere Teilmenge. U heißt *Unterraum* von V , falls für alle $\vec{x}, \vec{y} \in U$ und $\alpha \in \mathbb{K}$ gilt:

(i) $\vec{x} + \vec{y} \in U$

(ii) $\alpha \vec{x} \in U$.

(D.h. die Teilmenge U ist bzgl. der Vektoraddition und der Skalarmultiplikation *abgeschlossen*.)

Jeder Unterraum $U \subseteq V$ eines Vektorraums V ist mit der von V 'induzierten' ('ererbten') Vektoraddition und Skalarmultiplikation ein Vektorraum, denn: Die Unterraumaxiome (i) und (ii) stellen sicher, dass die Einschränkung der in V gegebenen Vektoraddition und der Skalarmultiplikation auf die Teilmenge U nicht aus U herausführt: $+ : U \times U \rightarrow U$, $\cdot : \mathbb{K} \times U \rightarrow U$. Die Eigenschaften der Verknüpfungen ('Vektorraumaxiome') bleiben bei der Einschränkung der Verknüpfungen von V auf U natürlich erhalten.

Bemerkung (Alternative Charakterisierung von Unterräumen). Eine Menge $U \subseteq V$ ist genau dann Unterraum des Vektorraums V , wenn

$$\forall \vec{x}, \vec{y} \in U, \alpha, \beta \in \mathbb{K} : \alpha \vec{x} + \beta \vec{y} \in U.$$

(Man kann leicht zeigen, dass diese Eigenschaft äquivalent ist zu obigem (i) \wedge (ii).)

Ein Kriterium, das manchmal nützlich ist, um zu zeigen, dass eine Teilmenge *kein* Unterraum ist:

Satz. Jeder Unterraum enthält den Nullvektor.

Begründung: Zum einen kann man so argumentieren: Jeder Unterraum ist Vektorraum, also insbesondere bezüglich der Addition eine Gruppe, muss also das additiv-neutrale Element $\vec{0}$ enthalten. Oder direkt mit der Unterraumeigenschaft (ii) mit $\alpha := 0$: Für beliebiges $\vec{x} \in U$ muss $\underbrace{0 \cdot \vec{x}}_{=\vec{0}} \in U$ sein.

Beispiele.

1. $\{\vec{0}\}$ sowie V sind immer Unterräume von V (die trivialen Unterräume).

2. Nach Unterraumeigenschaft (ii) muss mit einem Element auch jedes skalare Vielfache des Elements im Unterraum sein. Unterräume des \mathbb{R}^2 sind also alle Ursprungsgeraden! Außer den trivialen Unterräumen und den Ursprungsgeraden hat der \mathbb{R}^2 keine weiteren Unterräume! Geraden, die den Nullpunkt nicht enthalten, sind nach obigem Kriterium keine Unterräume.
3. Im \mathbb{R}^3 sind ebenfalls alle Ursprungsgeraden Unterräume. Daneben sind auch alle Ebenen, die den Nullpunkt enthalten, Unterräume. Weitere gibt es nicht (abgesehen von den trivialen $\{\vec{0}\}$ und \mathbb{R}^3).
4. Die Menge aller Polynome vom Grad $\leq n$ ($n \in \mathbb{N}$) ist ein Unterraum des Vektorraums $\text{Abb}(\mathbb{K}, \mathbb{K})$. Die Menge aller Polynome *beliebigen* Grades ebenfalls. Denn man prüft leicht nach: Die Summe zweier Polynome vom Grad $\leq n$ wie auch das skalare Vielfache eines Polynoms vom Grad $\leq n$ sind wieder Polynome vom Grad $\leq n$, und entsprechendes gilt für Polynome *beliebigen* Grades. (Die Menge aller Polynome mit *festem* Grad n jedoch bilden *keinen* Vektorraum. Warum?) Auch die Menge aller (Vorgriff auf 2. Semester bzw. Rückgriff auf Schule) 'stetigen' Funktionen von \mathbb{R} nach \mathbb{R} bilden einen Unterraum von $\text{Abb}(\mathbb{R}, \mathbb{R})$, ebenso die Menge aller 'differenzierbaren' Funktionen... Es gibt wahnsinnig viele Unterräume von $\text{Abb}(\mathbb{R}, \mathbb{R})$.
5. Ein LGS heißt *homogen*, wenn die rechten Seiten alle gleich null sind, andernfalls *inhomogen*. Die Lösungsmenge L eines homogenen LGS $(A|\vec{0})$, $A \in \mathbb{K}^{m \times n}$, ist ein Unterraum des \mathbb{K}^n .
Beweis: Sei $\alpha \in \mathbb{K}$ und seien \vec{x} und \vec{y} Lösungen des homogenen LGS, also

$$\sum_{j=1}^n a_{ij}x_j = 0 \quad \text{und} \quad \sum_{j=1}^n a_{ij}y_j = 0, \quad i = 1, \dots, m.$$

Addition der beiden Gleichungen liefert

$$0 = \sum_{j=1}^n a_{ij}x_j + \sum_{j=1}^n a_{ij}y_j = \sum_{j=1}^n a_{ij} \underbrace{(x_j + y_j)}_{\substack{\text{Komp. des} \\ \text{Vektors } \vec{x} + \vec{y}}}$$

Also: $\vec{x} + \vec{y}$ ist Lösung des LGS.

$$\text{Analog: } 0 = \alpha \sum_{j=1}^n a_{ij}x_j = \sum_{j=1}^n a_{ij}(\alpha x_j)$$

Also: $\alpha \vec{x}$ ist Lösung des LGS.

Es folgt, dass $\vec{x} + \vec{y} \in L$ und $\alpha \vec{x} \in L$, also ist L Unterraum.

Man sieht, dass das Nachrechnen der Unterraumeigenschaften viel weniger Arbeit ist als das Nachrechnen sämtlicher Vektorraumaxiome! Also, um zu zeigen, dass eine Menge ein Vektorraum ist, versuche, eine Obermenge zu finden, von der bereits bekannt ist, dass sie ein Vektorraum ist!

Beachte: Die Lösungsmenge eines *inhomogenen* LGS ist kein Unterraum!

Grund: Angenommen, L sei ein Unterraum. Dann muss $\vec{0} \in L$ sein. Aber Einsetzen des

Nullvektors ins inhomogene LGS zeigt, dass $\underbrace{\sum_{j=1}^n a_{ij} \cdot 0}_{=0} = b_i \quad \forall i = 1, \dots, m$, und da im

inhomogenen System mindestens eines der $b_i \neq 0$ ist, kann der Nullvektor nicht Lösung sein. Widerspruch.

Jedoch lässt sich einiges sagen über die

Struktur von Lösungsmengen linearer Gleichungssysteme:

Sei $(A|\vec{b})$ ein LGS, $A \in \mathbb{K}^{m \times n}$, $\vec{b} \in \mathbb{K}^m$. Sei L die Lösungsmenge, und sei L_{hom} die Lösungsmenge des zugehörigen homogenen LGS $(A|\vec{0})$. Sei $\vec{x} \in L$ eine beliebige, feste Lösung des inhomogenen LGS⁴⁰. Dann gilt

$$L = \{\vec{x}\} + L_{hom},$$

d.h.

$$L = \{\vec{x} + \vec{y} \mid \vec{y} \in L_{hom}\}.$$

Da L_{hom} ein Unterraum ist, handelt es sich bei L also um einen (um den Vektor x) *verschobenen* Unterraum.

Eine solche Menge, also ein um einen festen Vektor verschobener Unterraum, nennt man auch *affinen (Unter-)Raum* oder *affin-linearen Raum* (also: ein affiner Vektorraum ist kein Vektorraum). Beispiele: Geraden und Ebenen im \mathbb{R}^n (die nicht notwendigerweise den Nullpunkt enthalten) sind affine Räume.

Obige Formel für den Zusammenhang von L_{hom} und L besagt bzw. aus ihr kann man folgern:

- Die Summe einer Lösung des homogenen LGS und einer Lösung des inhomogenen LGS ist immer eine Lösung des inhomogenen LGS.
- Sobald man die Lösungsmenge des homogenen LGS sowie eine einzige Lösung des inhomogenen LGS kennt, kennt man die gesamte Lösungsmenge des inhomogenen LGS.
- Die Differenz zweier Lösungen des inhomogenen Systems ist Lösung des homogenen Systems. (x auf die linke Seite gebracht)
- Abändern der rechten Seite eines LGS unter Beibehaltung der Systemmatrix A 'verschiebt' die Lösungsmenge um einen festen Vektor.

Zum Beweis der obigen Formel: Wir wollen die Gleichheit obiger Mengen zeigen. Dies geschieht in zwei Schritten:

⁴⁰Eine feste, aber beliebige Lösung eines LGS bezeichnet man auch als *partikuläre* Lösung.

$L \supseteq \{\vec{x}\} + L_{hom}$: Sei $\vec{z} \in \{\vec{x}\} + L_{hom}$, also $\vec{z} = \vec{x} + \vec{y}$, wobei $\vec{y} \in L_{hom}$. Das bedeutet:

$$\sum_{j=1}^n a_{ij}x_j = b_i \quad \text{und} \quad \sum_{j=1}^n a_{ij}y_j = 0, \quad i = 1, \dots, m.$$

Durch Addition folgt

$$b_i = b_i + 0 = \sum_{j=1}^n a_{ij}x_j + \sum_{j=1}^n a_{ij}y_j = \sum_{j=1}^n a_{ij}(x_j + y_j) = \sum_{j=1}^n a_{ij}z_j,$$

also: $\vec{z} \in L$.

$L \subseteq \{\vec{x}\} + L_{hom}$: Sei $\vec{z} \in L$, also

$$\sum_{j=1}^n a_{ij}z_j = b_i, \quad i = 1, \dots, m;$$

sowie nach Voraussetzung

$$\sum_{j=1}^n a_{ij}x_j = b_i, \quad i = 1, \dots, m;$$

Wir müssen zeigen, dass sich \vec{z} als $\vec{z} = \vec{x} + \vec{y}$ schreiben lässt, wobei $\vec{y} \in L_{hom}$. Gleichbedeutend ist: $\vec{z} - \vec{x} \in L_{hom}$. Und in der Tat:

$$\sum_{j=1}^n a_{ij}(z_j - x_j) = \sum_{j=1}^n a_{ij}z_j - \sum_{j=1}^n a_{ij}x_j = b_i - b_i = 0, \quad i = 1, \dots, m,$$

also $\vec{z} - \vec{x} \in L_{hom}$.

Beispiel. Das LGS

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

hat $x_3 = \lambda \in \mathbb{R}$ frei wählbar, $x_2 = 2 - \lambda$, $x_1 = 1 + 2(2 - \lambda) - 4\lambda = 5 - 6\lambda$, also, die Lösungsmenge

$$L = \left\{ \left(\begin{array}{c} 5 - 6\lambda \\ 2 - \lambda \\ \lambda \end{array} \right) \mid \lambda \in \mathbb{R} \right\}.$$

Das zugehörige homogene System

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

hat

$$L_{hom} = \left\{ \begin{pmatrix} -6\lambda \\ -\lambda \\ \lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}.$$

Man kann umschreiben

$$L = \left\{ \begin{pmatrix} 5 \\ 2 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} -6 \\ -1 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

und

$$L_{hom} = \left\{ \lambda \begin{pmatrix} -6 \\ -1 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

also in der Tat $L = \{(5, 2, 0)^T\} + L_{hom}$, wobei $(5, 2, 0)^T$ die partikuläre Lösung ist. (Natürlich hätte man auch eine andere partikuläre Lösung zur Darstellung von L nehmen können, so ist z.B., mit $\lambda := 1$, auch $(-1, 1, 1)^T \in L$, d.h. man kann auch $L = \{(-1, 1, 1)^T + \lambda(-6, -1, 1)\} = \{(-1, 1, 1)^T\} + L_{hom}$ schreiben.)

3.2.3 Lineare Unabhängigkeit, Erzeugendensysteme, Basen, Dimension

Def. (Linearkombination, Lineare (Un-)Abhängigkeit) Seien $\vec{v}_1, \dots, \vec{v}_n$ Elemente eines \mathbb{K} -Vektorraums V gegeben. Vektoren der Bauart $\sum_{i=1}^n \alpha_i \vec{v}_i$, wobei $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, heißen *Linearkombinationen* (kurz: LK) der Vektoren $\vec{v}_1, \dots, \vec{v}_n$. Die Linearkombination mit $\alpha_1 = \dots = \alpha_n = 0$ heißt *triviale Linearkombination*.

Die Vektoren $\vec{v}_1, \dots, \vec{v}_n$ heißen *linear abhängig*, wenn es eine nichttriviale LK gibt, die den Nullvektor ergibt, also wenn es $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, nicht alle = 0, gibt, so dass $\sum_{i=1}^n \alpha_i \vec{v}_i = \vec{0}$.

Andernfalls, also wenn nur die triviale LK den Nullvektor ergibt, heißen die Vektoren *linear unabhängig*.

Geometrische Deutung. Die Lineare Abhängigkeit von Vektoren $\vec{v}_1, \dots, \vec{v}_n$ bedeutet, dass sich (mindestens) einer der Vektoren als LK der anderen schreiben lässt. Ist z.B. $v_1 + 0 \cdot \vec{v}_2 + 3\vec{v}_3 = \vec{0}$ (die Vektoren sind also linear abhängig, da eine nichttriviale LK den Nullvektor ergibt), so kann man z.B. $\vec{v}_1 = 0\vec{v}_2 - 3\vec{v}_3$ oder auch $\vec{v}_3 = -\frac{1}{3}\vec{v}_1 + 0\vec{v}_2$ (aber man kann hier nicht \vec{v}_2 als LK der beiden anderen schreiben!).

Geometrisch bedeutet die Lineare Abhängigkeit von 3 Vektoren im \mathbb{R}^3 (also einer ist LK der beiden anderen), dass die 3 Vektorpfeile in einer Ebene liegen. Die Lineare Abhängigkeit von 2 Vektoren im \mathbb{R}^3 oder im \mathbb{R}^2 bedeutet, dass sie auf einer Geraden liegen, also die gleiche Richtung haben (ggf. unterschiedliche Orientierung).

Die Überprüfung der linearen Unabhängigkeit kann mit Hilfe eines (homogenen) LGS erfolgen:

Beispiel. Sind die Vektoren $\vec{v}_1 = (1, 2, 0)^T$, $\vec{v}_2 = (2, 1, 1)^T$, $\vec{v}_3 = (4, 5, 1)^T$ linear (un-)abhängig? Es ist also zu prüfen, ob die Gleichung

$$\alpha_1 \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + \alpha_3 \begin{pmatrix} 4 \\ 5 \\ 1 \end{pmatrix} = \vec{0}$$

nur die 'triviale' Lösung $(\alpha_1, \alpha_2, \alpha_3)^T = (0, 0, 0)$ hat. Diese Vektorgleichung kann als System von 3 skalaren Gleichungen aufgefasst werden:

$$\begin{aligned} \alpha_1 + 2\alpha_2 + 4\alpha_3 &= 0 \\ 2\alpha_1 + \alpha_2 + 5\alpha_3 &= 0 \\ \alpha_2 + \alpha_3 &= 0 \end{aligned}$$

also kurz:

$$\left(\begin{array}{ccc|c} 1 & 2 & 4 & 0 \\ 2 & 1 & 5 & 0 \\ 0 & 1 & 1 & 0 \end{array} \right)$$

Mit dem Gauß-Algorithmus sieht man, dass es Lösungen

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \lambda \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}, \quad \lambda \in \mathbb{R},$$

gibt, also nichttriviale Lösungen, wie z.B. $(\alpha_1, \alpha_2, \alpha_3)^T = (2, 1, -1)^T$. Die Vektoren sind also linear abhängig; es gilt

$$2\vec{v}_1 + \vec{v}_2 - \vec{v}_3 = \vec{0}.$$

Der obige Rechenweg zeigt: $n+1$ (oder mehr) Vektoren im \mathbb{K}^n sind immer linear abhängig: Denn das obige homogene LGS hat in dieser Situation mehr Spalten als Zeilen, d.h. es muss in der zugehörigen Stufenform mindestens eine Stufe der Breite > 1 geben, d.h. der *mehrdeutige* Typ liegt vor⁴¹, und somit gibt es nichttriviale Lösungen, d.h. die Vektoren sind linear abhängig.⁴²

Def. (Erzeugendensystem) Vektoren $\vec{v}_1, \dots, \vec{v}_n$ eines Vektorraums V mit der Eigenschaft, dass sich *jeder* Vektor $\vec{x} \in V$ als Linearkombination der \vec{v}_i darstellen lässt, heißt *Erzeugendensystem* (EZS) von V .

⁴¹Beachte, dass wir hier die Homogenität des LGS ausgenutzt haben: Ein inhomogenes LGS könnte auch vom unlösbaren Typ sein.

⁴²Beachte, dass die ggf. aus der Schule bereits bekannte Methode, mittels Berechnung einer sog. *Determinante* (siehe Kap. 3.5) die Lineare Unabhängigkeit zu überprüfen, beschränkt ist auf den Fall von genau n Vektoren im \mathbb{K}^n , wohingegen obige Methode auch für m Vektoren im \mathbb{K}^n funktioniert.

Beispiel. Die Vektoren $(1, 0, 0)^T$, $(0, 1, 0)^T$, $(0, 0, 1)^T$ bilden ein EZS des \mathbb{R}^3 , denn: Jeder Vektor $x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ lässt sich als LK

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

schreiben.

Dies ist natürlich nicht das einzige EZS des \mathbb{R}^n ; es gibt im \mathbb{R}^3 sogar Erzeugendensysteme mit mehr als 3 Elementen, so kann man z.B. zu obigem EZS einen *beliebigen* vierten Vektor hinzufügen, und es bleibt offensichtlich weiterhin ein EZS.

Wie bestimmt man allgemein, ob Vektoren ein EZS bilden? Man kann dazu ebenfalls ein LGS aufstellen, bei dem auf der rechten Seite ein allgemeiner Vektor $(x_1, \dots, x_n)^T$ steht. Falls es für jede rechte Seite eine Lösung gibt, handelt es sich um ein EZS.⁴³

Def. (Spann/Lineare Hülle) Die Menge aller Linearkombinationen eines Systems von Vektoren heißt *Spann* oder der *von den Vektoren erzeugte/aufgespannte Raum* oder die *lineare Hülle* der Vektoren:⁴⁴

$$\text{span}\{\vec{v}_1, \dots, \vec{v}_n\} := \{\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n \mid \alpha_1, \dots, \alpha_n \in \mathbb{K}\}$$

Eine lineare Hülle ist immer ein Vektorraum, und zwar der kleinste Vektorraum, der die aufspannenden Vektoren $\vec{v}_1, \dots, \vec{v}_n$ enthält. Trivialerweise bilden $\vec{v}_1, \dots, \vec{v}_n$ immer ein EZS von $\text{span}\{\vec{v}_1, \dots, \vec{v}_n\}$.

Satz (einige Eigenschaften von Erzeugendensystemen und linear abhängigen/linear unabhängigen Vektoren)

1. Ist $\{\vec{v}_1, \dots, \vec{v}_n\}$ ein EZS eines Vektorraums und $\vec{v}_{n+1} \in V$ beliebig, so ist auch $\{\vec{v}_1, \dots, \vec{v}_n, \vec{v}_{n+1}\}$ ein EZS.
2. Sind die Vektoren $\{\vec{v}_1, \dots, \vec{v}_n\}$ linear abhängig und \vec{v}_{n+1} beliebig, so sind auch $\{\vec{v}_1, \dots, \vec{v}_n, \vec{v}_{n+1}\}$ linear abhängig.
3. Sind die Vektoren $\{\vec{v}_1, \dots, \vec{v}_{n-1}, \vec{v}_n\}$ linear unabhängig, so sind auch $\{\vec{v}_1, \dots, \vec{v}_{n-1}\}$ linear unabhängig.
4. Ein System von Vektoren $\{\vec{v}_1, \dots, \vec{v}_n\}$, bei dem einer der Vektoren der Nullvektor ist, ist immer linear abhängig.

⁴³Wir werden selten die Überprüfung der EZS-Eigenschaft in dieser Form durchführen, denn für viele Situationen werden wir Verfahren kennen lernen, die uns sogar eine *Basis* (Def. s.u.) liefern; eine Basis eines Vektorraums ist insbesondere auch ein EZS. In vielen Situationen ist die Frage nach einem EZS eines Raumes auch trivial, z.B. wenn ein Raum mittels erzeugender Vektoren gegeben ist, siehe "Lineare Hülle".

⁴⁴englisch: "span"

Beweis:

1. $\vec{x} = \alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n \Rightarrow \vec{x} = \alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n + 0 \cdot \vec{v}_{n+1}$
2. Gibt es $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, nicht alle gleich null, so dass $\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n = \vec{0}$, so sind auch $\alpha_1, \dots, \alpha_n, 0$ nicht alle null und es gilt $\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n + 0 \vec{v}_{n+1} = \vec{0}$
3. Angenommen, das verkürzte System $\vec{v}_1, \dots, \vec{v}_{n-1}$ sei linear abhängig. Dann ist nach Aussage 2 auch jedes verlängerte System, also insbesondere $\vec{v}_1, \dots, \vec{v}_n$, linear abhängig, was ein Widerspruch zur Voraussetzung ist.
4. Sei \vec{v}_{i_0} der Nullvektor. Wir geben einfach eine nichttriviale LK, die den Nullvektor ergibt, an:

$$0 \cdot \vec{v}_1 + \dots + 0 \cdot \vec{v}_{i_0-1} + 1 \cdot \underbrace{\vec{v}_{i_0}}_{=\vec{0}} + 0 \cdot \vec{v}_{i_0+1} + \dots + 0 \cdot \vec{v}_n = \vec{0}$$

Def. (Basis eines Vektorraums) Ein System von Vektoren, das (i) linear unabhängig ist und (ii) ein EZS bildet, heißt *Basis* (des Vektorraums). Die Anzahl der Elemente einer Basis heißt *Länge* der Basis.

Bemerkung. Nach unserer Definition sind Erzeugendensysteme und somit auch Basen immer aus *endlich* vielen Elementen bestehend. In diesem Sinne werden Räume wie $\text{Abb}(\mathbb{R}, \mathbb{R})$ keine Basis besitzen. Verallgemeinerungen des EZS- und des Basisbegriffs auf unendliche Systeme von Vektoren ist möglich; solche Betrachtungen fallen aber nicht mehr in das Gebiet der Linearen Algebra und gehören nicht in eine Grundlagenvorlesung.

Beispiel.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

sind linear unabhängig (das zugehörige homogene LGS hat bereits Stufenform, Typ I, also nur die triviale Lösung), und sie bilden ein EZS im \mathbb{R}^3 , wie oben bereits gezeigt. Sie bilden also eine Basis des \mathbb{R}^3 . Diese Basis wird auch die *Standardbasis* (oder die *kanonische Basis*) des \mathbb{R}^3 genannt. In jedem \mathbb{R}^n (und auch \mathbb{C}^n) kann man entsprechend eine solche (Standard-)Basis der Länge n bilden:

$$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \vec{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \dots, \quad \vec{e}_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

In jedem Vektorraum (außer dem Nullvektorraum $\{\vec{0}\}$) gibt es mehrere (sogar unendlich viele) Basen. Man sollte daher immer von *einer* Basis und niemals von *der* Basis eines VR sprechen. Ausnahme: *Die* Standardbasis.

Wir wollen nun den Begriff der *Dimension* eines Vektorraumes erklären: Die *Dimension* eines VR soll die *Länge einer Basis* des VR sein⁴⁵. Damit dieser Begriff wohldefiniert ist, müssen wir jedoch zunächst die Frage klären: Haben in einem VR alle Basen die gleiche Länge?

Dazu der folgende Hilfssatz:

Satz (das Austauschlemma). Sei $\mathcal{B}_1 := \{\vec{b}_1, \dots, \vec{b}_n\}$ eine Basis eines Vektorraums und sei \vec{v} ein Vektor mit einer Darstellung $\vec{v} = \sum_{i=1}^n c_i \vec{b}_i$, wobei $c_1 \neq 0$ sei. Dann ist auch $\mathcal{B}_2 := \{\vec{v}, \vec{b}_2, \dots, \vec{b}_n\}$ eine Basis.

Beweis. Es ist zu zeigen, dass \mathcal{B}_2 eine Basis ist.

Teil 1: Zeige Lineare Unabhängigkeit des Systems \mathcal{B}_2 :

Sei $\alpha_1 \vec{v} + \sum_{i=2}^n \alpha_i \vec{b}_i = \vec{0}$ (zu zeigen: $\alpha_1 = \dots = \alpha_n = 0$).

Mit Verwendung der Darstellung von \vec{v} ist dies äquivalent zu $\alpha_1 \sum_{i=1}^n c_i \vec{b}_i + \sum_{i=2}^n \alpha_i \vec{b}_i = \vec{0}$

$$\Leftrightarrow \alpha_1 c_1 \vec{b}_1 + \sum_{i=2}^n (\alpha_1 c_i + \alpha_i) \vec{b}_i = \vec{0}$$

Da diese Vektoren nach Voraussetzung eine Basis, also l.u., sind, sind die Koeffizienten alle null:

$$\alpha_1 c_1 = 0, \quad \alpha_1 c_i + \alpha_i = 0 \quad \forall i = 2, \dots, n$$

Da $c_1 \neq 0$ ist, folgt $\alpha_1 = 0$ und somit auch $\alpha_i = 0 \quad \forall i = 2, \dots, n$.

Teil 2: Zeige, dass \mathcal{B}_2 ein EZS ist:

Sei \vec{x} ein beliebiges Element des VR. Da \mathcal{B}_1 eine Basis ist, gibt es eine Darstellung $\vec{x} = \sum_{i=1}^n \alpha_i \vec{b}_i$. (zu zeigen: \vec{x} lässt sich auch bezüglich \mathcal{B}_2 darstellen)

Ich behaupte, dass die zugehörigen Koeffizienten $\beta_1 := \frac{\alpha_1}{c_1}$ und $\beta_i := \alpha_i - \beta_1 c_i$, $i = 2, \dots, n$ sind. Das überprüfen wir:

$$\vec{x} = \sum_{i=1}^n \alpha_i \vec{b}_i = \beta_1 c_1 \vec{b}_1 + \sum_{i=2}^n (\beta_i + \beta_1 c_i) \vec{b}_i = \beta_1 \underbrace{(c_1 \vec{b}_1 + \dots + c_n \vec{b}_n)}_{=\vec{v}} + \beta_2 \vec{b}_2 + \dots + \beta_n \vec{b}_n, \text{ d.h.}$$

\vec{x} lässt sich in der Tat als LK des Systems \mathcal{B}_2 darstellen, d.h. \mathcal{B}_2 ist ein EZS. \square

Wir können nun folgern:

Satz und Def. (Dimension) Alle Basen eines Vektorraums (sofern überhaupt endliche Basen existieren) haben die gleiche Länge. Die Länge der Basen eines

⁴⁵sofern der VR überhaupt eine Basis endlicher Länge hat

Vektorraums V heißt *Dimension* von V , $\dim(V) \in \mathbb{N}_0$. Hat ein Vektorraum keine Basis (aus endlich vielen Elementen), so heißt er *unendlichdimensional*; $\dim(V) = \infty$.

Beweis. Angenommen in einem VR haben wir zwei Basen $\vec{b}_1, \dots, \vec{b}_n$ und $\vec{v}_1, \dots, \vec{v}_n, \dots, \vec{v}_{n+m}$ mit $m > 0$, also Basen unterschiedlicher Länge.

Da $\vec{v}_1, \dots, \vec{v}_{n+m}$ eine Basis ist, lässt sich \vec{b}_1 als LK der \vec{v}_i darstellen. Mindestens einer der Koeffizienten ist dabei $\neq 0$ (da \vec{b}_1 als Element einer Basis $\neq \vec{0}$ ist). Nach eventueller Umnummerierung der \vec{v}_i sei \vec{v}_1 dasjenige Element mit Koeffizient $\neq 0$. Nach dem Austauschatz ist dann $\vec{b}_1, \vec{v}_2, \dots, \vec{v}_{n+m}$ eine Basis.

Daher lässt sich \vec{b}_2 als LK dieser Elemente darstellen. Dabei ist mindestens einer der Koeffizienten der \vec{v}_i ungleich null, denn wären diese alle null, so wäre \vec{b}_2 als Vielfaches von \vec{b}_1 dargestellt, also \vec{b}_1, \vec{b}_2 linear abhängig, und somit $\vec{b}_1, \dots, \vec{b}_n$ linear abhängig, was ein Widerspruch zur Voraussetzung ist. Nach eventueller Umnummerierung sei \vec{v}_2 dasjenige Element mit Koeffizient $\neq 0$. Nach dem Austauschatz ist dann $\vec{b}_1, \vec{b}_2, \vec{v}_3, \dots, \vec{v}_{n+m}$ eine Basis.

Und so fortfahrend enthält man, dass dann $\vec{b}_1, \dots, \vec{b}_n, \vec{v}_{n+1}, \dots, \vec{v}_{n+m}$ eine Basis ist. Da aber andererseits $\vec{b}_1, \dots, \vec{b}_n$ eine Basis ist, lässt sich z.B. \vec{v}_{n+1} als LK der $\vec{b}_1, \dots, \vec{b}_n$ schreiben: $\vec{v}_{n+1} = \alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n$; dabei sind nicht alle Koeffizienten gleich null, da $\vec{v}_{n+1} \neq \vec{0}$. Umgestellt ergibt dies $\alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n + (-1) \vec{v}_{n+1} + 0 \vec{v}_{n+2} + \dots + 0 \vec{v}_{n+m} = \vec{0}$. Das ist ein Widerspruch dazu, dass $\vec{b}_1, \dots, \vec{b}_n, \vec{v}_{n+1}, \dots, \vec{v}_{n+m}$ eine Basis ist. \square

Beispiele.

- Im \mathbb{R} -VR \mathbb{R}^n und im \mathbb{C} -VR \mathbb{C}^n kennen wir die kanonische Basis; diese hat die Länge n . Also ist

$$\dim(\mathbb{R}^n) = n, \quad \dim(\mathbb{C}^n) = n.$$

- Man kann zeigen, dass der Raum $\text{Abb}(\mathbb{R}, \mathbb{R})$ keine endliche Basis hat, es ist also $\dim(\text{Abb}(\mathbb{R}, \mathbb{R})) = \infty$.

Der Raum \mathbb{P}_n der Polynome vom Grad $\leq n$ bilden einen $n+1$ -dimensionalen Unterraum. Eine Basis bilden die $n+1$ Polynome $x \mapsto x^0, x \mapsto x^1, \dots, x \mapsto x^n$. Dass diese ein EZS bilden, ist trivial (jedes Polynom $p \in \mathbb{P}_n$ lässt sich offensichtlich als LK dieser Polynome schreiben). Dass sie linear unabhängig sind, kann man sich unter Verwendung des Fundamentalsatzes der Algebra überlegen.

- Haben wir einen Unterraum U eines Vektorraums V gegeben als $U = \text{span}\{\vec{v}_1, \dots, \vec{v}_n\}$, wobei die $\vec{v}_1, \dots, \vec{v}_n$ linear unabhängig sind, so ist $\dim(U) = n$.

Grund: Die \vec{v}_i bilden trivialerweise ein EZS von U , und zusammen mit der Linearen Unabhängigkeit bilden sie eine Basis der Länge n .

Wie wir praktisch die Lineare Unabhängigkeit von Vektoren nachweisen können, wissen wir bereits: mit einem LGS (s.o.)

Beispiel zur Berechnung der Dimension eines Raumes, dessen EZS gegeben ist, und Klärung verwandter Fragen.

Wir betrachten den Unterraum

$$U := \text{span} \left\{ \begin{pmatrix} 1 \\ 2 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 7 \\ 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ 3 \end{pmatrix} \right\} \subseteq \mathbb{R}^4$$

Wir bezeichnen die aufspannenden Vektoren von links nach rechts mit $\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4$.

Aufgabenstellungen: Bestimme die Dimension von U , gib insbesondere eine Basis von U an. Drücke jedes der \vec{v}_i durch diese Basis aus (d.h. als LK der Basisvektoren). Bestimme außerdem die Dimension von $\text{span}\{\vec{v}_1\}$, $\text{span}\{\vec{v}_1, \vec{v}_2\}$, $\text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$.

Wir berechnen zunächst, welche LK der \vec{v}_i den Nullvektor ergibt (wie bei der Prüfung der Linearen Unabhängigkeit):

$$\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 + \alpha_3 \vec{v}_3 + \alpha_4 \vec{v}_4 = \vec{0};$$

dies ist genau dann wenn $\vec{\alpha} := (\alpha_1, \alpha_2, \alpha_3, \alpha_4)^T$ das folgende homogene LGS erfüllt (welches wir mit dem Gauß-Verfahren lösen):⁴⁶

$$\begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 1 & 7 & 1 \\ 0 & 1 & 3 & -1 \\ 3 & 0 & 6 & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 3 & -1 \\ 0 & 1 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 3 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Wir haben eine Stufenform vom *mehrdeutigen* Typ, d.h. es gibt nichttriviale Lösungen, d.h. die Vektoren $\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4$ sind linear abhängig.

Indem wir uns einzelne Spalten 'wegdenken', erkennen wir (ohne den Gauß-Algorithmus erneut durchführen zu müssen): Auch $\vec{v}_1, \vec{v}_2, \vec{v}_3$ sind linear abhängig, \vec{v}_1, \vec{v}_2 sind linear unabhängig, \vec{v}_1 ist linear unabhängig, also $\dim(\text{span}\{\vec{v}_1\}) = 1$, $\dim(\text{span}\{\vec{v}_1, \vec{v}_2\}) = 2$. Berechnen wir die Lösungsmenge des LGS: $\alpha_3 = \lambda \in \mathbb{R}$ und $\alpha_4 = \mu \in \mathbb{R}$ können frei gewählt werden, $\alpha_2 = -3\lambda + \mu$, $\alpha_1 = -2\lambda - \mu$, also

$$\vec{\alpha} = \begin{pmatrix} -2\lambda - \mu \\ -3\lambda + \mu \\ \lambda \\ \mu \end{pmatrix} = \lambda \begin{pmatrix} -2 \\ -3 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} -1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad \lambda, \mu \in \mathbb{R}$$

sind Lösungen. Durch spezielle Wahl von λ, μ können wir \vec{v}_i durch andere \vec{v}_i ausdrücken: Mit $\lambda := 0, \mu := 1$ bekommen wir die Lösung $\vec{\alpha} = (-1, 1, 0, 1)^T$, d.h. $-\vec{v}_1 + \vec{v}_2 + \vec{v}_4 = \vec{0}$, also $\vec{v}_4 = \vec{v}_1 - \vec{v}_2$, also $\text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4\} = \text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$!

Mit $\lambda := 1, \mu := 0$ bekommen wir die Lösung $\vec{\alpha} = (-2, -3, 1, 0)^T$, d.h. $-2\vec{v}_1 - 3\vec{v}_2 + \vec{v}_3 = \vec{0}$,

⁴⁶Beim Gauß-Verfahren für *homogene* LGS braucht man die rechte Seite nicht hinzuschreiben, da bei der Umformung eine Nullspalte immer eine Nullspalte bleibt.

also $\vec{v}_3 = 2\vec{v}_1 + 3\vec{v}_2$, also $\text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3\} = \text{span}\{\vec{v}_1, \vec{v}_2\}$!

Somit

$$\dim(\text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4\}) = \dim(\text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}) = \dim(\text{span}\{\vec{v}_1, \vec{v}_2\}) = 2;$$

insbesondere ist $\{\vec{v}_1, \vec{v}_2\}$ (wegen der Linearen Unabhängigkeit dieser Vektoren) eine Basis von U .

Wir fassen zusammen:

Vektoren des \mathbb{K}^n sind genau dann linear abhängig, wenn das zugehörige homogene LGS, das entsteht, wenn man die Vektoren als Spalten der Systemmatrix nimmt, vom mehrdeutigen Typ ist, und sie sind genau dann linear unabhängig, wenn dieses LGS vom eindeutigen Typ ist. Bringt man das LGS auf Stufenform, so erhält man die folgenden Informationen: Diejenigen Vektoren, die nicht zu Stufen gehören, lassen sich als LK der Stufenvariablen schreiben; die Vektoren, die zu Stufen gehören, bilden eine Basis des von den gegebenen Vektoren aufgespannten Raums. Insbesondere ist die Dimension des von den gegebenen Vektoren aufgespannten Raums gleich der Anzahl der Stufen in der Stufenform der Matrix.

Weitere Fragestellungen im Zusammenhang von Unterräumen, Basen, Dimensionen: Seien Basen von zwei Unterräumen U_1, U_2 des \mathbb{K}^n gegeben. Wie bestimmt man die Dimension bzw. eine Basis der Unterräume $U_1 \cap U_2$, $U_1 + U_2$ (dass dies wieder Unterräume sind, dazu siehe Übung)? (Im \mathbb{R}^3 z.B. ergibt sich diese Fragestellung beim Schnitt von (Ursprungs-)Ebenen.)

Beispiel: Seien die Unterräume

$$U_1 = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\}, \quad U_2 = \text{span} \left\{ \begin{pmatrix} 0 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

gegeben. Wie berechnet man eine Basis (und die Dimension) von $U_1 \cap U_2$? Wir bezeichnen die aufspannenden Vektoren von U_1 mit \vec{v}_1, \vec{v}_2 und die von U_2 mit \vec{w}_1, \vec{w}_2 .

Wir suchen $U_1 \cap U_2$, also die Menge der Vektoren \vec{x} , die sich sowohl als $\vec{x} = \alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2$ als auch als $\vec{x} = \alpha_3 \vec{w}_1 + \alpha_4 \vec{w}_2$ schreiben lassen. Wir lösen also das LGS (für die Unbekannten $\alpha_1, \alpha_2, \alpha_3, \alpha_4$)

$$\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 = \alpha_3 \vec{w}_1 + \alpha_4 \vec{w}_2 :$$

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

Wir sehen, dass es nichttriviale Lösungen gibt, da Stufenform vom Typ 2; also ist die Schnittmenge größer als nur $\{\vec{0}\}$. Genauer:

Wir finden die Lösungen: $\alpha_4 = \lambda \in \mathbb{R}$ frei wählbar, $\alpha_3 = \alpha_4 = \lambda$, $\alpha_2 = -\alpha_3 = -\lambda$,

$\alpha_1 = -\alpha_2 + \alpha_4 = 2\lambda$, also $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)^T = \lambda \cdot (2, -1, 1, 1)^T$. Die Elemente der Schnittmenge haben also die Form

$$\vec{x} = \lambda(2\vec{v}_1 - \vec{v}_2) = \lambda \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \quad \text{bzw.} \quad \vec{x} = \lambda(\vec{w}_1 + \vec{w}_2) = \lambda \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

(Beide Darstellungen müssen den gleichen Raum $U_1 \cap U_2$ ergeben, d.h. es reicht eine der beiden Darstellungen, d.h. es reicht, α_3, α_4 zu bestimmen; um die andere Darstellung als 'Probe' verwenden zu können, kann auch die Berechnung von α_1, α_2 nützlich sein.) Es ist also $\dim(U_1 \cap U_2) = 1$ und $\{(1, 0, -1)^T\}$ ist eine Basis.

Wie bestimmt man eine Basis bzw. die Dimension für den Raum $U_1 + U_2$? Nun offensichtlich ist $\{\vec{v}_1, \vec{v}_2, \vec{w}_1, \vec{w}_2\}$ ein EZS von $U_1 + U_2$. Wie man in einem EZS Vektoren ausfindig macht, die sich als LK der übrigen Vektoren schreiben lassen, und so eine Basis bestimmt, haben wir bereits weiter oben gesehen: Wir lösen das homogene LGS $\alpha_1\vec{v}_1 + \alpha_2\vec{v}_2 + \alpha_3\vec{w}_1 + \alpha_4\vec{w}_2 = \vec{0}$; eine Basis bekommen wir, indem wir die zu den Stufen gehörenden Vektoren nehmen, also hier $\vec{v}_1, \vec{v}_2, \vec{w}_1$; die Dimension von $U + V$ ist die Anzahl dieser Stufen, also hier 3.

Wir bemerken: Das LGS zur Bestimmung der Dimension/einer Basis von $U \cap V$ und das LGS zur Bestimmung der Dimension/einer Basis von $U + V$ stimmen bis auf Vorzeichen gewisser Spalten genau überein, insbesondere ihre Stufenzahlen stimmen überein. Wir bekommen:

$$\dim(U + V) = \#\text{Stufen des LGS}$$

$$\dim(U \cap V) = \#\text{Nicht-Stufen des LGS,}$$

also

$$\dim(U + V) + \dim(U \cap V) = \#\text{Spalten} = \dim(U) + \dim(V).$$

Dies führt auf folgende allgemeingültige *Dimensionsformel*:

Satz (Dimensionsformel für Unterräume). Seien U_1, U_2 endlichdimensionale Unterräume eines Vektorraums. Dann gilt:

$$\boxed{\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)}.$$

Beispiel. Im \mathbb{R}^3 kann der Schnitt zweier Ursprungsebenen (2-dimensionaler Räume) eine Ursprungsgerade sein; in diesem Fall erzeugen die aufspannenden Vektoren der beiden Ebenen den ganzen Raum; die Dimensionsformel ergibt hier $2+2=1+3$. Falls beide zu schneidenden Ebenen identisch sind, lautet die Dimensionsformel $2+2=2+2$. Ähnliche Anwendungen ergeben sich beim Schneiden von Ebenen mit Geraden.

Bemerkung. Die Lineare Algebra beschäftigt sich ausschließlich mit *endlichdimensionalen* Vektorräumen (insbesondere also dem \mathbb{R}^n und dem \mathbb{C}^n) sowie 'linearen Abbildungen' (siehe nächstes

Kapitel) zwischen *endlichdimensionalen* Vektorräumen. Mathematik in *unendlichdimensionalen* Vektorräumen (vor allem Funktionenräumen) zu betreiben ist erheblich schwieriger (interessanter); damit beschäftigt sich insbesondere das Gebiet der sog. *Funktionalanalysis*.

3.3 Lineare Abbildungen, Bild und Kern

Def. (Lineare Abbildung) Seien U und V \mathbb{K} -Vektorräume. Eine Abbildung $f : U \rightarrow V$ heißt *linear*, wenn

- (i) $\forall \vec{x}, \vec{y} \in U : f(\vec{x} + \vec{y}) = f(\vec{x}) + f(\vec{y})$
- (ii) $\forall \vec{x} \in U, \alpha \in \mathbb{K} : f(\alpha \vec{x}) = \alpha f(\vec{x})$

Die Menge aller linearen Abbildungen von U nach V wollen wir mit

$$\text{Lin}(U, V)$$

bezeichnen; es ist offensichtlich $\text{Lin}(U, V) \subseteq \text{Abb}(U, V)$.

Man sieht sofort: Für jede lineare Abbildung f gilt: $f(\vec{0}) = f(0 \cdot \vec{x}) \stackrel{\text{(ii)}}{=} 0 \cdot f(\vec{x}) = \vec{0}$ (Dabei ist der linke Nullvektor der in U , der rechte der in V , und $\vec{x} \in U$ beliebig.)

Beispiele.

$f : \mathbb{R}^2 \rightarrow \mathbb{R}^2, f \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} -y \\ x \end{pmatrix}$ ist eine lineare Abbildung. Geometrische Deutung: Drehung aller Punkte (x, y) um den Nullpunkt um 90 Grad.

$f \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 2x + 3y \\ x - y \end{pmatrix}$ ist eine lineare Abbildung von \mathbb{R}^2 nach \mathbb{R}^2 , wie man durch Nachrechnen der beiden Eigenschaften (i) und (ii) leicht zeigen kann.

Dagegen ist $f \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 2x + 3y \\ x - y + 1 \end{pmatrix}$ *keine* lineare Abbildung, da offensichtlich $f(\vec{0}) = (0, 1)^T \neq \vec{0}$ ist!⁴⁷

Obige lineare Abbildung kann man umschreiben zu:

$$f \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + 3y \\ x - y \end{pmatrix} = x \begin{pmatrix} 2 \\ 1 \end{pmatrix} + y \begin{pmatrix} 3 \\ -1 \end{pmatrix}$$

Vergleicht man dies mit den *Bildern der Standardbasis* $\vec{e}_1 = (1, 0)^T, \vec{e}_2 = (0, 1)^T$,

$$f \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \quad f \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix},$$

⁴⁷Analog ist also auch die 'Geradengleichung' $f(x) := 2x + 3, f : \mathbb{R} \rightarrow \mathbb{R}$, keine lineare Abbildung in dem oben definierten Sinn, da $f(0) = 3 \neq 0$. In *Analysis(!)*-Büchern wird manchmal ein von dem der Linearen Algebra abweichender Begriff von Linearität benutzt, nach dem jedes Polynom vom Grad kleiner gleich eins als 'linear' bezeichnet wird.

so ergibt sich

$$f \begin{pmatrix} x \\ y \end{pmatrix} = x f(\vec{e}_1) + y f(\vec{e}_2),$$

d.h. jeder Funktionswert ergibt sich als LK der Funktionswerte der Basiselemente. Dieses Prinzip gilt allgemein für alle lineare Abbildungen $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$. Jedes Element des Urbildraums $\vec{x} = (x_1, \dots, x_n)^T \in \mathbb{K}^n$ wird bezüglich einer Basis $\vec{b}_1, \dots, \vec{b}_n$ ausgedrückt, und die Linearität von f wird ausgenutzt:

$$\vec{x} = \sum_{i=1}^n \alpha_i \vec{b}_i \in \mathbb{K}^n \implies f(\vec{x}) = f \left(\sum_{i=1}^n \alpha_i \vec{b}_i \right) = \sum_{i=1}^n f(\alpha_i \vec{b}_i) = \sum_{i=1}^n \alpha_i f(\vec{b}_i)$$

Das bedeutet, dass, sobald man nur die Wirkungsweise einer linearen Abbildung auf die Vektoren einer Basis kennt, man die gesamte lineare Abbildung 'kennt'. Im Spezialfall, dass die Basis die Standardbasis ist:

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_n \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + x_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \sum_{i=1}^n x_i \vec{e}_i$$

und mit der Linearität von f folgt

$$f(\vec{x}) = f \left(\sum_{i=1}^n x_i \vec{e}_i \right) = \sum_{i=1}^n f(x_i \vec{e}_i) = \sum_{i=1}^n x_i f(\vec{e}_i).$$

Wir haben somit hergeleitet:

Satz (Darstellungssatz für lineare Abbildungen, das Prinzip der linearen Fortsetzung). Sei $\vec{b}_1, \dots, \vec{b}_n$ eine Basis des \mathbb{K}^n und $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ eine lineare Abbildung.

Seien die Bilder der Basiselemente, also $f(\vec{b}_1), \dots, f(\vec{b}_n) \in \mathbb{K}^m$, bekannt. Dann ist die lineare Abbildung f dadurch eindeutig festgelegt, und es gilt für beliebige Vektoren

$$\vec{x} = \sum_{i=1}^n \alpha_i \vec{b}_i \in \mathbb{K}^n:$$

$$f(\vec{x}) = f \left(\sum_{i=1}^n \alpha_i \vec{b}_i \right) = \sum_{i=1}^n \alpha_i f(\vec{b}_i).$$

Ferner kann man sicher sein, dass eine lineare Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ mit beliebig vorgegebenen Werten $f(\vec{b}_1), \dots, f(\vec{b}_n) \in \mathbb{K}^m$ immer existiert.

Man sagt, die lineare Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ entsteht durch *lineare Fortsetzung* der Abbildung $\{\vec{b}_1, \dots, \vec{b}_n\} \rightarrow \{f(\vec{b}_1), \dots, f(\vec{b}_n)\}$.

Es gibt einen engen Bezug von linearen Abbildungen zu Unterräumen:

Def. (Kern und Bild einer linearen Abbildung). Sei $f : U \rightarrow V$ linear. Dann ist

$$\text{Kern}(f) := \{\vec{x} \in U \mid f(\vec{x}) = \vec{0}\} \subseteq U$$

der *Kern* (=Nullraum) von f (also die Menge aller Nullstellen von f), und

$$\text{Bild}(f) := \{f(\vec{x}) \mid \vec{x} \in U\} = f(U) \subseteq V$$

das *Bild* von f .

Offensichtlich sind Kern und Bild niemals leer; sie enthalten immer mindestens den Nullvektor, da $f(\vec{0}) = \vec{0}$. Wir können leicht nachrechnen, dass $\text{Kern}(f)$ und $\text{Bild}(f)$ immer *Vektorräume* sind:

Satz. Sei $f : U \rightarrow V$ eine lineare Abbildung. Dann ist $\text{Kern}(f)$ ein Unterraum von U und $\text{Bild}(f)$ ist ein Unterraum von V .

Beweis. (i) Wir zeigen, dass $\text{Kern}(f)$ die Unterraum-Axiome erfüllt:

Seien $\vec{x}, \vec{y} \in \text{Kern}(U) \Rightarrow f(\vec{x}) = \vec{0}, f(\vec{y}) = \vec{0} \Rightarrow f(\vec{x} + \vec{y}) = f(\vec{x}) + f(\vec{y}) = \vec{0} + \vec{0} = \vec{0}$, also $\vec{x} + \vec{y} \in \text{Kern}(f)$.

Sei $\vec{x} \in \text{Kern}(f)$ und $\alpha \in \mathbb{K}$. Also $f(\vec{x}) = \vec{0}$.

Dann ist $f(\alpha\vec{x}) = \alpha f(\vec{x}) = \alpha \cdot \vec{0} = \vec{0}$, also $\alpha\vec{x} \in \text{Kern}(f)$.

(ii) Wir zeigen, dass $\text{Bild}(f)$ die Unterraum-Axiome erfüllt:

Seien $\vec{y}_1, \vec{y}_2 \in \text{Bild}(f)$. Dann gibt es $\vec{x}_1, \vec{x}_2 \in U$ mit $f(\vec{x}_1) = \vec{y}_1, f(\vec{x}_2) = \vec{y}_2$.

Dann ist $f(\vec{x}_1 + \vec{x}_2) = f(\vec{x}_1) + f(\vec{x}_2) = \vec{y}_1 + \vec{y}_2$, also $\vec{y}_1 + \vec{y}_2 \in \text{Bild}(f)$.

Sei $\vec{y} \in \text{Bild}(f)$ und $\alpha \in \mathbb{K}$. Dann gibt es $\vec{x} \in U$ mit $f(\vec{x}) = \vec{y}$. Dann ist $f(\alpha\vec{x}) = \alpha f(\vec{x}) = \alpha\vec{y}$, d.h. $\alpha\vec{y} \in \text{Bild}(f)$.

Frage: Wie berechnet man in der Praxis Kern und Bild einer linearen Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$?

Wir gehen dazu davon aus, dass f bezüglich der Standard-Basis von \mathbb{R}^n gegeben ist, dass also $f(\vec{e}_1), \dots, f(\vec{e}_n) \in \mathbb{K}^m$ gegeben sind, wobei $\vec{e}_1, \dots, \vec{e}_n$ die Standard-Basis des \mathbb{K}^n sei.⁴⁸

Zur Berechnung der Kerns von f :

Wir suchen also alle $\vec{x} \in \mathbb{K}^n$, für die $f(\vec{x}) = \vec{0}$ ist. Wir stellen die gesuchten \vec{x} dar bezüglich der gegebenen (Standard-)Basis des \mathbb{K}^n : $\vec{x} = \sum_{i=1}^n x_i \vec{e}_i$, und suchen also alle $\vec{x} \in \mathbb{K}^n$ mit

$$f\left(\sum_{i=1}^n x_i \vec{e}_i\right) = \vec{0},$$

⁴⁸Man kann die nun folgende Überlegung auch übertragen auf den Fall, dass f bezüglich einer *beliebigen* Basis gegeben ist; die Berechnung der Dimension des Kerns ändert sich nicht, jedoch die Berechnung des Kerns selbst ein wenig.

also, mit der Linearität von f ,

$$\sum_{i=1}^n x_i f(\vec{e}_i) = \vec{0}$$

Dies ist nichts anderes als ein homogenes LGS, und zwar sind die Spalten der Systemmatrix gerade die gegebenen Bildvektoren $f(\vec{e}_1), \dots, f(\vec{e}_n)$. Wie wir die Lösungsmenge (den Lösungsraum) mit dem Gauß-Verfahren berechnen, wissen wir. Die Dimension des Lösungsraums ist gerade die Anzahl der frei zu wählenden Variablen, also die Anzahl der Spalten der Stufenform, in denen keine neue Stufe beginnt.

Beispiel zur Berechnung einer Basis (und der Dimension) des Kerns.

Sei $f : \mathbb{R}^6 \rightarrow \mathbb{R}^4$ lineare Abbildung, gegeben durch

$$f(\vec{e}_1) = \vec{0}, \quad f(\vec{e}_2) = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \quad f(\vec{e}_3) = \begin{pmatrix} -1 \\ -2 \\ 0 \\ 0 \end{pmatrix}, \quad f(\vec{e}_4) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \quad f(\vec{e}_5) = \begin{pmatrix} 0 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \quad f(\vec{e}_6) = \begin{pmatrix} 1 \\ -4 \\ 0 \\ 2 \end{pmatrix}$$

Wir lösen das zugehörige homogene LGS mit Gauß:

$$\begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 2 & -2 & 0 & 3 & -4 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 3 & -6 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Es ist also $x_1 = \lambda_1$, $x_3 = \lambda_2$, $x_6 = \lambda_3 \in \mathbb{R}$ frei wählbar, und $x_5 = 2x_6 = 2\lambda_3$, $x_4 = -x_5 = -2\lambda_3$, $x_2 = x_3 - x_6 = \lambda_2 - \lambda_3$, also

$$\begin{aligned} \text{Kern}(f) &= \left\{ \begin{pmatrix} \lambda_1 \\ \lambda_2 - \lambda_3 \\ \lambda_2 \\ -2\lambda_3 \\ 2\lambda_3 \\ \lambda_3 \end{pmatrix} \mid \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R} \right\} \\ &= \left\{ \lambda_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 \\ -1 \\ 0 \\ -2 \\ 2 \\ 1 \end{pmatrix} \mid \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R} \right\} \\ &= \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ -2 \\ 2 \\ 1 \end{pmatrix} \right\} \end{aligned}$$

die Dimension des Kerns ist 3 (das Gauß-Verfahren liefert immer eine Darstellung der Lösungsmenge mit *minimaler* Parameterzahl, d.h. die gelieferten aufspannenden Vektoren der Lösungsmenge sind immer eine Basis des Lösungsraums).

Nun noch zur Frage, wie man eine Basis des Bildes von f bekommt:

Offensichtlich bilden nach dem Darstellungssatz die gegebenen Vektoren $f(\vec{e}_i)$ ein EZS von $\text{Bild}(f)$. Wie man aus einem EZS eine Basis extrahiert, wurde auf S. 64 vorgestellt: Man betrachtet das *selbe* LGS, das wir eben zur Bestimmung des Kerns betrachtet hatten, und bringen es auf Stufenform (was wir bereits erledigt haben); dann nimmt man zu jeder *Stufe* den zugehörigen Basisvektor des ursprünglichen Systems, d.h. in obigem Beispiel erhalten wir Stufen in den Spalten Nr. 2, 4, 5, d.h. $\{f(\vec{e}_2), f(\vec{e}_4), f(\vec{e}_5)\}$ bilden eine Basis von $\text{Bild}(f)$.

Man kann also mit einem *einmaligen* Durchführen des Gauß-Verfahrens sowohl eine Basis des Kerns als auch eine Basis des Bildes einer linearen Abbildung bestimmen. Das Gauß-Verfahren wird auf die Spalten der Matrix angewendet, die aus den Bildern der Basisvektoren besteht.

Die obige Berechnung zeigt: Die Dimension des Bildes einer linearen Abbildung ist die Anzahl der Stufen des auf Stufenform gebrachten homogenen LGS, dessen Spalten die Bildvektoren der Basisvektoren sind. Die Dimension des Kerns einer linearen Abbildung ist gleich der Anzahl der Spalten, die keine Stufe enthalten. Die Summe beider Dimensionen ergibt also die Gesamtspaltenzahl. Wir erhalten die Dimensionsformel für Kern und Bild einer linearen Abbildung:

Satz (Dimensionsformel für Bild und Kern einer linearen Abbildung). Sei $f \in \text{Lin}(\mathbb{K}^n, \mathbb{K}^m)$. Dann ist

$$\boxed{\dim(\text{Kern}(f)) + \dim(\text{Bild}(f)) = n}.$$

Einschub. Wir geben nun noch eine Variante des Gauß-Verfahrens an, die sogenannte Gauß-Jordan-Elimination, die man zum Lösen linearer Gleichungssysteme benutzen kann, also auch insbesondere zur Bestimmung einer Basis von Bild und Kern. Der Vorteil dieses Verfahrens gegenüber dem klassischen Gauß-Verfahren ist, dass man das Rückwärtseinsetzen nicht explizit durchführen muss:

Gauß-Jordan-Verfahren zum Lösen des LGS $(A|\vec{b})$:

1. Bringe das LGS wie gewohnt mit dem uns bekannten Gauß-Verfahren auf Stufenform.
2. Dividiere alle Zeilen durch das Stufenelement. (Auf den Stufen stehen danach lauter Einsen.)
3. Durch elementare Zeilenoperationen erzeuge Nullen auch *oberhalb* aller Stufen.
4. Durch Einfügen oder Streichen von Nullzeilen Sorge dafür, dass alle Stufenelemente auf der Diagonalen der Systemmatrix liegen und insbesondere die Zeilenzahl gleich der Spaltenzahl wird.
(Bisher haben wir lediglich Äquivalenzumformungen durchgeführt.)
5. Wir lesen nun die Lösungsmenge direkt ab, ohne dass wir das Rückwärtseinsetzen explizit durchführen müssen:
Im homogenen Fall erhält man eine Basis des Lösungsraumes, indem man alle Spalten des

transformierten LGS, die zu keiner Stufe gehören, nimmt, wobei man jedoch die Diagonalelemente (die null sind) durch -1 ersetzt.

Im inhomogenen Fall addiert man zu diesem Raum den Vektor, der auf der rechten Seite des transformierten LGS steht.

Die Schritte 1.-4. sind offensichtlich Äquivalenzumformungen, ändern also die Lösungsmenge nicht. Begründen werden müsste lediglich Schritt 5. Dazu müsste man eine in den Schritten 1.-3. erzeugte Stufenform in allgemeiner Form (Einträge a_{ij} oberhalb der Diagonale in den Nicht-Stufen-Spalten, ...) betrachten und das uns bekannte Rückwärtseinsetzen durchführen; das liefert die in Schritt 5 behauptete Lösung. Wir wollen hier darauf verzichten und uns nur das Gauß-Jordan-Verfahren für das Beispiel von S. 70 für das dortige homogene LGS anschauen:

Schritt 1 lieferte (s. S. 70):

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

Schritt 2 erfordert lediglich ein Durchmultiplizieren der 3. Zeile mit -1 .

Schritt 3 erzeugt in der 5. Spalte eine Null oberhalb des Stufenelements:

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

Schritt 4 liefert dann

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

Nun nimmt man in Schritt 5 alle Nicht-Stufen-Spalten, das sind hier die Spalten 1, 3, 6; diese liefern eine Basis des Lösungsraums des homogenen LGS (also eine Basis des Kerns), wenn man die Diagonal-Nullen durch -1 ersetzt, also

$$L_{hom} = \text{Kern}(f) = \text{span} \left\{ \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 2 \\ -2 \\ -1 \end{pmatrix} \right\} = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ -2 \\ 2 \\ 1 \end{pmatrix} \right\},$$

also in der Tat das gleiche Ergebnis wie auf S. 70.

Wir wollen nun auf die Begriffe Injektivität, Surjektivität, Bijektivität, die wir in Kap. 1.4 allgemein für Abbildungen definiert hatten, zurückkommen im Zusammenhang mit *linearen* Abbildungen. Es stellt sich heraus, dass es für lineare Abbildungen einfache Kriterien für Injektivität, Surjektivität, Bijektivität gibt:

Satz. (Charakterisierung der Injektivität/Surjektivität/Bijektivität von linearen Abbildungen)

Seien U, V endlichdimensionale \mathbb{K} -Vektorräume und $f : U \rightarrow V$ linear. Sei $\mathcal{B} = \{\vec{b}_1, \dots, \vec{b}_n\}$ eine Basis von U . Dann gilt:

- (i) f injektiv $\iff \text{Kern}(f) = \{\vec{0}\} \iff \{f(\vec{b}_1), \dots, f(\vec{b}_n)\}$ sind linear unabhängig
- (ii) f surjektiv $\iff \text{Bild}(f) = V \iff \{f(\vec{b}_1), \dots, f(\vec{b}_n)\}$ bilden ein EZS von V
- (iii) f ist bijektiv $\iff \text{Bild}(f) = V \wedge \text{Kern}(f) = \{\vec{0}\} \iff \{f(\vec{b}_1), \dots, f(\vec{b}_n)\}$ ist eine Basis von V

Beweis. Es reicht (i) und (ii) zu zeigen, denn (iii) ist eine triviale Folgerung aus (i) und (ii).

zu (i):

Statt $A \iff B \iff C$ gehen wir wie folgt vor: $A \Rightarrow B, B \Rightarrow C, C \Rightarrow A$:

- Sei f injektiv. (zeige: $\text{Kern}(f) = \{\vec{0}\}$)
 Sei $\vec{x} \in \text{Kern}(f)$ (also z.z.: $\vec{x} = \vec{0}$),
 also $f(\vec{x}) = \vec{0}$. Da auch $f(\vec{0}) = \vec{0}$, ist offensichtlich $f(\vec{x}) = f(\vec{0})$, und wegen der Injektivität von f folgt $\vec{x} = \vec{0}$.
 Also: $\text{Kern}(f) = \{\vec{0}\}$.
- Sei $\text{Kern}(f) = \{\vec{0}\}$. Um die lineare Unabhängigkeit der Vektoren $f(\vec{b}_i)$ zu zeigen, sei $\sum_{i=1}^n \alpha_i f(\vec{b}_i) = \vec{0}$ eine LK, die den Nullvektor ergibt. (z.z.: $\alpha_1 = \dots = \alpha_n = 0$)
 Mit der Linearität von f folgt $f(\sum_{i=1}^n \alpha_i \vec{b}_i) = \vec{0}$. Also ist $\sum_{i=1}^n \alpha_i \vec{b}_i \in \text{Kern}(f)$. Nach Voraussetzung ist dann $\sum_{i=1}^n \alpha_i \vec{b}_i = \vec{0}$. Da die \vec{b}_i eine Basis von U sind, folgt, dass alle $\alpha_i = 0$ sind.
- Seien die $f(\vec{b}_i)$ linear unabhängig. Wir zeigen die Injektivität von f . Seien dazu $\vec{x}, \vec{y} \in U$ mit $f(\vec{x}) = f(\vec{y})$. (z.z.: $\vec{x} = \vec{y}$)
 Wir stellen \vec{x} und \vec{y} bezüglich der Basis $\vec{b}_1, \dots, \vec{b}_n$ dar:

$$\vec{x} = \sum_{i=1}^n \alpha_i \vec{b}_i, \vec{y} = \sum_{i=1}^n \beta_i \vec{b}_i.$$
 Mit der Linearität von f folgt $\sum_{i=1}^n \alpha_i f(\vec{b}_i) = \sum_{i=1}^n \beta_i f(\vec{b}_i)$, also $\sum_{i=1}^n (\alpha_i - \beta_i) f(\vec{b}_i) = \vec{0}$.
 Da die $f(\vec{b}_i)$ linear unabhängig sind, folgt $\alpha_i - \beta_i = 0$ für alle i und somit $\vec{x} = \vec{y}$.

zu (ii):

Die Aussage " f surjektiv $\iff \text{Bild}(f) = V$ " ist nichts anderes als die Definition der Surjektivität (und gilt in auch für nichtlineare Abbildungen). Es bleibt die Äquivalenz zur EZS-Eigenschaft der $f(\vec{b}_i)$ zu zeigen:

Sei f surjektiv. Sei $\vec{y} \in V$ beliebig. Aus der Surjektivität folgt, dass es ein $\vec{x} \in U$ gibt mit $f(\vec{x}) = \vec{y}$. Wir stellen \vec{x} bezüglich der Basis $\vec{b}_1, \dots, \vec{b}_n$ dar: $\vec{x} = \sum_{i=1}^n \alpha_i \vec{b}_i$. Auf

diese Gleichung wenden wir f an und nutzen die Linearität von f aus; es folgt:

$$\sum_{i=1}^n \alpha_i f(\vec{b}_i) = \vec{y}.$$

Wir haben also jeden beliebigen Vektor $\vec{y} \in V$ als LK der $f(\vec{b}_i)$ darstellen können, d.h. die $f(\vec{b}_i)$ bilden ein EZS von V .

Seien nun umgekehrt die $f(\vec{b}_i)$ ein EZS von V . Wir zeigen die Surjektivität. Sei dazu $\vec{y} \in V$ beliebig. Da die $f(\vec{b}_i)$ ein EZS von V bilden, gibt es eine Darstellung $\vec{y} = \sum_{i=1}^n \alpha_i f(\vec{b}_i)$. Mit der Linearität von f folgt $\vec{y} = f(\sum_{i=1}^n \alpha_i \vec{b}_i)$. Also ist $\vec{y} \in \text{Bild}(f)$ und somit f surjektiv. \square

Bemerkung. Das obige Kriterium der Surjektivität, "Bild(f) = V " kann äquivalent(!) umgeschrieben werden zu: "dim(Bild(f)) = dim(V)". Hintergrund ist folgender Sachverhalt (hier ohne Beweis): Gilt für zwei endlichdimensionale Vektorräume, dass $U \subseteq V$ und dim(U) = dim(V), so ist $U = V$.

Def. (Isomorphismus) Seien U, V \mathbb{K} -Vektorräume. Eine bijektive lineare Abbildung $f : U \rightarrow V$ heißt *Isomorphismus von Vektorräumen*. Gibt es einen solchen Isomorphismus, so heißen U und V *isomorph*.

Eine lineare Abbildung ist also (siehe obiger Satz) genau dann ein Isomorphismus, wenn sie Basen auf Basen abbildet, was insbesondere bedeutet, dass die beiden beteiligten Vektorräume *die gleiche Dimension* haben müssen. Umgekehrt, wenn zwei (endlichdimensionale) Vektorräume die gleiche Dimension haben, kann man immer leicht einen Isomorphismus konstruieren, indem man eine Basis des einen Raumes auf eine Basis des anderen Raumes abbilden lässt und den Rest der linearen Fortsetzung überlässt. Es folgt:

Satz. Zwei endlichdimensionale \mathbb{K} -Vektorräume U, V sind genau dann isomorph, wenn sie die gleiche Dimension haben. Insbesondere sind also alle n -dimensionalen \mathbb{K} -Vektorräume isomorph zum \mathbb{K}^n .

Isomorphie von Vektorräumen bedeutet, dass diese 'im wesentlichen', d.h. bis auf Umbenennung der Elemente, gleich sind. Alle Vektorräume der Dimension n (n fest) sind isomorph, d.h. haben die gleiche Struktur, d.h. sind bis auf Umbenennung der Elemente identisch.

Am Ende dieses Kapitels wollen wir uns noch mit *Verknüpfungen* und *Verkettungen* von linearen Abbildungen beschäftigen. So, wie allgemein Abbildungen $f, g : M \rightarrow \mathbb{K}$ oder $f, g : M \rightarrow V$ von einer Menge $M \neq \emptyset$ in einen Körper \mathbb{K} oder auch einen \mathbb{K} -Vektorraum V *addiert* werden können oder auch mit Skalaren multipliziert werden können, so kann man dies natürlich insbesondere mit *linearen* Abbildungen $f, g \in \text{Lin}(U, V)$ machen

per

$$(f+g)(\vec{x}) := f(\vec{x}) + g(\vec{x}), \quad (\alpha f)(\vec{x}) := \alpha f(\vec{x})$$

Es sind dann auch $f+g, \alpha f \in \text{Lin}(U, V)$, also

$$+ : \text{Lin}(U, V) \times \text{Lin}(U, V) \longrightarrow \text{Lin}(U, V), \quad \cdot : \mathbb{K} \times \text{Lin}(U, V) \longrightarrow \text{Lin}(U, V)$$

Man kann leicht nachrechnen, dass $\text{Lin}(U, V)$ mit diesen beiden Verknüpfungen ein \mathbb{K} -Vektorraum ist (z.B. indem man zeigt, dass $\text{Lin}(U, V)$ ein Unterraum von $\text{Abb}(U, V)$ ist):

Satz. Seien U, V \mathbb{K} -Vektorräume. Dann ist die Menge aller linearen Abbildungen $(\text{Lin}(U, V), +, \cdot)$ mit den oben genannten Verknüpfungen '+' und '·' wieder ein \mathbb{K} -Vektorraum.

Neben dieser Addition und Skalarmultiplikation von linearen Abbildungen, die zwischen den *selben* Räumen operieren, kann man auch lineare Abbildungen hintereinanderschalten, wenn der Bildraum der einen gleich dem Definitionsbereich der anderen ist:

Sind U, V, W \mathbb{K} -Vektorräume und die Abbildungen $g : U \rightarrow V$ und $f : V \rightarrow W$ linear, so ist auch die Verkettung $f \circ g : U \rightarrow W$ linear. (Der Nachweis dieser Tatsache ist elementar.)

3.4 Matrizen

Motivation. Wir kennen bisher den Begriff 'Matrix' im Zusammenhang mit linearen Gleichungssystemen als 'Systemmatrix'. Auch im Zusammenhang mit linearen Abbildungen (Bestimmung von Kern/Bild einer linearen Abbildung) haben wir gewisse Matrizen aufgestellt und auf diese den Gauß-Algorithmus angewendet. Wir wollen in diesem Kapitel genauer definieren, was wir unter einer Matrix verstehen, und wie wir Matrizen miteinander verknüpfen können (wir werden für Matrizen (1.) Addition, (2.) Skalarmultiplikation, (3.) Matrix-Matrix-Multiplikation, (4.) Matrix-Vektor-Multiplikation erklären). Es wird sich herausstellen, dass Matrizen nicht nur im Zusammenhang mit linearen Gleichungssystemen auftreten, sondern dass man mittels Matrizen *lineare Abbildungen* elegant beschreiben kann. Zu jeder Matrix gibt es eine zugehörige lineare Abbildung, und zu jeder linearen Abbildung gibt es eine zugehörige Matrix. **Man kann Matrizen somit einfach als eine neue Schreibweise für lineare Abbildungen begreifen; Matrizen 'sind' nichts anderes als lineare Abbildungen, wird sich herausstellen.** Diese neue Schreibweise macht das Handtieren mit linearen Abbildungen (z.B.: Wie sieht die Hintereinanderschaltung zweier linearer Abbildungen aus? Wie berechnet man die Umkehrfunktion einer linearen Abbildung?) einfacher. Wir wollen zunächst die Menge der Matrizen sowie die Addition

und skalarmultiplikation von Matrizen definieren, und uns dann anschließend überlegen, was Matrizen mit linearen Abbildungen zu tun haben.

Wie schon in den vorangegangenen Kapiteln sei weiterhin $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$.

Def. (Matrix). Seien $m, n \in \mathbb{N}$. Unter einer $m \times n$ -Matrix über dem Körper \mathbb{K} verstehen wir ein 'Schema' von Zahlen

$$A = (a_{ij})_{\substack{i=1..m \\ j=1..n}} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & & \dots & a_{mn} \end{pmatrix}$$

wobei⁴⁹ die $a_{ij} \in \mathbb{K}$, $i = 1, \dots, m$, $j = 1, \dots, n$. Die Menge aller $m \times n$ -Matrizen über \mathbb{K} wird mit $\mathbb{K}^{m \times n}$ bezeichnet.

Letztendlich ist also $\mathbb{K}^{m \times n}$ nichts anderes als die Menge der $m \cdot n$ -Tupel $\mathbb{K}^{m \cdot n}$, nur dass die Komponenten der Tupel in einem rechteckigen Schema angeordnet worden sind statt alle übereinander zu stehen.

Damit können wir natürlich auch die uns für den Vektorraum der Tupel $\mathbb{K}^{m \cdot n}$ bekannte Vektoraddition und Skalarmultiplikation in $\mathbb{K}^{m \times n}$ durchführen, d.h. wir definieren: Wenn A wie oben und

$$B = (b_{ij})_{\substack{i=1..m \\ j=1..n}} = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix},$$

also wenn $A, B \in \mathbb{K}^{m \times n}$ Matrizen vom gleichen Format sind, und $\alpha \in \mathbb{K}$, dann sei

$$A + B := (a_{ij} + b_{ij})_{\substack{i=1..m \\ j=1..n}} = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \vdots & & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

und

$$\alpha A := (\alpha a_{ij})_{\substack{i=1..m \\ j=1..n}} = \begin{pmatrix} \alpha b_{11} & \dots & \alpha b_{1n} \\ \vdots & & \vdots \\ \alpha b_{m1} & \dots & \alpha b_{mn} \end{pmatrix},$$

d.h. wir haben die Addition und die Skalarmultiplikation, wie auch schon in den Tupelräumen \mathbb{K}^n , *komponentenweise* definiert.

Es folgen sofort (wie schon in \mathbb{K}^n) die Kommutativ- und Distributivgesetze

$$A + B = B + A, \quad \alpha(A + B) = \alpha A + \alpha B, \quad (\alpha + \beta)A = \alpha A + \beta A,$$

⁴⁹Die Schreibweise a_{ij} ist im Sinne von $a_{i,j}$ (und nicht im Sinne von $a_{i \cdot j}$) zu verstehen. Um Missverständnisse zu vermeiden, kann man auch direkt $a_{i,j}$ schreiben.

und das neutrale Element in $(\mathbb{K}^{m \times n}, +)$ ist die Null-Matrix

$$0_{m \times n} := \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in \mathbb{K}^{m \times n}.$$

Ferner gilt $\alpha(\beta A) = (\alpha\beta)A$ und $1 \cdot A = A$; somit ist die Menge aller $m \times n$ -Matrizen mit Einträgen in \mathbb{K} , also $\mathbb{K}^{m \times n}$, ist mit obiger Addition und Skalarmultiplikation also ein \mathbb{K} -Vektorraum! (Kürzer argumentiert: Da die Verknüpfungen auf $\mathbb{K}^{m \times n}$ genau so wie im Vektorraum $\mathbb{K}^{m \cdot n}$ definiert sind, ist klar, dass $\mathbb{K}^{m \times n}$ ein Vektorraum ist.)

Zur Übung: Finden Sie eine Basis von $\mathbb{K}^{m \times n}$. $\dim(\mathbb{K}^{m \times n}) = ?$.

(Ein erster) Zusammenhang von Matrizen und linearen Abbildungen.

Wo ist nun der Zusammenhang zu linearen Abbildungen?

Wie wir aus Kapitel 3.3 wissen, können wir lineare Abbildungen angeben, indem wir ihre Wirkungsweise auf eine Basis des Urbildraumes angeben (Prinzip der linearen Fortsetzung). Ist $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ linear, so können wir z.B. durch Angabe von

$$f(\vec{e}_1) = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} = \sum_{i=1}^m a_{i1} \vec{e}_i, \quad \dots, \quad f(\vec{e}_n) = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \sum_{i=1}^m a_{in} \vec{e}_i,$$

f komplett beschreiben. Das heißt, es reicht die Zahlen a_{ij} , $i = 1, \dots, m$, $j = 1, \dots, n$, anzugeben, um die lineare Abbildung f zu beschreiben. Diese a_{ij} können wir in Form einer $m \times n$ -Matrix angeben!

Haben wir also z.B. eine lineare Abbildung $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ mit $f(\vec{e}_1) = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$, $f(\vec{e}_2) = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$, $f(\vec{e}_3) = \begin{pmatrix} 0 \\ 5 \end{pmatrix}$, so können wir diese Angaben kurz zusammenfassen durch Angabe einer 2×3 -Matrix

$$A = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 1 & 5 \end{pmatrix}$$

Wir sagen: A ist die zu f gehörende Matrix.⁵⁰

Umgekehrt können wir jede $m \times n$ -Matrix sofort als lineare Abbildung von \mathbb{K}^n nach \mathbb{K}^m interpretieren; wir sprechen von der zu A gehörenden linearen Abbildung.

Die Addition in der Menge der linearen Abbildungen und die Addition in der Menge der Matrizen sind so definiert, dass gilt: Ist A die zu f gehörende Matrix und B die zu g gehörende Matrix, dann ist $A+B$ die zu $f+g$ gehörende Matrix. Und analog für

⁵⁰So völlig neu ist die Idee, eine lineare Abbildung in Form einer Matrix hinzuschreiben, für uns nicht: Zur Bestimmung einer Basis von Kern und Bild einer linearen Abbildung haben wir in Kap. 3.3 bereits die zu der linearen Abbildung gehörende Matrix hingeschrieben und das Gauß-Verfahren auf sie angewendet.

die Skalarmultiplikation ist αA die zu αf gehörende Matrix. Wir können also lineare Abbildungen addieren oder skalarmultiplizieren, indem wir ihre zugehörigen Matrizen addieren bzw. skalarmultiplizieren!

Wir können also die Menge der $m \times n$ -Matrizen $\mathbb{K}^{m \times n}$ mit der Menge der linearen Abbildungen $\text{Lin}(\mathbb{K}^n, \mathbb{K}^m)$ 'identifizieren'. Genauer, mathematisch gesprochen sind die beiden Vektorräume $\text{Lin}(\mathbb{K}^n, \mathbb{K}^m)$ und $\mathbb{K}^{m \times n}$ *isomorph*: Indem wir zu jeder linearen Abbildung eine Matrix (oder zu jeder Matrix eine lineare Abbildung) angeben, haben wir eine *Bijektion* zwischen den beiden Vektorräumen $\text{Lin}(\mathbb{K}^n, \mathbb{K}^m)$ und $\mathbb{K}^{m \times n}$ angegeben, also einen Isomorphismus.

Aus der Isomorphie folgt insbesondere (siehe Kap. 3.3), dass beide Räume die gleiche Dimension haben. Da $\mathbb{K}^{m \times n}$ nichts anderes als \mathbb{K}^{mn} ist, ist offensichtlich also

$$\dim(\text{Lin}(\mathbb{K}^n, \mathbb{K}^m)) = \dim(\mathbb{K}^{m \times n}) = \dim(\mathbb{K}^{m \cdot n}) = n \cdot m$$

(Zur Übung: Geben Sie eine Basis des Vektorraums $\text{Lin}(\mathbb{K}^n, \mathbb{K}^m)$ an!).

Bemerkung. Als wir oben die Einträge der zu einer linearen Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ gehörenden Matrix definiert haben, haben wir im Urbildraum \mathbb{K}^n die Darstellung bezüglich der *Standardbasis* $\vec{e}_1, \dots, \vec{e}_n$ gewählt, und auch bei der Darstellung der Vektoren $f(\vec{e}_j)$ haben wir die *Standardbasis* im Zielraum \mathbb{K}^m gewählt, d.h. die a_{ij} sind die Koeffizienten von $f(\vec{e}_j)$ bezüglich der Standardbasis: $f(\vec{e}_j) = \sum_{i=1}^m a_{ij} \vec{e}_i$. Man kann anstelle der Standardbasen sowohl im Urbild- als auch im Bildraum andere Basen wählen und mittels dieser die zu f gehörende Matrix definieren. Solange keine Angabe über die Wahl der Basen gemacht wurde, ist immer davon auszugehen, dass die Standardbasen gewählt wurden.

Die Matrix-Matrix-Multiplikation. Motivation mit Hilfe der Verkettung von linearen Abbildungen.

Hat auch die *Verkettung* von linearen Abbildungen⁵¹ $g : \mathbb{K}^m \rightarrow \mathbb{K}^n$, $f : \mathbb{K}^n \rightarrow \mathbb{K}^r$ eine Entsprechung in der Welt der Matrizen? Dazu schauen wir und nochmal genau an, wie wir die Verkettung von linearen Abbildungen berechnen, und übertragen diese Verknüpfung dann auf Matrizen:

Seien f und g gegeben durch die Matrizen $A = (a_{ij}) \in \mathbb{K}^{r \times n}$ und $B = (b_{ij}) \in \mathbb{K}^{n \times m}$, also

$$f(\vec{e}_j) = (a_{1j}, \dots, a_{rj})^T = \sum_{i=1}^r a_{ij} \vec{e}_i, \quad j = 1, \dots, n,$$

und

$$g(\vec{e}_k) = (b_{1k}, \dots, b_{nk})^T = \sum_{j=1}^n b_{jk} \vec{e}_j, \quad k = 1, \dots, m.$$

⁵¹...wie wir sie in Aufgabe A34 auf Blatt 9 durchgeführt haben...

Es ist dann

$$\begin{aligned} f \circ g(\vec{e}_k) &= f(g(\vec{e}_k)) = f\left(\sum_{j=1}^n b_{jk} \vec{e}_j\right) = \sum_{j=1}^n b_{jk} f(\vec{e}_j) = \sum_{j=1}^n b_{jk} \left(\sum_{i=1}^r a_{ij} \vec{e}_i\right) \\ &= \sum_{i=1}^r \left(\sum_{j=1}^n a_{ij} b_{jk}\right) \vec{e}_i \end{aligned}$$

Die Matrix C , die zur Abbildung $f \circ g$ gehört (sie muss, da $f \circ g : \mathbb{K}^m \rightarrow \mathbb{K}^r$, eine $r \times m$ -Matrix sein), hat also die Einträge

$$c_{ik} = \sum_{j=1}^n a_{ij} b_{jk}.$$

Dies motiviert die folgende Definition:

Das Produkt $C = (c_{ij}) = AB$ zweier Matrizen $A = (a_{ij}) \in \mathbb{K}^{r \times n}$ und $B = (b_{ij}) \in \mathbb{K}^{n \times m}$ ist eine $r \times m$ -Matrix $C = (c_{ik}) = AB \in \mathbb{K}^{r \times m}$ mit den Einträgen

$$\boxed{c_{ik} = \sum_{j=1}^n a_{ij} b_{jk}} \quad \forall i = 1, \dots, r, \forall j = 1, \dots, m.$$

Der Eintrag in der i -ten Zeile und k -ten Spalte von $C = A \cdot B$ berechnet sich also unter Verwendung der i -ten Zeile von A und der k -ten Spalte von B . Die Multiplikation von Matrizen erfordert also, dass die Spaltenzahl des ersten Faktors gleich der Zeilenzahl des zweiten Faktors ist, kurz

$$\cdot : \mathbb{K}^{r \times n} \times \mathbb{K}^{n \times m} \longrightarrow \mathbb{K}^{r \times m}.$$

Die Multiplikation von Matrizen wird auch als *Matrix-Matrix-Multiplikation* bezeichnet.

Beispiel Matrix-Matrix-Multiplikation:

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 1 & 0 & 0 \\ 2 & 6 & 0 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix} \implies AB = \begin{pmatrix} 9 & 13 & 0 & 2 \\ 5 & 7 & 3 & 3 \end{pmatrix}$$

denn $1 \cdot 5 + 2 \cdot 2 + 0 \cdot 0 = 9$, $1 \cdot 1 + 2 \cdot 6 + 0 \cdot 2 = 13$, usw.

Und noch einmal zur Motivation: Anders als die Matrix-Addition haben wir die Matrix-Multiplikation nicht einfach komponentenweise, sondern etwas komplizierter definiert. Der Grund dafür ist, wie wir oben bereits dargelegt haben: Wir haben die Multiplikation von Matrizen so und nicht anders definiert, damit sie die Verkettung von linearen Abbildungen widerspiegelt. Durch obige Definition der Matrix-Matrix-Multiplikation haben wir erreicht: Ist A die zu f gehörende Matrix und B die zu g gehörende Matrix, so ist AB die zu $f \circ g$ gehörende Matrix. Dank der Matrix-Schreibweise linearer

Abbildungen können wir also die Verkettung linearer Abbildungen schnell durchführen.

Da wir wissen, dass die Verkettung von Abbildungen (egal ob lineare oder beliebige Abbildungen) assoziativ und distributiv, jedoch i.a. nicht kommutativ ist, folgt, dass auch die Matrix-Matrix-Multiplikation assoziativ und distributiv ist,⁵²

$$(AB)C = A(BC) =: ABC, \quad A(B+C) = AB + AC, \quad (A+B)C = AC + BC,$$

jedoch i.a. nicht kommutativ,

$$AB \neq BA,$$

(Gegenbeispiele sind leicht zu finden, siehe Übung). Ferner gilt für Skalare $\alpha, \beta \in \mathbb{K}$:

$$\alpha(AB) = (\alpha A)B = A(\alpha B), \quad \alpha(A+B) = \alpha A + \alpha B, \quad (\alpha + \beta)A = \alpha A + \beta A$$

Spezialfall: Multiplikation *quadratischer* Matrizen. Einheitsmatrix. Inverse Matrix.

Wir betrachten nun die Matrix-Matrix-Multiplikation im Spezialfall $m = n = r$. In diesem Fall haben wir eine Verknüpfung, die den Raum der quadratischen Matrizen $\mathbb{K}^{n \times n}$ nicht verlässt:

$$\cdot : \mathbb{K}^{n \times n} \times \mathbb{K}^{n \times n} \longrightarrow \mathbb{K}^{n \times n}$$

Naheliegender ist die Frage, ob es sich bei $(\mathbb{K}^{n \times n}, \cdot)$ oder zumindest bei $(\mathbb{K}^{n \times n} \setminus \{0_{n \times n}\}, \cdot)$ um eine Gruppe handelt. Bei Abbildungen ist das neutrale Element bezüglich der Verkettung die identische Abbildung, die jedes \vec{e}_j auf \vec{e}_j abbildet. Die zur identischen Abbildung gehörende Matrix ist offensichtlich

$$E_n := \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix},$$

die sogenannte $n \times n$ -*Einheitsmatrix*. In der Tat sieht man sofort, dass E_n das neutrale Element der Matrix-Matrix-Multiplikation ist.

Auch das Assoziativgesetz gilt (s.o.). Die Antwort auf obige Frage, ob $(\mathbb{K}^{n \times n}, \cdot)$ eine Gruppe ist, lautet trotzdem für $n > 1$ *nein*, denn **nicht jede $\mathbb{K}^{n \times n}$ -Matrix besitzt ein Inverses**. Als Gegenbeispiel kann man sofort die Nullmatrix anführen, die offensichtlich kein Inverses hat, oder man verweist darauf, dass in $\text{Lin}(\mathbb{K}^n, \mathbb{K}^m)$ nicht alle Elemente ein Inverses bezüglich der Verkettung, d.h. eine Umkehrfunktion, haben (sondern nur die bijektiven).

⁵²Hier wird immer vorausgesetzt, dass die Dimensionen der zu verknüpfenden Matrizen 'zueinander passen'.

Die Struktur $(\mathbb{K}^{n \times n}, +, \cdot)$ ist also kein Körper, sondern lediglich ein Ring (mit Einselement, jedoch nicht kommutativ).⁵³

Man nennt Matrizen, die ein Inverses besitzen, *invertierbar* oder *regulär*.

Eine wichtige Rechenregel für die Inverse einer Matrix lautet:

Satz. Wenn $A, B \in \mathbb{K}^{n \times n}$ invertierbar sind, so ist AB (und BA) invertierbar, und es ist

$$\boxed{(AB)^{-1} = B^{-1}A^{-1}}.$$

Diese auf den ersten Blick erstaunliche Umkehrung der Reihenfolge lässt sich leicht einsehen, wenn man die zugehörigen linearen Abbildungen betrachtet und sich erinnert, dass $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$; ein direkter Beweis kann jedoch auch einfach erfolgen unter Verwendung der Assoziativität der Matrix-Matrix-Multiplikation: $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AE_nA^{-1} = AA^{-1} = E_n$ und umgekehrt auch $(B^{-1}A^{-1})(AB) = \dots = E_n$, woraus die obige Behauptung folgt.

Aus obigem Satz folgt, dass die Menge der invertierbaren Matrizen abgeschlossen ist bezüglich der Multiplikation. Die Menge der invertierbaren Matrizen (von Algebraikern mit $GL(n, \mathbb{K})$ bezeichnet, für frz. *groupe linéaire* oder engl. *general linear group*) ist also eine (nichtkommutative) Gruppe. (Jedoch ist natürlich auch $(GL(n, \mathbb{K}), +, \cdot)$ i.a. *kein* Körper, da diese Menge nicht bezüglich '+' abgeschlossen ist.)

Berechnung von Inversen von Matrizen bzw. von Umkehrfunktionen linearer Abbildungen.

Es bleibt nun noch zu untersuchen, wie wir *Umkehrfunktionen* linearer Abbildungen effizient mit Hilfe von Matrixschreibweise und Gauß-Algorithmus berechnen können (dies wurde bereits auf Blatt 9 für ein Beispiel durchgeführt, hier nochmal die *allgemeine* Version).

Da die Verkettung von linearen Abbildungen in Matrixschreibweise gerade der Matrix-Matrix-Multiplikation entspricht, entspricht das Suchen einer Umkehrabbildung gerade dem Suchen nach einer *inversen Matrix*: Ist A die zu einer (bijektiven) linearen Abbildung gehörende Matrix, so ist die inverse Matrix A^{-1} gerade die zur Umkehrabbildung f^{-1} gehörende Matrix.

Damit eine lineare Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ überhaupt eine Umkehrfunktion f^{-1}

⁵³Zur Erinnerung: Wir kannten bisher als Beispiele für Ringe die Menge der ganzen Zahlen sowie die Menge der Polynome; beide dieser Ringe sind kommutativ. Die Menge der quadratischen Matrizen $\mathbb{K}^{n \times n}, +, \cdot$ ist, zusammen mit dem dazu 'isomorphen' Ring $(\text{Lin}(\mathbb{K}^n, \mathbb{K}^n), +, \circ)$ unser erstes Beispiel für einen nicht-kommutativen Ring. (Aber auch $(\text{Abb}(\mathbb{K}^n, \mathbb{K}^n), +, \circ)$ ist ein nichtkommutativer Ring mit Eins.)

Zwei Ringe R, S heißen isomorph, wenn es eine bijektive Abbildung $f : R \rightarrow S$ gibt mit $f(a+b) = f(a)+f(b)$ und $f(a \cdot b) = f(a) \cdot f(b)$ für alle $a, b \in R$.

hat, muss f natürlich bijektiv sein. Nach dem Satz aus Kap. 3.3 muss dazu notwendigerweise die Dimension von Urbildraum und Wertevorrat gleich sein: $m = n$. Die Aufgabenstellung ist also nur sinnvoll für $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$, wenn also die zugehörige Matrix A *quadratisch* ist (heißt: gleich viele Spalten wie Zeilen hat). In Matrix-Sprechweise also: Das Suchen nach Inversen von Matrizen ist nur sinnvoll für *quadratische* Matrizen. Wir wollen $f^{-1} : \mathbb{K}^n \rightarrow \mathbb{K}^n$ berechnen, d.h. wir wollen die Vektoren $f^{-1}(\vec{e}_1), \dots, f^{-1}(\vec{e}_n)$ angeben, denn das sind die Spalten der zu f^{-1} gehörenden Matrix, also die Spalten von $A^{-1} =: (b_{ij})$. Diese gesuchten Vektoren bezeichnen wir mit $f^{-1}(\vec{e}_1) =: \vec{b}_1, \dots, f^{-1}(\vec{e}_n) =: \vec{b}_n$. Die gesuchten Vektoren sollen also die Bedingungen

$$f(\vec{b}_1) = \vec{e}_1, \dots, f(\vec{b}_n) = \vec{e}_n \quad (*)$$

erfüllen. Wir stellen \vec{b}_j bezüglich der Standardbasis dar:

$$\vec{b}_1 = \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} = \sum_{i=1}^n b_{i1} \vec{e}_i, \quad \dots, \quad \vec{b}_n = \begin{pmatrix} b_{1n} \\ \vdots \\ b_{nn} \end{pmatrix} = \sum_{i=1}^n b_{in} \vec{e}_i,$$

d.h. wir suchen jetzt die Komponenten der Vektoren \vec{b}_j , d.h. die b_{ij} . Mit der Linearität von f erhalten wir aus (*) die Bedingungen

$$\sum_{i=1}^n f(\vec{e}_i) b_{i1} = \vec{e}_1, \quad \dots, \quad \sum_{i=1}^n f(\vec{e}_i) b_{in} = \vec{e}_n$$

Jede dieser n Bedingungen stellt für sich genommen ein LGS dar, das nun gelöst werden muss; die b_{ij} sind die Unbekannten. Alle diese n linearen Gleichungssysteme haben jedoch *die selbe* Systemmatrix, bestehend aus den (gegebenen) Spaltenvektoren $f(\vec{e}_i)$; die Systemmatrix ist also jedesmal die zu f gehörende Matrix, also A . Lediglich die rechten Seiten der n Gleichungssysteme unterscheiden sich; sie sind $\vec{e}_1, \dots, \vec{e}_n$. Statt *nacheinander* diese n LGS

$$(A|\vec{e}_1), \dots, (A|\vec{e}_n)$$

zu lösen, können wir, um Zeit und Platz zu sparen, diese n LGS *simultan* lösen: Wir führen die Gauß-Elimination für das Schema

$$(A|\vec{e}_1|\dots|\vec{e}_n),$$

oder, noch kürzer geschrieben, für das Schema

$$(A|E_n),$$

durch. Wenn wir hier die Gauß-Jordan-Variante verwenden (d.h. wir erzeugen nicht nur unterhalb sondern auch oberhalb der Diagonalen Nullen), also solange rechnen, bis auf der linken Seite die Einheitsmatrix erscheint, können wir die n Lösungsvektoren der n

linearen Gleichungssysteme direkt ablesen: Die gesuchten Vektoren $\vec{x}_1, \dots, \vec{x}_n$ lesen wir nach Durchführung von Gauß-Jordan in der rechten Seite des Schemas ab:

$$(A | \underbrace{\vec{e}_1 | \dots | \vec{e}_n}_{=E_n}) \longrightarrow \dots \longrightarrow (\underbrace{\vec{e}_1 | \dots | \vec{e}_n}_{E_n} | \underbrace{\vec{x}_1 | \dots | \vec{x}_n}_{=A^{-1}}).$$

Da die berechneten Spaltenvektoren $\vec{x}_1, \dots, \vec{x}_n$ gerade die lineare Abbildung f^{-1} repräsentieren, und da die zu f^{-1} gehörende Matrix gerade A^{-1} ist, haben wir somit auch ein *Verfahren zur Berechnung inverser Matrizen*:

$$\boxed{(A | E_n) \xrightarrow{\text{Gauß}} (E_n | A^{-1})}$$

Noch eine Bemerkung: Kann bei der Berechnung etwas schief gehen? Möglicherweise kann man die linke Hälfte nicht auf die Form der Einheitsmatrix bringen, d.h. die linearen Gleichungssysteme, die wir lösen wollen, sind nicht vom eindeutigen Typ. Das ist genau dann der Fall, wenn die Vektoren $f(\vec{e}_1), \dots, f(\vec{e}_n)$ linear abhängig waren, also, nach einem früheren Satz, die Abbildung f nicht bijektiv war. Fazit: Gelingt es nicht, auf der linken Seite die Einheitsmatrix zu erhalten, dann war die Abbildung f nicht bijektiv, d.h. dann gibt es keine Umkehrabbildung, bzw. dann ist die Matrix A nicht invertierbar, d.h. A^{-1} existiert dann nicht. Man muss also bei dem obigen Verfahren nicht vorab auf Existenz der inversen Matrix/der Umkehrfunktion prüfen; diese Frage beantwortet sich im Verlauf der Rechnung von selbst.

Beispiel zur Berechnung der Inversen einer Matrix (bzw. der Umkehrfunktion einer linearen Abbildung):

Sei $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 1 \end{pmatrix}$. Rechnung:

$$\begin{aligned} \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 2 & 1 & 1 & 0 & 0 & 1 \end{array} \right) &\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & -2 & 0 & 1 \end{array} \right) &\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & -3 & -2 & -1 & 1 \end{array} \right) \\ &\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \\ 0 & 1 & 0 & -\frac{4}{3} & \frac{1}{3} & \frac{2}{3} \\ 0 & 0 & 1 & \frac{2}{3} & \frac{1}{3} & -\frac{1}{3} \end{array} \right) \end{aligned}$$

Also $A^{-1} = \frac{1}{3} \begin{pmatrix} 1 & -1 & 1 \\ -4 & 1 & 2 \\ 2 & 1 & -1 \end{pmatrix}$.

Matrix-Vektor-Multiplikation.

Ist $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$ gegeben durch die zugehörige Matrix $A \in \mathbb{K}^{m \times n}$, also $f(\vec{e}_j) =$

$(a_{1j}, \dots, a_{mj})^T$, $j = 1, \dots, n$, dann ist es naheliegend zu fragen, wie man $f(\vec{x})$ berechnet unter Verwendung von A und \vec{x} . Wir rechnen:

$$f(\vec{x}) = f\left(\sum_{j=1}^n x_j \vec{e}_j\right) = \sum_{j=1}^n x_j f(\vec{e}_j) = \sum_{j=1}^n x_j \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1j} x_j \\ \vdots \\ \sum_{j=1}^n a_{mj} x_j \end{pmatrix}$$

Wir definieren nun ein sog. Matrix-Vektor-Produkt $A \cdot \vec{x}$ genau so, dass $A \cdot \vec{x} = f(\vec{x})$ gilt. Oben ablesend definieren wir also:

Def. (Matrix-Vektor-Produkt) Sei $A \in \mathbb{K}^{m \times n}$ und $\vec{x} \in \mathbb{K}^n$. Dann sei $A\vec{x}$ der Vektor in \mathbb{K}^m mit den Komponenten

$$(A\vec{x})_i := \sum_{j=1}^n a_{ij} x_j \quad \forall i = 1, \dots, m.$$

Wir haben somit eine Multiplikation $\mathbb{K}^{m \times n} \times \mathbb{K}^n \rightarrow \mathbb{K}^m$ definiert. Der Multiplikationspunkt wird i.a. nicht hingeschrieben. Statt Multiplikation von A und \vec{x} sagt man auch 'A wird auf \vec{x} angewendet'. Das spiegelt die Tatsache wider, dass $A\vec{x}$ gleich der *Anwendung* der zugehörigen linearen Abbildung f auf \vec{x} , also $A\vec{x} = f(\vec{x})$, ist.

Beispiel Matrix-Vektor-Multiplikation:

$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 19 \\ 27 \\ 8 \end{pmatrix}$$

Interpretation: $f((2, 5)^T) = (19, 27, 8)^T$

Beachte, dass die Formate von Matrix und Vektor in gewisser Weise zusammenpassen müssen. Dies spiegelt den Sachverhalt wieder, dass eine lineare Abbildung auf \mathbb{K}^n definiert sein muss, damit man sie auf ein $\vec{x} \in \mathbb{K}^n$ anwenden kann.

Ferner beachte man, dass das Matrix-Vektor-Produkt identisch ist mit dem Matrix-Matrix-Produkt für den Fall, dass die 'rechte' Matrix aus nur einer Spalte besteht.

An dieser Stelle ist es sinnvoll, nochmal an lineare Gleichungssysteme zu denken.

Diese hatten ja die Form $\sum_{j=1}^n a_{ij} x_j = b_i$, $i = 1, \dots, r$. Mit obiger Matrix-Vektor-Multiplikation können wir dieses LGS also kurz schreiben als⁵⁴

$$\boxed{A\vec{x} = \vec{b}} !$$

⁵⁴Im Zusammenhang mit der Matrix-Vektor-Multiplikation ist es einsichtig, warum es sinnvoll ist, Vektoren als Spalten zu schreiben (statt, wie zu Beginn des Kurses für Tupel, als Zeilenvektor; anders formuliert, warum es sinnvoll ist, Spaltenvektoren und Zeilenvektoren (\vec{x}, \vec{x}^T) sauber zu unterscheiden: Auf einen Zeilenvektor kann man die Matrix-Vektor-Multiplikation nicht anwenden.

Rechenregeln: Die die Matrix-Vektor-Multiplikation ein Spezialfall der Matrix-Matrix-Multiplikation ist, gelten auch Assoziativ- und Distributivgesetze entsprechend:

$$(AB)\vec{x} = A(B\vec{x}) =: AB\vec{x}, \quad (A+B)\vec{x} = A\vec{x} + B\vec{x}, \quad A(\vec{x}+\vec{y}) = A\vec{x} + A\vec{y}$$

Neben dieser wichtigen Anwendung zur Notation von Linearen Gleichungssystemen hat die Matrix-Vektor-Multiplikation noch eine weitere Bedeutung, und zwar im Zusammenhang mit Linearkombinationen von Vektoren: Bei der Matrix-Vektor-Multiplikation werden die Einträge der 1. Spalte der Matrix mit dem 1. Eintrag des Vektors multipliziert, die Einträge der 2. Spalte der Matrix mit dem 2. Eintrag des Vektors, usw.. Daraus folgt:

Die Anwendung einer Matrix auf einen Vektor ist derjenige Vektor, den man erhält, wenn man eine Linearkombination der Spalten der Matrix mit den Einträgen des Vektors als Koeffizienten berechnet.

Im obigen Zahlenbeispiel:

$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \end{pmatrix} = 2 \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix} + 5 \begin{pmatrix} 3 \\ 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 19 \\ 27 \\ 8 \end{pmatrix}$$

Zusammenhang Inverse Matrix und Lösung von Linearen Gleichungssystemen.

Betrachten wir ein LGS

$$A\vec{x} = \vec{b}$$

mit quadratischer Systemmatrix A . Falls A invertierbar ist, so kann man durch Anwendung von A^{-1} auf diese Gleichung die Gleichung

$$\vec{x} = A^{-1}\vec{b}$$

bekommen! Das bedeutet zum einen eine 'explizite' Lösungsformel; zum anderen, dass das LGS genau eine Lösung hat! Ist die Systemmatrix invertierbar, so hat ein zugehöriges LGS (für jedes beliebige \vec{b}) also genau eine Lösung! Um zu klären, ob auch die Umkehrung gilt, brauchen wir einen Hilfssatz:

Satz. Für eine lineare Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$ gilt:

$$f \text{ injektiv} \iff f \text{ surjektiv} \iff f \text{ bijektiv}$$

Diese erstaunliche Tatsache ist eine Folgerung aus dem Satz über die Charakterisierung von Injektivität/Surjektivität/Bijektivität von linearen Abbildungen auf S. 72:

f injektiv \iff Spalten von zug. Matrix A l.u. \iff Stufenform von A hat in jeder Spalte eine Stufe $\xleftrightarrow{A \text{ quadratisch}}$ Stufenform von A hat $n = \dim(\text{Zielraum})$ viele Stufen \iff Spalten von A bilden EZS des Zielraums $\iff f$ surjektiv \square

Wichtig: Diese Äquivalenz von Injektivität und Surjektivität gilt nur, wenn die beiden Räume, zwischen denen f operiert, die gleiche Dimension haben!

Nun zurück zur Frage, ob unter der Voraussetzung, dass ein LGS genau eine Lösung hat, die Invertierbarkeit der zugehörigen Systemmatrix folgt:

Es habe das LGS $A\vec{x} = \vec{b}$, mit quadratischer Matrix A , genau eine Lösung. Dann hat, da die Lösungsmenge des inhomogenen Systems nur die Verschiebung der Lösungsmenge des homogenen Systems $A\vec{x} = \vec{0}$ ist, auch das homogenen System genau eine Lösung (die Null-Lösung), d.h. der Kern von A ist trivial, und somit ist die zu A gehörende lineare Abbildung f injektiv. Nach obigem Satz ist f dann bijektiv, also A invertierbar.

Wir fassen beide Richtungen zusammen:

Satz. Für lineare Gleichungssysteme $A\vec{x} = \vec{b}$ mit quadratischer Matrix A gilt: Das LGS ist (für eine beliebige rechte Seite) genau dann eindeutig lösbar, wenn A invertierbar ist. In diesem Fall ist die Lösung gegeben durch $\vec{x} = A^{-1}\vec{b}$.

Bemerkung zur Nützlichkeit: Diese Formel ist nicht von allzu großem praktischen Nutzen: Wir haben gesehen, dass die Berechnung einer Inversen aufwändiger ist als das direkte Lösen eines LGS, da das Gauß-Verfahren auf ein größeres Schema angewendet werden muss. Der Umweg, lineare Gleichungssysteme über die Berechnung der inversen Matrix zu lösen, ist also nicht zu empfehlen.

Die Transponierte einer Matrix.

Def. Die *transponierte Matrix* einer Matrix $A = (a_{ij}) \in \mathbb{K}^{m \times n}$ ist die Matrix $A^T := (a_{ji}) \in \mathbb{K}^{n \times m}$. (Schreibweise oft auch A^t statt A^T .)

Das heißt: Der Eintrag, der in A in Zeile i und Spalte j steht, steht in der Matrix A^T in Zeile j und Spalte i . Man transponiert eine Matrix also, indem man an der Hauptdiagonalen spiegelt (Zeilen und Spalten vertauscht):

$$A = \begin{pmatrix} 1 & 3 & 0 \\ 2 & 5 & 7 \end{pmatrix} \implies A^T = \begin{pmatrix} 1 & 2 \\ 3 & 5 \\ 0 & 7 \end{pmatrix}$$

Rechenregeln (Beweise siehe ggf. Übung): Die wichtigsten sind: $(A^T)^T = A$, $(AB)^T = B^T A^T$, und für quadratisches invertierbares A : $(A^T)^{-1} = (A^{-1})^T$.

Der Rang von Matrizen.

Def. (Matrixrang). Der *Rang*⁵⁵ einer Matrix bzw. der zugehörigen linearen Abbildung ist die Dimension des Bildes der zugehörigen linearen Abbildung, also gleich der Dimension des Raumes, der von den Spalten der Matrix aufgespannt wird.

Also: Sei $A \in \mathbb{K}^{m \times n}$ und $f : \mathbb{K}^n \rightarrow \mathbb{K}^m$. Dann ist

$$\text{rang}(A) := \text{rang}(f) := \dim(\text{Bild}(f)) \leq n.$$

⁵⁵engl.: rank

Sind alle Spalten einer Matrix linear unabhängig, so ist also $\text{Rang}(A) = n$; man sagt dann auch, die Matrix habe vollen Spaltenrang.

Wie man den Rang einer Matrix praktisch berechnet, haben wir bereits auf S. 63 kennengelernt, nämlich dort haben wir die Dimension des Bildes von linearen Abbildungen berechnet (nämlich als Anzahl der Stufen der Stufenform von A).

Man kann zeigen (wir wollen hier auf einen Beweis verzichten):

Satz. $\text{rang}(A) = \text{rang}(A^T)$.⁵⁶

Da die Spalten von A gerade die Zeilen von A^T sind, bedeutet das:

Die Dimension des Raumes, der von den Spalten(-vektoren) einer Matrix aufgespannt wird, und die Dimension des Raumes, der von den Zeilen(-vektoren) einer Matrix aufgespannt wird, ist immer gleich: Beispiel: Für $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ ist

$$\dim \left(\text{span} \left\{ \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix} \right\} \right) = \dim \left(\text{span} \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\} \right) = 2. \text{ Deshalb}$$

ist der Rang einer Matrix immer sowohl kleiner gleich der Spalten- als auch der Zeilenzahl:

$$\text{rang}(A) = \dim(\text{Bild}(f)) \leq \min\{m, n\}$$

Im Fall *quadratischer*(!) Matrizen $A \in \mathbb{K}^{n \times n}$ folgt, da der Raum, der von den Spalten aufgespannt wird, und der Raum, der von den Zeilen aufgespannt wird, immer die gleiche Dimension haben, dass die Zeilen der Matrix genau dann linear unabhängig sind, wenn die Spalten linear unabhängig sind. Wir können somit die beiden vorangegangenen Sätze zusammenfassen und ergänzen zu:

Satz. Für eine lineare Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$ und die zugehörige Matrix $A \in \mathbb{K}^{n \times n}$ gilt die Äquivalenz:

$$\begin{aligned} f \text{ injektiv} &\iff f \text{ surjektiv} \iff f \text{ bijektiv} \iff A^{-1} \text{ existiert} \\ &\iff \text{das LGS } A\vec{x} = \vec{b} \text{ hat für alle } \vec{b} \in \mathbb{K}^n \text{ jeweils genau eine Lösung} \\ &\iff \text{die Spalten von } A \text{ sind l.u.} \iff \text{die Zeilen von } A \text{ sind l.u.} \end{aligned}$$

Für "f injektiv" können wir die uns bekannte Charakterisierungen, wie "Kern(f) = {0}" und "Spalten von A sind l.u." aus dem Satz über die Charakterisierung von injektiven linearen Abbildungen ebenfalls in die obige Kette der Äquivalenzen einfügen, ebenso die uns bekannten Charakterisierungen der Surjektivität als "Bild(f) = \mathbb{K}^n ", "Spalten von A bilden EZS von \mathbb{K}^n ", "Rang(A) = n".

⁵⁶Ein Beweis könnte so erfolgen, dass man zeigt, dass eine Stufenform von A und eine Stufenform von A^T gleich viele Stufen haben.

3.5 Determinanten

In diesem Kapitel geht es darum, den *Volumeninhalt* eines sog. *Spats* zu berechnen. (Genau dies ist nämlich die geometrische Deutung der Determinante.)

Def. (Spat). Ein *Spat* (auch genannt: *Parallelotop*, *Parallelfach*, *Parallelepipid*) ist eine Menge (Teilmenge des \mathbb{R}^n) der Form

$$\left\{ \sum_{i=1}^n \alpha_i \vec{a}_i \mid \forall i=1, \dots, n : 0 \leq \alpha_i \leq 1 \right\}$$

für gegebene Vektoren $\vec{a}_1, \dots, \vec{a}_n \in \mathbb{R}^n$. Im Fall $n=2$ ist ein Spat ein *Parallelogramm*.

Wir wollen eine Formel für das ('orientierte')⁵⁷ Volumen V eines von n Vektoren des \mathbb{R}^n aufgespannten Spats aufstellen. Da wir (nur) in den Fällen $n=2$ und $n=3$ eine gute anschauliche Vorstellung davon haben, was wir unter dem Volumen (Flächeninhalt im Fall $n=2$) eines Spats/Parallelogramms haben, wollen wir uns überlegen, welche Eigenschaften die Formel $V(\vec{a}_1, \dots, \vec{a}_n)$ in den Fällen $n \in \{2, 3\}$ hat und wollen fordern, dass diese Eigenschaften auch für größere n gelten soll.

Im Fall $n \in \{2, 3\}$ muss eine Volumenformel $V(\vec{a}_1, \dots, \vec{a}_n)$ offensichtlich folgende Eigenschaften haben:

1. Normierungseigenschaft:
 $V(\vec{e}_1, \dots, \vec{e}_n) = 1$ (d.h. der Einheitswürfel soll das Volumen 1 haben)
2. Linearität in jedem Argument (= "Multilinearität"):
 $V(\vec{a}_1, \dots, \vec{a}_{k-1}, \alpha \vec{a}_k, \vec{a}_{k+1}, \dots, \vec{a}_n) = \alpha V(\vec{a}_1, \dots, \vec{a}_n)$ und
 $V(\vec{a}_1, \dots, \vec{a}_{k-1}, \vec{a}_k + \vec{y}, \vec{a}_{k+1}, \dots, \vec{a}_n) = V(\vec{a}_1, \dots, \vec{a}_{k-1}, \vec{a}_k, \vec{a}_{k+1}, \dots, \vec{a}_n) + V(\vec{a}_1, \dots, \vec{a}_{k-1}, \vec{y}, \vec{a}_{k+1}, \dots, \vec{a}_n)$
3. $\vec{a}_1, \dots, \vec{a}_n$ linear abhängig $\implies V(\vec{a}_1, \dots, \vec{a}_n) = 0$

Wie wir gleich sehen werden, reichen diese drei Eigenschaften aus, um das Volumen V für jeden beliebigen Spat im \mathbb{R}^n auszurechnen!

Als Vorüberlegung einige Folgerungen aus obigen Eigenschaften:

4. Beim Vertauschen zweier Argumente (Spalten) a_i, a_j ($i \neq j$) ändert sich (nur) das Vorzeichen von V :⁵⁸ $V(\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_j, \dots, \vec{a}_n) = -V(\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_i, \dots, \vec{a}_n)$.
 Beweis: Es ist $V(\vec{a}_1, \dots, \vec{a}_i + \vec{a}_j, \dots, \vec{a}_i + \vec{a}_j, \dots, \vec{a}_n) = 0$, da die Argumente linear abhängig sind. Mit der Multilinearität folgt $V(\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_i, \dots, \vec{a}_n) +$

⁵⁷Unsere Formel wird sowohl positive als auch negative Werte liefern können, je nachdem ob die Vektoren ein sog. Rechts- oder ein Linkssystem bilden.

⁵⁸Geometrische Deutung: Beim Vertauschen von zwei Vektoren wird aus einem Rechts- ein Linkssystem und umgekehrt.

$V(\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_j, \dots, \vec{a}_n) + V(\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_i, \dots, \vec{a}_n) + V(\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_j, \dots, \vec{a}_n) = 0$.
 Der erste und der letzte Summand sind null, wieder wegen linearer Abhängigkeit.
 Es folgt die Behauptung.

5. Besteht eine Spalte oder eine Zeile der aus $\vec{a}_1, \dots, \vec{a}_n$ gebildeten Matrix $A \in \mathbb{R}^{n \times n}$ vollständig aus Nullen, so ist $V(\vec{a}_1, \dots, \vec{a}_n) = 0$.

Beweis: Im Fall einer Nullspalte ist die Aussage klar, da dann die Spalten linear abhängig sind. Im Fall einer Nullzeile ist $\text{rang}(A) < n$, also sind nach einem Satz aus dem vorigen Kapitel die Spalten von A linear abhängig, und es folgt die Behauptung.

6. Addiert man zu einer Spalte a_i ein Vielfaches einer anderen Spalte a_j ($i \neq j$), so ändert sich die Determinante nicht:

$$V(\vec{a}_1, \dots, \vec{a}_i + \alpha \vec{a}_j, \dots, \vec{a}_n) = V(\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_n) + \alpha \underbrace{V(\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_n)}_{=0 \text{ wegen (3.)}}$$

$$\text{Beispiel: } V \left(\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix} \right) = V \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix} \right)$$

Wir können nun eine Berechnung von V vornehmen. Aus Gründen der Übersichtlichkeit führen wir sie hier für $n=2$ und für $n=3$ durch; die Rechnung funktioniert aber offensichtlich auch für alle anderen $n \in \mathbb{N}$:

$$V \left(\begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} \right) = V \left(\begin{pmatrix} a_{11} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_{21} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} \right)$$

$$\stackrel{(2.)}{=} V \left(\begin{pmatrix} a_{11} \\ 0 \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} \right) + V \left(\begin{pmatrix} 0 \\ a_{21} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} \right)$$

$$= V \left(\begin{pmatrix} a_{11} \\ 0 \end{pmatrix}, \begin{pmatrix} a_{12} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_{22} \end{pmatrix} \right) + V \left(\begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}, \begin{pmatrix} a_{12} \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_{22} \end{pmatrix} \right)$$

$$\stackrel{(2.)}{=} \underbrace{V \left(\begin{pmatrix} a_{11} \\ 0 \end{pmatrix}, \begin{pmatrix} a_{12} \\ 0 \end{pmatrix} \right)}_{=0 \text{ nach (5.)}} + V \left(\begin{pmatrix} a_{11} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ a_{22} \end{pmatrix} \right) + V \left(\begin{pmatrix} 0 \\ a_{21} \end{pmatrix}, \begin{pmatrix} a_{12} \\ 0 \end{pmatrix} \right) + \underbrace{V \left(\begin{pmatrix} 0 \\ a_{21} \end{pmatrix}, \begin{pmatrix} 0 \\ a_{22} \end{pmatrix} \right)}_{=0 \text{ nach (5.)}}$$

$$\stackrel{(2.)}{=} a_{11} a_{22} V \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) + a_{21} a_{12} V \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

$$\stackrel{(4.)}{=} a_{11} a_{22} V \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) - a_{21} a_{12} V \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

$$\stackrel{(1.)}{=} a_{11} a_{22} - a_{21} a_{12}$$

$$\begin{aligned}
& +V \begin{pmatrix} 0 & 0 & a_{13} \\ a_{21} & 0 & 0 \\ 0 & a_{22} & 0 \end{pmatrix} + V \begin{pmatrix} 0 & 0 & 0 \\ a_{21} & 0 & a_{23} \\ 0 & a_{32} & 0 \end{pmatrix} + V \begin{pmatrix} 0 & 0 & 0 \\ a_{21} & 0 & 0 \\ 0 & a_{32} & a_{33} \end{pmatrix} \\
& +V \begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & 0 \\ a_{31} & 0 & 0 \end{pmatrix} + V \begin{pmatrix} 0 & a_{12} & 0 \\ 0 & 0 & a_{32} \\ a_{13} & 0 & 0 \end{pmatrix} + V \begin{pmatrix} 0 & a_{12} & 0 \\ 0 & 0 & 0 \\ a_{31} & 0 & a_{33} \end{pmatrix} \\
& +V \begin{pmatrix} 0 & 0 & a_{13} \\ 0 & a_{22} & 0 \\ a_{31} & 0 & 0 \end{pmatrix} + V \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ a_{31} & 0 & 0 \end{pmatrix} + V \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_{22} & 0 \\ a_{31} & 0 & a_{33} \end{pmatrix} \\
& +V \begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & 0 \\ a_{31} & a_{32} & 0 \end{pmatrix} + V \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_{23} \\ a_{31} & a_{32} & 0 \end{pmatrix} + V \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}
\end{aligned}$$

Alle Matrizen, in denen eine Nullzeile vorkommt, liefern keinen Beitrag. Bei allen übrigen Matrizen ziehen wir Faktoren mittels der Linearität heraus. Wir erhalten

$$\begin{aligned}
& V \left(\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \end{pmatrix}, \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \end{pmatrix} \right) \\
& = a_{11}a_{22}a_{33}V \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + a_{11}a_{23}a_{32}V \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} + a_{12}a_{21}a_{33}V \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
& + a_{13}a_{21}a_{32}V \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + a_{12}a_{23}a_{31}V \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + a_{13}a_{22}a_{31}V \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}
\end{aligned}$$

Jede der stehengebliebenen Matrizen hat in jeder Zeile und in jeder Spalte genau eine Eins. Durch Tausch von Spalten unter Beachtung des Vorzeichenwechsels folgt

$$\begin{aligned}
V \left(\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \end{pmatrix}, \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \end{pmatrix} \right) & = a_{11}a_{22}a_{33}V(E_3) - a_{11}a_{23}a_{32}V(E_3) - a_{12}a_{21}a_{33}V(E_3) \\
& + a_{13}a_{21}a_{32}V(E_3) + a_{12}a_{23}a_{31}V(E_3) - a_{13}a_{22}a_{31}V(E_3)
\end{aligned}$$

Da $V(E_3) = 1$ folgt

$$\begin{aligned}
V \left(\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \end{pmatrix}, \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \end{pmatrix} \right) & = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} \\
& + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31}
\end{aligned}$$

Eine solche Rechnung lässt sich offenbar auch für andere $n \in \mathbb{N}$ durchführen.

Fazit: Die obigen drei Bedingungen 1.-3. legen $V(\vec{a}_1, \dots, \vec{a}_n)$ eindeutig fest, d.h. es gibt nur *genau eine* Funktion $V : \mathbb{R}^n \times \dots \times \mathbb{R}^n \rightarrow \mathbb{R}$ mit den drei obigen Eigenschaften einer Volumenformel. Wir nennen diese eindeutig bestimmte Funktion V von nun an die **Determinante** der Vektoren $\vec{a}_1, \dots, \vec{a}_n$ bzw. der aus den Vektoren gebildeten Matrix:

$$\det[\vec{a}_1, \dots, \vec{a}_n] := V(\vec{a}_1, \dots, \vec{a}_n)$$

Die n Vektoren $\vec{a} \in \mathbb{K}^n$ bilden eine $n \times n$ -Matrix $A = (a_{ij})$; daher schreibt man i.a. auch

$\det(A)$ anstelle von $\det[\vec{a}_1, \dots, \vec{a}_n]$:

$$\det(A) := V(\vec{a}_1, \dots, \vec{a}_n)$$

Die Determinante $\det : \underbrace{\mathbb{R}^n \times \dots \times \mathbb{R}^n}_{n \text{ mal}} \rightarrow \mathbb{R}$ (oder auch $\det : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}$) hat also die Eigenschaften 1.-6.

Wir wollen uns nun überlegen, wie diese Formel für allgemeine $n \in \mathbb{N}$ lauten muss. Dazu müssen wir uns insbesondere überlegen, wie wir Matrizen, die in jeder Zeile und in jeder Spalte genau einen Eintrag a_{ij} haben und ansonsten nur Nullen, sich allgemein mathematisch beschreiben lassen, und wie wir das zu verwendende Vorzeichen vor jedem Summanden mathematisch exakt beschreiben können. Dazu brauchen wir sog. *Permutationen*.

Einschub/Wiederholung: Permutationen

Def. Eine Permutation auf der Menge $\{1, \dots, n\}$ ist eine bijektive Abbildung $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. Die Menge aller Permutationen auf $\{1, \dots, n\}$ wird mit S_n bezeichnet:

$$S_n := \{\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid \sigma \text{ ist bijektiv}\},$$

Eine Permutation heißt *Transposition* (oder *Vertauschung*), wenn sie lediglich zwei Elemente aus $\{1, \dots, n\}$ vertauscht und alle anderen fix lässt, also $\sigma(i) = j$, $\sigma(j) = i$ für feste $i \neq j \in \{1, \dots, n\}$, und $\sigma(k) = k$ für alle $k \in \{1, \dots, n\} \setminus \{i, j\}$.

Man kann zeigen: Jede Permutation lässt sich als Verkettung von Transpositionen schreiben. Je nachdem, ob die Anzahl der dazu benötigten Transpositionen gerade oder ungerade ist, sagt man, das *Signum* der Permutation $\sigma \in S_n$ ist $+1$ bzw. -1 :

$$\text{sgn}(\sigma) := (-1)^{\#\text{Transpositionen}}$$

Man kann zeigen: $\text{sgn}(\sigma) = \text{sgn}(\sigma^{-1})$ (siehe Übung).

Es gibt $n!$ Permutationen auf $\{1, \dots, n\}$, d.h. S_n hat $n!$ Elemente. Die Summanden, die die Formel für die Determinante ergeben, sind (s.o., Fall $n=3$) gerade diejenigen, die in jeder Zeile und in jeder Spalte einen Eintrag a_{ij} haben, und ansonsten nur Nullen. Solche Matrizen kann man in der Form

$$M = M(\sigma) = (m_{ij}) \quad \text{mit} \quad m_{ij} = \begin{cases} a_{ij} & , \text{ falls } j = \sigma(i) \\ 0 & , \text{ sonst} \end{cases}$$

schreiben, denn die Bijektivität einer Permutation sorgt dann dafür, dass in jeder Spalte genau ein von Null verschiedenes Element steht. So z.B. ergibt die Permutation σ mit $\sigma(1)=2$, $\sigma(2)=3$, $\sigma(3)=1$ die Matrix

$$M(\sigma) = \begin{pmatrix} 0 & a_{12} & 0 \\ 0 & 0 & a_{23} \\ a_{31} & 0 & 0 \end{pmatrix}$$

Es ist somit

$$\det[\vec{a}_1, \dots, \vec{a}_n] = \det(A) = \sum_{\sigma \in S_n} \det(M(\sigma)).$$

Und die Determinante einer solchen Matrix $M(\sigma)$ ist, bis aufs Vorzeichen, gerade das Produkt aus den vorhandenen nichtverschwindenden Einträgen, also $\prod_{i=1}^n a_{i,\sigma(i)}$. Das Vorzeichen des Terms ergibt sich daraus, wie oft Spalten vertauscht werden müssen, um auf Diagonalform zu kommen, also daraus, wie viele Transpositionen (=Vertauschungen) man braucht, um σ zu bilden.

Führt man also die Rechnung, die wir oben für $n=2$ und $n=3$ durchgeführt haben, für *allgemeines* $n \in \mathbb{N}$ durch, so ergibt sich demnach folgende allgemeine Formel für die Determinante:

$$\det[\vec{a}_1, \dots, \vec{a}_n] = \det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}$$

Diese Formel heißt **Leibniz-Formel**⁵⁹ der Determinante.

Man kann zeigen, dass es genau $n!$ Elemente in S_n gibt, dass also obige Leibniz-Formel für die Determinante $n!$ Summanden enthält und somit $(n-1) \cdot n!$ Multiplikationen erfordert. Zum Beispiel für $n=5$ sind das 480 Multiplikationen; für $n=10$ mehr als $32 \cdot 10^6$. Für praktische Zwecke ist die Leibniz-Formel für $n > 3$ daher äußerst unbefriedigend. Jedoch liefert sie folgendes Resultat:

Satz.

$$\det(A) = \det(A^T)$$

Beweis. Nach der Leibniz-Formel für A^T ist

$$\det(A^T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n a_{\sigma(i),i}$$

Mit der Substitution $j := \sigma(i)$ folgt

$$\det(A^T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^n a_{j,\sigma^{-1}(j)}$$

Da $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ folgt mit Setzung $\tau := \sigma^{-1}$:

$$\det(A^T) = \sum_{\tau^{-1} \in S_n} \operatorname{sgn}(\tau) \prod_{j=1}^n a_{j,\tau(j)}$$

Da $\tau \in S_n \Leftrightarrow \tau^{-1} \in S_n$, folgt

$$\det(A^T) = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \prod_{j=1}^n a_{j,\tau(j)} = \det(A).$$

⁵⁹Gottfried Wilhelm Leibniz, 1646-1716. Neben Verdiensten um die Lineare Algebra (Determinanten) ist Leibniz - zusammen mit seinem 'Gegenspieler' Isaac Newton - auch der Begründer der Differentialrechnung, insbesondere des Begriffs der Ableitung

Der Satz hat die wichtige Konsequenz:

Weitere Eigenschaften der Determinante. Die Eigenschaften 2., 3., 4., 6., die das Verhalten der Determinante bei Manipulation von *Spalten* beschreiben, gelten sinngemäß genau so für Manipulation von *Zeilen*! Man darf also beispielsweise ein Vielfaches einer Zeile zu einer anderen Zeile addieren, ohne dass sich der Wert der Determinante ändert, und man darf Faktoren aus einer Zeile aus der Determinante herausziehen. Dies werden wir später benutzen, um Matrizen effizient zu berechnen.

Zunächst der wichtige

Satz (Laplace'scher Entwicklungssatz). Die Berechnung einer $n \times n$ -Determinante kann man zurückführen auf die Berechnung von $(n-1) \times (n-1)$ -Determinanten per

$$\det(A) = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det(A_{i,j}), \quad j \in \{1, \dots, n\}$$

oder

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det(A_{i,j}), \quad i \in \{1, \dots, n\}$$

wobei $A_{i,j}$ die $(n-1) \times (n-1)$ -Matrix sei, die aus A durch Streichen der i -ten Zeile und der j -ten Spalte entsteht. Man sagt: "Die Determinante wird entwickelt nach der j -ten Spalte" (obere Gleichung) bzw. "... nach der i -ten Zeile" (untere Gleichung).

Die Koeffizienten $(-1)^{i+j}$ ergeben dabei ein 'Vorzeichenmuster'

$$\begin{pmatrix} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & - & \dots \\ - & + & - & + & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Der Beweis kann unter Verwendung der Leibniz-Formel erfolgen.

Beispiel:

Entwicklung nach der 1. Spalte:

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

Entwicklung nach der 2. Zeile:

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

Für Determinanten sehr großen Formats ist die rekursive Berechnung nach dem Laplace'schen Entwicklungssatz jedoch auch sehr aufwändig. Großen Nutzen ziehen wir aus dem Laplace'schen Entwicklungssatz jedoch dadurch, dass dieser die folgende Folgerung erlaubt:

Folgerung (Determinante für Dreiecksmatrizen). Die Determinante einer (rechten/oberen oder auch einer linken/unteren) Dreiecksmatrix ist gleich dem Produkt ihrer Diagonaleinträge:

$$\det \begin{pmatrix} a_{11} & \dots & \dots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} = \prod_{i=1}^n a_{ii}$$

Beweis: Folgt sofort durch wiederholtes Entwickeln nach der ersten Spalte:

$$\begin{aligned} \det \begin{pmatrix} a_{11} & \dots & \dots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} &= a_{11} \cdot \det \begin{pmatrix} a_{22} & \dots & \dots & a_{2n} \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} [+0 + \dots + 0] \\ &= a_{11} \cdot [a_{22} \cdot \det \begin{pmatrix} a_{33} & \dots & \dots & a_{3n} \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} + 0 + \dots + 0] = \dots = \prod_{i=1}^n a_{ii} \end{aligned}$$

Bemerkung: Alternativ zu obigem Beweis kann man die Formel auch aus der Leibniz-Formel herauslesen: Für Dreiecksmatrizen ist nur ein einziger Summand in der Leibniz-Formel von null verschieden, und zwar gerade derjenige, der der Permutation $\sigma = \text{id}$ entspricht, also $\prod_{i=1}^n a_{ii}$.

Nun haben wir alles beisammen, um auch Determinanten großen Formats effizient zu berechnen:

Praktische Berechnung von Determinanten großen Formats: Mit elementaren Zeilen- und Spaltenoperationen (Addition eines Vielfachen einer Zeile/Spalte zu einer anderen Zeile/Spalte, Vertauschen von Zeilen, Vertauschen von Spalten) bringen wir eine gegebene Determinante auf Dreiecksform. Dies erfordert (vgl. Gauß-Elimination) nicht mehr als n^3 Operationen, was akzeptabel ist. Mit obiger Folgerung lesen wir dann das Ergebnis als Produkt der Diagonaleinträge ab.

Hier am Beispiel einer (3×3) -Matrix:

$$\det \begin{pmatrix} 1 & 3 & 1 \\ 1 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & 3 & 1 \\ 0 & -2 & 1 \\ 0 & -6 & -1 \end{pmatrix} = \det \begin{pmatrix} 1 & 3 & 1 \\ 0 & -2 & 1 \\ 0 & 0 & -4 \end{pmatrix} = 1 \cdot (-2) \cdot (-4) = 8$$

wobei wir hier Vielfache von Zeilen zu Zeilen addiert haben; alternativ kann man auch Vielfache von Spalten zu Spalten addieren.

Vergleich des Verfahrens zur Berechnung der Determinante mit dem Gauß-Verfahren zum Lösen linearer Gleichungssysteme:

Es bestehen folgende Unterschiede:

- Bei der Berechnung der Determinante sind auch Spaltenoperationen erlaubt, bei Gauß i.a. nicht (bzw. bei Gauß bedeutet ein Tauschen von Spalten ein Vertauschen der Unbekannten).
- Bei Gauß ist die Multiplikation von Zeilen mit Faktoren $\neq 0$ erlaubt. Bei der Determinante kann man Faktoren bestenfalls herausziehen.

Determinanten und lineare (Un-)Abhängigkeit:

Nach Konstruktion ist für linear abhängige Spaltenvektoren die Determinante null. Gilt auch die Umkehrung? Dazu überführen wir durch wiederholtes Addieren eines Vielfachen einer Zeile zu einer anderen Zeile die gegebene Matrix A in eine Stufenform \tilde{A} . Bei diesen Operationen ändert sich die Determinante nicht: $\det(A) = \det(\tilde{A})$. Matrix \tilde{A} ist Dreiecksmatrix; die Determinante ist also genau dann ungleich null, wenn alle Diagonalelemente von \tilde{A} ungleich null sind. Das ist genau dann der Fall, wenn \tilde{A} vom Typ I ist, also alle Stufen die Breite 1 haben. Und dies ist, wie wir im Kapitel über Lineare (Un-)Abhängigkeit gelernt haben, genau dann der Fall, wenn die Spalten von A linear unabhängig sind. Es gilt also auch die Umkehrung, also $\det(A) = 0 \Leftrightarrow$ Spalten von A sind linear abhängig. Dies können wir dem Satz vom Ende von Kapitel 3.4 hinzufügen, und bekommen den Satz

Satz (Äquivalente Eigenschaften für quadratische Matrizen). Für eine lineare Abbildung $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$ und die zugehörige Matrix $A \in \mathbb{K}^{n \times n}$ gilt die Äquivalenz:

$$\begin{aligned} f \text{ injektiv} &\iff f \text{ surjektiv} \iff f \text{ bijektiv} \\ &\iff \text{Kern}(A) = \{\vec{0}\} \iff \text{Bild}(A) = \mathbb{K}^n \iff A^{-1} \text{ existiert} \\ &\iff \text{das LGS } A\vec{x} = \vec{b} \text{ ist für alle } \vec{b} \in \mathbb{K}^n \text{ eindeutig lösbar} \\ &\iff \text{die Spalten von } A \text{ sind l.u.} \iff \text{die Zeilen von } A \text{ sind l.u.} \\ &\iff \det(A) \neq 0 \iff \det(A^T) \neq 0 \end{aligned}$$

Weitere Rechenregel für Determinanten:

Satz (Determinantenproduktsatz). Für $A, B \in \mathbb{R}^{n \times n}$ gilt:⁶⁰

$$\boxed{\det(AB) = \det(A) \cdot \det(B)}$$

⁶⁰Einen Beweis kann man z.B. im Grabmüller-Skript S. 251 finden.

Es folgt sofort (durch wiederholtes Anwenden):

$$\det(A^m) = \det(A)^m$$

sowie, für invertierbares A , indem man $B := A^{-1}$ setzt:

$$\det(A) \cdot \det(A^{-1}) = \det(AA^{-1}) = \det(E_n) = 1,$$

also

$$\boxed{\det(A^{-1}) = \frac{1}{\det(A)}}.$$

Anmerkung: Für $\det(A+B)$ gibt es dagegen keine einfache Formel.

Satz. (folgt direkt aus der Multilinearität):

$$\det(\lambda A) = \lambda^n \det(A) \quad \forall \lambda \in \mathbb{R}, A \in \mathbb{R}^{n \times n}$$

Nochmal zusammengefasst die erlaubten elementaren Umformungen und wichtige Eigenschaften von Determinanten:

- Es darf ein Vielfaches einer Zeile zu einer anderen Zeile sowie ein Vielfaches einer Spalte zu einer anderen Spalte addiert werden, ohne dass sich der Wert der Determinante ändert
- Beim Vertauschen zweier Zeilen oder zweier Spalten ändert sich (nur) das Vorzeichen der Determinante
- Faktoren dürfen aus einer Zeile oder Spalte vorgezogen werden
- Die Determinante null genau dann wenn die Spalten (gleichbedeutend: die Zeilen) linear abhängig sind; insbesondere also wenn eine Nullzeile oder Nullspalte vorhanden ist, oder auch wenn zwei Spalten identisch oder zwei Zeilen identisch sind.
- Es ist $\det(A) = \det(A^T)$, $\det(E_n) = 1$, $\det(AB) = \det(A) \det(B)$, und $\det(A^m) = \det(A)^m$ für $m \in \mathbb{N}_0$ bzw., falls $\det(A) \neq 0$, für $m \in \mathbb{Z}$.

Anwendungen für Determinanten.

1. Geometrische Anwendungen: Indem wir uns erinnern, wie wir die Determinante konstruiert haben, folgt: Das Volumen eines n -dimensionalen Spats, der von den Vektoren $\vec{a}_1, \dots, \vec{a}_n \in \mathbb{R}^n$ aufgespannt wird, ist

$$V_{\text{spat}} = |\det(\vec{a}_1, \dots, \vec{a}_n)|.$$

Insbesondere, für $n=2$: Der Flächeninhalt eines Parallelogramms, das von $\vec{a}_1, \vec{a}_2 \in \mathbb{R}^2$ aufgespannt wird, ist

$$F_{\text{Parallelogramm}} = |\det(\vec{a}_1, \vec{a}_2)|.$$

[Das Vorzeichen der Determinante gibt wieder, ob es sich bei den Vektoren $\vec{a}_1, \dots, \vec{a}_n$ um ein Rechts- oder ein Linkssystem handelt: Man definiert, dass Vektoren ein Rechtssystem bilden, falls die Determinante positiv ist, und dass sie ein Linkssystem bilden, falls die Determinante negativ ist. Rechtssysteme spielen u.a. in der Physik (Elektrotechnik) eine Rolle, 'Rechte-Hand-Regel'.]

Indem man ein Parallelogramm in zwei Dreiecke zerlegt, folgt:

Der Flächeninhalt eines Dreiecks, das von $\vec{a}_1, \vec{a}_2 \in \mathbb{R}^2$ aufgespannt wird, hat den Flächeninhalt

$$F_{Dreieck} = \frac{1}{2} |\det(\vec{a}_1, \vec{a}_2)|$$

(d.h.: die Punkte $\vec{0}, \vec{a}_1, \vec{a}_2 \in \mathbb{R}^2$ sind die Eckpunkte des Dreiecks). Falls $\vec{0}$ kein Eckpunkt ist, sondern $\vec{p}_1, \vec{p}_2, \vec{p}_3$, so bekommt man durch Verschiebung (dabei bleibt der Flächeninhalt unverändert) die Ecken $\vec{0}, \vec{p}_2 - \vec{p}_1, \vec{p}_3 - \vec{p}_1$, also

$$F_{Dreieck} = \frac{1}{2} |\det(\vec{p}_2 - \vec{p}_1, \vec{p}_3 - \vec{p}_1)|.$$

Analog kann man einen Spat im \mathbb{R}^3 in 6 gleich große Tetraeder zerlegen (ein Tetraeder im \mathbb{R}^3 ist ein Gebilde mit 4 Ecken und 4 dreiecksförmigen Seitenflächen); das Volumen eines Tetraeders, das von den Vektoren $\vec{a}_1, \vec{a}_2, \vec{a}_3$ aufgespannt wird, ist somit

$$V_{Tetraeder} = \frac{1}{6} |\det(\vec{a}_1, \vec{a}_2, \vec{a}_3)|.$$

2. Die Determinante gibt an, um welchen Faktor sich Volumina von Objekten verändern, wenn man eine lineare Abbildung $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ anwendet (siehe Übung).
3. Zum Testen, ob n Vektoren im \mathbb{R}^n linear (un-)abhängig sind:

$$\{\vec{a}_1, \dots, \vec{a}_n\} \text{ im } \mathbb{R}^n \text{ linear abhängig} \iff \det(\vec{a}_1, \dots, \vec{a}_n) = 0$$

(Beachte: Anzahl der Vektoren und Dimension des Raumes müssen übereinstimmen; andernfalls, wie gehabt: Wenn Anzahl der Vektoren kleiner als Raumdimension ist, mit Gauß-Algorithmus, und dann schauen, ob jede Spalte der Stufenform eine Stufe hat. Wenn Anzahl der Vektoren größer als Raumdimension ist, sind sie grundsätzlich linear abhängig.)

4. Zur Berechnung von sog. *Eigenwerten* von Matrizen, siehe das folgende Kapitel.

Ergänzungen.

- Für den Fall $n=3$ (aber *nur* für diesen Fall!) gibt es eine Merkregel für die oben hergeleitete Formel (Leibniz-Formel für $n=3$):

$$\det(A) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} :$$

Man schreibt neben die 3×3 -Matrix nochmal die beiden ersten Spalten, also

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{array}$$

Die drei Diagonalen von links oben nach rechts unten ergeben die Produkte mit positivem Vorzeichen, und die drei Diagonalen von links unten nach rechts oben ergeben die drei Produkte mit negativem Vorzeichen. Dies ist die sog. **Sarrus-Regel**. Mit der Sarrus-Regel kann man 3×3 -Determinanten unmittelbar und effizient berechnen, ohne den Laplace'schen Entwicklungssatz oder die Gauß-Umformung auf Dreiecksform anwenden zu müssen.

Für den Fall $n=2$ hatten wir oben schon eine einfache Formel

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Ferner gilt im Trivialfall $n=1$: $\det(a_{11}) = a_{11}$.

- Man kann die Determinante auch für komplexwertige Argumente, also $\det : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}$, definieren. Alle in diesem Kapitel genannten Rechenregeln und Eigenschaften bleiben erhalten, bis auf die geometrische Deutung der Determinante als Volumen/Flächeninhalt. Insbesondere kann man also die Lineare Unabhängigkeit von n Vektoren im \mathbb{C}^n ebenfalls mittels Determinante testen.

3.6 Eigenwerte und Eigenvektoren

So wie bereits im vorangegangenen Kapitel über Determinanten geht es auch im Kapitel über Eigenwerte und Eigenvektoren ausschließlich um *quadratische* Matrizen.

Die zentralen Begriffe dieses Kapitels wollen wir nun definieren:

Def. (Eigenwert, Eigenvektor) Sei $A \in \mathbb{C}^{n \times n}$. Eine Zahl $\lambda \in \mathbb{C}$ heißt *Eigenwert*⁶¹ von A , wenn es ein $\vec{x} \in \mathbb{C}^n \setminus \{\vec{0}\}$ gibt, so dass

$$A\vec{x} = \lambda\vec{x} \quad (*)$$

gilt. Ein $\vec{x} \neq \vec{0}$, das diese Gleichung erfüllt, heißt *Eigenvektor*⁶² von A zum Eigenwert λ .⁶³

⁶¹engl.: eigenvalue

⁶²engl.: eigenvector

⁶³Bemerkung zum Raum: *Reelle* Matrizen $A \in \mathbb{R}^{n \times n}$ fassen wir wegen $\mathbb{R} \subset \mathbb{C}$ als Spezialfall komplexer Matrizen auf. Es ergibt also durchaus Sinn, auch für reelle Matrizen nach komplexen (nicht-reellen) Eigenwerten und Eigenvektoren zu suchen. Wird nach Eigenwerten/Eigenvektoren einer reellen Matrix gesucht, so sollte mit angegeben werden, ob lediglich reelle oder auch komplexe, nicht-reelle gesucht sind.

Geometrische Deutung (reeller) Eigenvektoren: Ein Eigenvektor ist dadurch gekennzeichnet, dass bei Anwendung der Matrix A (bzw. der zu A gehörenden linearen Abbildung) sich seine Richtung nicht ändert, sondern er lediglich gestreckt oder gestaucht wird. Der zu einem Eigenvektor gehörende Eigenwert λ ist gerade der Streckfaktor.

Beispiel. Eine Diagonalmatrix $A = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$ hat offensichtlich sowohl \vec{e}_1 als auch \vec{e}_2 als Eigenvektoren, denn diese beiden Vektoren werden um den Faktor a_1 bzw. a_2 gestreckt. Aber auch alle skalaren Vielfachen $\alpha \vec{e}_1$ sowie $\alpha \vec{e}_2$ ($\alpha \neq 0$) sind Eigenvektoren, denn auch sie verändern ihre Richtung nicht und werden lediglich um den Faktor a_1 bzw. a_2 gestreckt. (Alle anderen Vektoren, die nicht in Richtung einer Achse zeigen, sind jedoch i.a. keine Eigenvektoren von A , da sie ihre Richtung ändern bei Anwendung von A ; es sei denn dass $a_1 = a_2$.)

Struktur der Menge der Eigenvektoren. Welche Struktur hat, bei vorgegebenem Eigenwert λ , die Menge der Vektoren \vec{x} , für die $A\vec{x} = \lambda\vec{x}$ gilt? Es ist

$$A\vec{x} = \lambda\vec{x} \Leftrightarrow A\vec{x} - \lambda\vec{x} = \vec{0} \Leftrightarrow (A - \lambda E_n)\vec{x} = \vec{0} \Leftrightarrow \vec{x} \in \text{Kern}(A - \lambda E_n).$$

Also: λ ist Eigenwert von A , wenn das homogene LGS mit Systemmatrix $A - \lambda E_n$ nichttriviale Lösungen hat. Die Menge aller \vec{x} , die (*) erfüllen, ist die Lösungsmenge des homogenen LGS mit Systemmatrix $A - \lambda E_n$. Es folgt: Die Menge aller Lösungen von (*), für einen festen Eigenwert λ , ist ein Unterraum von \mathbb{C}^n , genannt *Eigenraum*:

Sei $\lambda \in \mathbb{C}$ ein Eigenwert der Matrix $A \in \mathbb{C}^{n \times n}$. Dann heißt der Vektorraum

$$\text{Eig}(\lambda) := \{\vec{x} \in \mathbb{C}^n \mid A\vec{x} = \lambda\vec{x}\} = \text{Kern}(A - \lambda E_n)$$

der *Eigenraum* von A zum Eigenwert λ .

Beachte den feinen Unterschied zwischen den Begriffen "Eigenvektor" und "Element des Eigenraums": Der Nullvektor wird nicht als Eigenvektor bezeichnet, obwohl er die Gleichung $A\vec{x} = \lambda\vec{x}$ erfüllt und somit im Eigenraum liegt; es ist "Eigenraum = Menge aller Eigenvektoren $\cup \{\vec{0}\}$ ".

Der Schnitt zweier verschiedener Eigenräume besteht immer nur aus dem Nullvektor:

$$\text{Eig}(\lambda_1) \cap \text{Eig}(\lambda_2) = \{\vec{0}\} \quad \text{für } \lambda_1 \neq \lambda_2$$

Grund: Sei $\vec{x} \in \text{Eig}(\lambda_1)$ und $\vec{x} \in \text{Eig}(\lambda_2)$. Dann ist $\lambda_1\vec{x} = A\vec{x} = \lambda_2\vec{x}$, also $\underbrace{(\lambda_1 - \lambda_2)}_{\neq 0} \vec{x} = \vec{0}$,

also $\vec{x} = \vec{0}$.

Berechnung von Eigenwerten und Eigenvektoren: Erster Versuch.

Im Prinzip wissen wir bereits, wie man Eigenwerte und Eigenräume berechnen kann,

denn wir haben gesehen: λ ist Eigenwert von A genau dann wenn das homogene LGS mit Systemmatrix $A - \lambda E_n$ nichttriviale Lösungen hat. Die (nichttriviale) Lösungsmenge des LGS ist der zugehörige Eigenraum. Die Frage nach Eigenwerte/Eigenräumen kann also umformuliert werden zu:

”(a) Für welche $\lambda \in \mathbb{C}$ hat das LGS $(A - \lambda E_n) \vec{x} = \vec{0}$ eine nichttriviale Lösungsmenge.
 (b) Bestimmen Sie für diese λ die Lösungsmenge.”

Beispiel:

$$A = \begin{pmatrix} 1 & 2 \\ 5 & 4 \end{pmatrix} \Rightarrow A - \lambda E_2 = \begin{pmatrix} 1-\lambda & 2 \\ 5 & 4-\lambda \end{pmatrix}$$

Indem wir auf diese Matrix Gauß-Elimination anwenden, könnten wir diese Fragen beantworten. Allerdings: Gauß-Elimination für Matrizen, die von Parametern (hier: λ) abhängen, sind unangenehm⁶⁴. Wir gehen stattdessen wie folgt vor.

3.6.1 Berechnung von Eigenwerten, Charakteristisches Polynom

Es gibt eine bessere Strategie als die oben genannte: Wir konzentrieren uns zunächst nur auf die Frage (a). Diese Frage können wir mittels Determinantenberechnung beantworten, denn:

$$\begin{aligned} (A - \lambda E_n) \vec{x} = \vec{0} \text{ hat nichttriviale Lösungen} &\iff A - \lambda E_n \text{ ist nicht invertierbar} \\ &\iff \det(A - \lambda E_n) = 0 \end{aligned}$$

Wir haben somit ein Kriterium hergeleitet, welches auch für die praktische Berechnung von Eigenwerten verwendet wird (Berechnung der Determinante über Laplace'schen Entwicklungssatz, nicht über Gauß):

$$\lambda \text{ ist Eigenwert von } A \iff \det(A - \lambda E_n) = 0$$

Im Beispiel:

$$\det(A - \lambda E_2) = (1 - \lambda)(4 - \lambda) - 10 = \lambda^2 - 5\lambda - 6$$

Dies ist genau dann null, wenn $\lambda_{1,2} = \frac{5}{2} \pm \sqrt{\frac{25}{4} + 6} = \frac{5}{2} \pm \frac{7}{2}$, also:

$\lambda_1 = 6$ und $\lambda_2 = -1$ sind die Eigenwerte von A .

Man sieht: Für beliebige $n \times n$ -Matrix A ist $\det(A - \lambda E_n)$ immer ein *polynomieller* Ausdruck in λ , denn beim Entwickeln nach Laplace werden die Matrixeinträge lediglich addiert und multipliziert.

⁶⁴Im 2×2 -Fall könnte Zeilentauschen helfen, um Division der zweiten Zeile durch $a_{11} - \lambda$ zu vermeiden; bei der Eigenwertbestimmung von größeren Matrizen, bei denen also viele Einträge vom Parameter abhängen, muss man jedoch mit vielen unangenehmen Fallunterscheidungen rechnen. Man beachte, dass bei Gaußumformungen eine etwaige *Multiplikation* von Zeilen mit λ -abhängigen Werten ebenfalls heikel ist: Dies ist i.a. keine Äquivalenzumformung, da der Faktor null sein könnte.

Def. Das Polynom

$$p(\lambda) := \det(A - \lambda E_n)$$

heißt *Charakteristisches Polynom* von A .

Die Eigenwerte einer Matrix A sind also die Nullstellen des charakteristischen Polynoms von A .

Ist A reelle Matrix, so hat das charakteristische Polynom reelle Koeffizienten. Nichtsdestotrotz kann man für ein reelles Polynom sowohl in \mathbb{R} als auch in \mathbb{C} nach Nullstellen suchen; dies entspricht der Suche nach Eigenwerten von A in \mathbb{R} bzw. in \mathbb{C} .

Satz (Eigenschaften des charakteristischen Polynoms) Sei $A \in \mathbb{C}^{n \times n}$ und p das zugehörige charakteristische Polynom. Dann gilt:

- a) Das Polynom p hat den Grad n ; wir können also schreiben

$$p(\lambda) = a_n \lambda^n + \dots + a_1 \lambda + a_0,$$

mit $a_0, \dots, a_n \in \mathbb{C}$.

Falls $A \in \mathbb{R}^{n \times n}$, so sind $a_0, \dots, a_n \in \mathbb{R}$.

- b) Der Leitkoeffizient von p ist $a_n = (-1)^n$.
- c) Da jedes Polynom über \mathbb{C} in Linearfaktoren zerfällt (Fundamentalsatz der Algebra), kann man schreiben⁶⁵

$$p(\lambda) = (\lambda_1 - \lambda) \cdot \dots \cdot (\lambda_n - \lambda),$$

wobei die $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ gerade die Nullstellen von p , also die Eigenwerte von A , sind; es gibt also höchstens n Eigenwerte von A . (Es können auch weniger sein, nämlich wenn mehrere λ_i zusammenfallen, also p mehrfache Nullstellen hat.)

- d) Jede Matrix $A \in \mathbb{C}^{n \times n}$ (also auch: $A \in \mathbb{R}^{n \times n}$) hat mindestens einen Eigenwert in \mathbb{C} . (Bem.: Mehrere λ_i können zusammenfallen.)
- e) Es ist $a_{n-1} = (-1)^{n-1} \sum_{i=1}^n a_{ii}$. Die Summe aller Diagonaleinträge einer quadratischen Matrix wird auch als *Spur* der Matrix bezeichnet:

$$\text{spur}(A) := \sum_{i=1}^n a_{ii}$$

⁶⁵Hier geht auch b) ein, denn andernfalls müsste man in der Produktdarstellung noch einen Vorfaktor einbauen.

Da nach c) offensichtlich $a_{n-1} = (-1)^{n-1} \sum_{i=1}^n \lambda_i$, folgt also

$$\sum_{i=1}^n \lambda_i = \text{spur}(A)$$

d.h. die Summe aller (komplexen) Eigenwerte, wobei mehrfache Eigenwerte entsprechend ihrer Vielfachheit mehrfach gezählt werden, ist gleich der Summe der Diagonaleinträge der Matrix, und diese wiederum ist, bis auf ein Vorzeichen $(-1)^{n-1}$, gleich dem Koeffizienten der zweithöchsten Potenz im Polynom p .

f) Das absolute Glied ist gleich dem Produkt aller Eigenwerte: $a_0 = \det(A) = \prod_{i=1}^n \lambda_i$

Beweis.

a), b), e) Anhand der Leibniz-Formel der Determinante sieht man, dass die höchste λ -Potenz, die auftritt, λ^n ist, und zwar in dem Summanden für die Permutation $\sigma = \text{id}$. Alle anderen $\sigma \in S_n$ liefern nur λ -Potenzen niedrigerer Ordnung. Der Summand für $\sigma = \text{id}$ lautet $\prod_{i=1}^n (a_{ii} - \lambda)$. Ausmultiplizieren liefert als höchste Potenz $(-\lambda)^n = (-1)^n \lambda^n$ ist, und dessen nächsthöchste Potenz $(a_{11} + \dots + a_{nn})(-\lambda)^{n-1} = \text{spur}(A)(-1)^{n-1} \lambda^{n-1}$. Alle übrigen $\sigma \in S_n \setminus \{\text{id}\}$ liefern keinen Beitrag zur Potenz λ^{n-1} , also ist $a_{n-1} = \text{spur}(A)(-1)^{n-1}$.
Die Darstellung aus c) liefert als zweithöchste λ -Potenz $(\lambda_1 + \dots + \lambda_n)(-1)^{n-1} \lambda^{n-1}$.

f) Es ist $a_0 = p(0) = \det(A)$ und nach b) $p(0) = \prod_{i=1}^n \lambda_i$.

c), d) sind klar.

Bemerkung. Der Fakt, dass die Summe der Eigenwerte gleich der Spur sein muss, (ggf. auch, dass das Produkt der Eigenwerte die Determinante ergibt), lässt sich als Kontrolle (Probe) verwenden. Im Beispiel: $\text{spur}(A) = 1 + 4 = 5$, $\lambda_1 + \lambda_2 = 6 - 1 = 5$, und $\det(A) = 4 - 10 = -6$, $\lambda_1 \cdot \lambda_2 = -6$.

3.6.2 Eigenräume, Ähnlichkeitstransformationen, Diagonalisierbarkeit

Hat man die Eigenwerte als Nullstellen λ_i des charakteristischen Polynoms berechnet, kann man anschließend die zugehörigen Eigenräume als

$$\text{Eig}(\lambda_i) = \{\vec{x} \in \mathbb{C}^n \mid (A - \lambda_i E_n) \vec{x} = \vec{0}\} = \text{Kern}(A - \lambda_i E_n)$$

berechnen. Dies erfordert nun kein umständliches Hantieren mit einer parameterbehafteten Matrix, da der konkrete Zahlenwert von λ_i bekannt ist!

Beispiel zur Berechnung von Eigenwerten und Eigenräumen einer Matrix

$$A := \begin{pmatrix} -3 & 7 & -3 \\ -4 & 7 & -2 \\ -3 & 3 & 1 \end{pmatrix}$$

hat das charakteristische Polynom

$$\begin{aligned} p(\lambda) &= \det \begin{pmatrix} -3-\lambda & 7 & -3 \\ -4 & 7-\lambda & -2 \\ -3 & 3 & 1-\lambda \end{pmatrix} \\ &\stackrel{(*)}{=} -3 \det \begin{pmatrix} 7 & -3 \\ 7-\lambda & -2 \end{pmatrix} - 3 \det \begin{pmatrix} -3-\lambda & -3 \\ -4 & -2 \end{pmatrix} + (1-\lambda) \det \begin{pmatrix} -3-\lambda & 7 \\ -4 & 7-\lambda \end{pmatrix} \\ &= -3[-14 + 3(7-\lambda)] - 3[2(3+\lambda) - 12] + (1-\lambda)[(3+\lambda)(\lambda-7) + 28] \\ &= 3\lambda - 3 + (1-\lambda)(\lambda^2 - 4\lambda + 7) = (1-\lambda)(\lambda^2 - 4\lambda + 4) = (1-\lambda)(2-\lambda)^2 \end{aligned}$$

wobei in (*) nach der letzten Zeile entwickelt wurde.⁶⁶

Es sind also $\lambda_1=1$ und $\lambda_2=2$ Eigenwerte.

Berechnung der Eigenräume:

$$\text{Eig}(\lambda_1) = \text{Kern}(A - \lambda_1 E_2):$$

$$A - \lambda_1 E_2 = \begin{pmatrix} -4 & 7 & -3 \\ -4 & 6 & -2 \\ -3 & 3 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} -4 & 7 & -3 \\ 0 & -1 & 1 \\ 0 & -\frac{9}{4} & \frac{9}{4} \end{pmatrix} \rightarrow \begin{pmatrix} -4 & 0 & 4 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\implies \text{Eig}(\lambda_1) = \text{span}\{(1, 1, 1)^T\}$$

$$\text{Eig}(\lambda_2) = \text{Kern}(A - \lambda_2 E_2):$$

$$A - \lambda_2 E_2 = \begin{pmatrix} -5 & 7 & -3 \\ -4 & 5 & -2 \\ -3 & 3 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} -5 & 7 & -3 \\ 0 & -\frac{3}{5} & \frac{2}{5} \\ 0 & -\frac{6}{5} & \frac{4}{5} \end{pmatrix} \rightarrow \begin{pmatrix} -5 & 7 & -3 \\ 0 & -3 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\implies \text{Eig}(\lambda_2) = \text{span}\{(1, 2, 3)^T\}$$

Def. (algebraische und geometrische Vielfachheit eines Eigenwertes). Die Vielfachheit der Nullstelle λ_i des charakteristischen Polynoms wird als *algebraische Vielfachheit* des Eigenwertes λ_i bezeichnet. Die Dimension des Eigenraumes $\text{Eig}(\lambda_i)$ wird als die *geometrische Vielfachheit* des Eigenwertes λ_i bezeichnet.

Aus dem Fundamentalsatz der Algebra folgt sofort, dass die Summe der algebraischen Vielfachheiten aller (komplexen) Eigenwerte einer $n \times n$ -Matrix immer genau n ist. Für die geometrischen Vielfachheiten muss dies nicht wahr sein; siehe obiges Beispiel mit

⁶⁶Beachte: Wir sind an einer *faktorierten* Form von p interessiert; falls also ein Linearfaktor, so wie hier $1-\lambda$, erkennbar wird, sollte man diesen nicht in die restlichen Terme hineinmultiplizieren!

$n=3$, wo die Summe der geometrischen Vielfachheiten nur 2 ist.

Was man jedoch zeigen kann (hier ohne Beweis):

Satz (alg. und geom. Vielfachheit). Für jeden Eigenwert einer jeden quadratischen Matrix gilt: Die geometrische Vielfachheit ist kleiner gleich der algebraischen Vielfachheit.

Eigenwerte und -räume von Diagonalmatrizen. Diagonalmatrizen haben die Besonderheit, dass man ihnen die Eigenwerte und Eigenräume ohne Rechnung

direkt ansehen kann: Ist $A = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$, so ist $p(\lambda) = \prod_{i=1}^n (a_{ii} - \lambda)$, und

so sind $\lambda_1 = a_{11}, \dots, \lambda_n = a_{nn}$ die (nicht notwendigerweise paarweise verschiedenen) Eigenwerte von A , und es ist $\text{Eig}(\lambda_i) = \text{span}\{\vec{e}_j \mid a_{jj} = \lambda_i\}$. Also z.B. die Matrix

$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}$ hat $p(\lambda) = (2-\lambda)^2(3-\lambda)(7-\lambda)$; die Eigenwerte sind 2, 3, 7, und

es ist $\text{Eig}(2) = \text{span}\{\vec{e}_1, \vec{e}_3\}$, $\text{Eig}(3) = \text{span}\{\vec{e}_2\}$, $\text{Eig}(7) = \text{span}\{\vec{e}_4\}$.

Für $n \times n$ -Diagonalmatrizen gibt es also immer eine Basis des \mathbb{C}^n aus Eigenvektoren (nämlich $\vec{e}_1, \dots, \vec{e}_n$); die Summe der Dimensionen der Eigenräume (Summe der geometrischen Vielfachheiten) ist also gerade n , und die geometrische Vielfachheit ist für alle Eigenwerte gleich der algebraischen! Für Nicht-Diagonalmatrizen ist die Situation leider unübersichtlicher: Es können geometrische und algebraische Vielfachheit voneinander abweichen, und die Summe der Dimensionen der Eigenräume kann kleiner als n sein. (siehe obiges 3×3 -Beispiel).

Wir wollen uns im folgenden davon überzeugen, dass es neben den Diagonalmatrizen glücklicherweise noch eine deutlich größere Klasse von Matrizen gibt, die die Eigenschaft hat, dass algebraische und geometrische Vielfachheiten, so wie bei den Diagonalmatrizen, immer übereinstimmen, und somit auch die Summe der Dimensionen der Eigenräume gerade n ist, es somit eine Basis des \mathbb{K}^n gibt bestehend aus Eigenvektoren: Dies sind die sogenannten *diagonalähnlichen* bzw. *diagonalisierbaren* Matrizen:

Wir definieren dazu den Begriff der *Ähnlichkeit* von Matrizen:

Def. (Ähnlichkeit, Diagonalisierbarkeit). Zwei Matrizen $A, B \in \mathbb{C}^{n \times n}$ heißen *ähnlich*, wenn es eine invertierbare Matrix $C \in \mathbb{C}^{n \times n}$ gibt, so dass

$$B = CAC^{-1}.$$

Eine Matrix, die ähnlich zu einer Diagonalmatrix ist, heißt (*diagonalähnlich* oder besser) *diagonalisierbar*.

Man kann leicht zeigen: Ähnlichkeit ist eine Äquivalenzrelation auf der Menge $\mathbb{C}^{n \times n}$ (siehe Übung).

Sind zwei Matrizen ähnlich, so haben sie diverse Gemeinsamkeiten, z.B. die gleiche Determinante:

$$\det(B) = \det(CAC^{-1}) = \det(C) \det(A) \det(C^{-1}) = \det(A)$$

Nicht nur das; sie haben sogar das gleiche charakteristische Polynom:

$$\begin{aligned} p_B(\lambda) &= \det(B - \lambda E_n) = \det(CAC^{-1} - \lambda E_n) = \det(CAC^{-1} - \lambda E_n C C^{-1}) \\ &= \det(CAC^{-1} - C(\lambda E_n)C^{-1}) = \det(C(A - \lambda E_n)C^{-1}) \\ &= \det(C) \det(A - \lambda E_n) \det(C^{-1}) = p_A(\lambda) \end{aligned}$$

Es folgt sofort, dass ähnliche Matrizen die gleichen Eigenwerte haben, sowie auch die gleiche Spur:

Satz (ähnliche Matrizen). Sind zwei Matrizen ähnlich, so haben sie das gleiche charakteristische Polynom, und somit insbesondere die gleiche Determinante, die gleiche Spur und die gleichen Eigenwerte.

Die Eigenräume zweier ähnlicher Matrizen stimmen jedoch i.a. nicht überein. Wir wollen uns zumindest im Fall der Ähnlichkeit zu einer Diagonalmatrix (also der Diagonalisierbarkeit) anschauen, wie sich die Eigenräume zueinander verhalten:

Satz (Diagonalisierbarkeit). Sei $L = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \in \mathbb{C}^{n \times n}$ eine Diagonalmatrix,

sei $X \in \mathbb{C}^{n \times n}$ invertierbar, und sei $A = X L X^{-1}$ (A also diagonalisierbar). Dann sind $\lambda_1, \dots, \lambda_n$ gerade die Eigenwerte von A , und die Spalten der Matrix X sind Eigenvektoren von A (genauer: die i -te Spalte von X ist EV zu λ_i). Da die Spalten von X wegen der Invertierbarkeit linear unabhängig sind, gibt es also eine Basis des \mathbb{C}^n aus Eigenvektoren von A , d.h. die geometrischen Vielfachheiten der Eigenwerte von A addieren sich zu n auf.

Umgekehrt: Gibt es zu einer Matrix A eine Basis des \mathbb{C}^n bestehend aus Eigenvektoren, so ist A diagonalisierbar: Man bildet die Diagonalmatrix L aus den Eigenwerten von A und X aus den Eigenvektoren derart, dass die i -te Spalte von X als EV zum i -ten Diagonaleintrag von L gewählt wird.

Beweis. Wir multiplizieren $A = X L X^{-1}$ mit X von rechts und bekommen

$$AX = XL.$$

Dabei ist

$$XL = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & \dots & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \begin{pmatrix} \lambda_1 x_{11} & \dots & \lambda_n x_{1n} \\ \vdots & & \vdots \\ \lambda_1 x_{n1} & \dots & \lambda_n x_{nn} \end{pmatrix} = [\lambda_1 \vec{x}_1, \dots, \lambda_n \vec{x}_n]$$

und

$$AX = [A\vec{x}_1, \dots, A\vec{x}_n].$$

Es folgt $A\vec{x}_i = \lambda_i\vec{x}_i$, d.h. die λ_i sind Eigenwerte von A und die \vec{x}_i die zugehörigen Eigenvektoren. Die geometrische Vielfachheit eines Eigenwertes λ_i von A ist gerade die Häufigkeit, mit der λ_i in L vorkommt.

Beispiel.

Im Beispiel der 2×2 -Matrix von S. 101 hatten wir die EW $\lambda_1 = 6$ und $\lambda_2 = -1$ berechnet. Wir berechnen noch die zugehörigen Eigenräume:

$$A - \lambda_1 E_2 = \begin{pmatrix} -5 & 2 \\ 5 & -2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -\frac{2}{5} \\ 0 & 0 \end{pmatrix} \Rightarrow \text{Eig}(\lambda_1) = \text{span} \left\{ \begin{pmatrix} -\frac{2}{5} \\ -1 \end{pmatrix} \right\} = \text{span} \left\{ \begin{pmatrix} 2 \\ 5 \end{pmatrix} \right\}$$

$$A - \lambda_2 E_2 = \begin{pmatrix} 2 & 2 \\ 5 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow \text{Eig}(\lambda_2) = \text{span} \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

Nach dem Satz ist also $A = X LX^{-1}$ mit $L = \begin{pmatrix} 6 & 0 \\ 0 & -1 \end{pmatrix}$, $X = \begin{pmatrix} 2 & 1 \\ 5 & -1 \end{pmatrix}$.

Kontrolle:

Es ist $X^{-1} = \frac{1}{-7} \begin{pmatrix} -1 & -1 \\ -5 & 2 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 1 & 1 \\ 5 & -2 \end{pmatrix}$, und

$$\begin{aligned} \frac{1}{7} \begin{pmatrix} 2 & 1 \\ 5 & -1 \end{pmatrix} \begin{pmatrix} 6 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 5 & -2 \end{pmatrix} &= \frac{1}{7} \begin{pmatrix} 12 & -1 \\ 30 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 5 & -2 \end{pmatrix} \\ &= \frac{1}{7} \begin{pmatrix} 7 & 14 \\ 35 & 28 \end{pmatrix} = A \end{aligned}$$

Wir fassen zusammen: Eine Matrix $A \in \mathbb{C}^{n \times n}$ ist dann und nur dann diagonalisierbar, wenn sie Eigenvektoren hat, die eine Basis des \mathbb{C}^n bilden, sich also die geometrischen Vielfachheiten der Eigenwerte zu n addieren. Es gilt dann $A = X LX^{-1}$, wobei L Diagonalmatrix ist, bestehend aus den Eigenwerten von A , und die Spalten von X sind Eigenvektoren von A .

– Die Darstellung von A als $A = X LX^{-1}$ ist nicht eindeutig; so kann man z.B. die Reihenfolge der Diagonaleinträge von L variieren, sofern man die Spalten von X ebenfalls entsprechend tauscht, oder man kann Spalten von X mit Vielfachen $\neq 0$ multiplizieren (da eine Skalarmultiplikation die Eigenschaft, EV zu sein, nicht tangiert).

– Wir werden im nächsten Kapitel sehen, dass alle symmetrischen reellen Matrizen (für die also $A = A^T$ gilt), diagonalisierbar sind.

– Versuch einer geometrischen Deutung der Diagonalisierung einer Matrix $A = X LX^{-1}$ (nur im Fall, dass alle Eigenwerte/Eigenräume reell sind): A hat (reelle) Eigenwerte λ_i und zugehörige EV \vec{x}_i ; das bedeutet, dass unter Anwendung von A die \vec{x}_i um den Faktor λ_i gestreckt werden sollen. Die Diagonalmatrix L hat die gleichen EW wie A (ähnliche Matrizen haben gleiche EW), jedoch streckt eine Diagonalmatrix genau die Achsen des Koordinatensystems (die Standardbasisvektoren \vec{e}_i) um

den Faktor λ_i ; siehe Bsp. auf S. 100. Die zur Matrix X gehörende lineare Abbildung bildet offenbar Standardbasisvektoren auf die Spalten von X , also auf die Eigenvektoren von A , ab. X^{-1} stellt die Umkehrung, also die Abbildung der Eigenvektoren von A auf die Standardbasisvektoren, dar.

Die Darstellung $A = X L X^{-1}$ bedeutet: Die Anwendung von A kann man zerlegen in die Hintereinanderschaltung von drei linearen Abbildungen, und zwar zunächst einer Abbildung X^{-1} , die die 'Streckrichtungen' von A abbildet auf die Standardbasisvektoren, anschließend einer Streckung der Standardbasisvektoren um die Faktoren λ_i , und anschließend einer Abbildung X , die die Standardbasisvektoren auf die Eigenvektoren von A abbildet.

– Ausblick/Anwendung von EW/EV/Diagonalisierung (3. Semester): Viele Naturvorgänge lassen sich durch Systeme von sog. Differentialgleichungen beschreiben: Lineare Differentialgleichungssysteme haben die Form $\frac{d}{dt}\vec{x}(t) = A\vec{x}(t) + \vec{b}$; dabei sind A und \vec{b} gegeben, und die Funktion $\vec{x}(t)$ ist gesucht; t ist meist die Zeit. Das Lösen solcher Systeme erfordert, die Eigenwerte/Eigenvektoren von A zu berechnen; falls A diagonalisierbar ist, kann man die Lösungen einigermaßen leicht bestimmen, andernfalls ist das mühsamer.

3.7 Das Skalarprodukt und Anwendungen

In diesem Kapitel geht es um Orthogonalität von Vektoren sowie um die Messung der Länge von Vektoren (somit auch der Messung des Abstandes von Punkten).

Def. (Euklidisches Skalarprodukt). Im \mathbb{R} -Vektorraum \mathbb{R}^n bezeichnet man die Abbildung $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ definiert durch

$$\langle \vec{x}, \vec{y} \rangle := \sum_{i=1}^n x_i y_i = \vec{x}^T \vec{y}$$

als das *Euklidische Skalarprodukt*. Im \mathbb{C} -Vektorraum \mathbb{C}^n bezeichnet man die Abbildung $\langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$ definiert durch

$$\langle \vec{x}, \vec{y} \rangle := \sum_{i=1}^n x_i \bar{y}_i = \vec{x}^T \vec{\bar{y}}$$

als das *Euklidische Skalarprodukt*.

Das reelle Euklidische Skalarprodukt ist also nichts anderes als das komplexe, eingeschränkt auf $\mathbb{R}^n \subset \mathbb{C}^n$.

Wichtige Eigenschaften des Euklidischen Skalarprodukts:

(folgen unmittelbar aus der Definition)

S1: $\langle \vec{x}, \vec{x} \rangle \geq 0 \quad \forall \vec{x} \in \mathbb{R}^n$ ⁶⁷

S2: $\langle \vec{x}, \vec{x} \rangle = 0 \Leftrightarrow \vec{x} = \vec{0}$

⁶⁷Insbesondere also ist $\langle \vec{x}, \vec{x} \rangle \in \mathbb{R}$, damit das " ≥ 0 " überhaupt Sinn macht. Man vereinbart nämlich für komplexe Zahlen z : Für " $z \in \mathbb{R}$ und $z \geq 0$ " schreiben wir kurz " $z \geq 0$ ".

$$\text{S3: } \langle \vec{x}, \vec{y} \rangle = \overline{\langle \vec{y}, \vec{x} \rangle} \quad \forall \vec{x} \in \mathbb{K}^n \text{ }^{68}$$

$$\text{S4: } \langle \alpha \vec{x}, \vec{y} \rangle = \alpha \langle \vec{x}, \vec{y} \rangle \quad \forall \alpha \in \mathbb{K}, \vec{x}, \vec{y} \in \mathbb{K}^n$$

$$\text{S5: } \langle \vec{x} + \vec{y}, \vec{z} \rangle = \langle \vec{x}, \vec{z} \rangle + \langle \vec{y}, \vec{z} \rangle \quad \forall \vec{x}, \vec{y}, \vec{z} \in \mathbb{K}^n$$

Der Begriff des Skalarproduktes lässt sich auf beliebige Vektorräume verallgemeinern: Ist V ein \mathbb{K} -Vektorraum, so nennt man jede Abbildung $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{K}$, die die obigen Eigenschaften S1-S5 erfüllt (dabei " \mathbb{K}^n " immer durch " V " ersetzt), ein *Skalarprodukt* auf V .

Auf \mathbb{K}^n ist das Euklidische Skalarprodukt somit nicht das einzige; z.B. auch $\langle \vec{x}, \vec{y} \rangle := \sum_{i=1}^n \alpha_i x_i \bar{y}_i$, wobei die α_i feste, positive Zahlen sind, ist ein Skalarprodukt. Was unendlichdimensionale Vektorräume (Funktionsräume) angeht, so kann man auf dem Vektorraum $V = \{f : [a, b] \rightarrow \mathbb{R} \mid \int_a^b f^2(x) dx < \infty\}$ (oder auch auf $V = \{f : [a, b] \rightarrow \mathbb{R} \mid f \text{ ist stetig}\}$) mittels $\langle f, g \rangle := \int_a^b f(x) g(x) dx$ ein Skalarprodukt definieren; Die Summe über alle Komponenten im endlichdimensionalen Fall wird also ersetzt durch das Integral im unendlichdimensionalen Fall.

Schreibweisen: Neben $\langle \vec{x}, \vec{y} \rangle$ sind auch die Schreibweisen (\vec{x}, \vec{y}) sowie $\vec{x} \bullet \vec{y}$ gebräuchlich.

Eigenschaften S4 und S5 bedeuten, dass das Skalarprodukt *linear* in ersten Argument ist. Auf reellen Vektorräumen kann man auch sofort die Linearität im 2. Argument folgern; im komplexen Fall jedoch darf ein Konjugiert-Komplex-Zeichen nicht vergessen werden:

$$\langle \vec{x}, \alpha \vec{y} \rangle = \overline{\langle \alpha \vec{y}, \vec{x} \rangle} = \overline{\alpha \langle \vec{y}, \vec{x} \rangle} = \bar{\alpha} \overline{\langle \vec{y}, \vec{x} \rangle} = \bar{\alpha} \langle \vec{x}, \vec{y} \rangle$$

Analog kann man mit S5 und S3 auch zeigen, dass die Eigenschaft S5 auch fürs zweite Argument gilt:

$$\langle \vec{x}, \vec{y} + \vec{z} \rangle = \overline{\langle \vec{y} + \vec{z}, \vec{x} \rangle} = \overline{\langle \vec{y}, \vec{x} \rangle + \langle \vec{z}, \vec{x} \rangle} = \overline{\langle \vec{y}, \vec{x} \rangle} + \overline{\langle \vec{z}, \vec{x} \rangle} = \langle \vec{x}, \vec{y} \rangle + \langle \vec{x}, \vec{z} \rangle$$

Def. (Orthogonalität). Vektoren \vec{x}, \vec{y} heißen *orthogonal* (bezüglich des Skalarproduktes $\langle \cdot, \cdot \rangle$), wenn

$$\langle \vec{x}, \vec{y} \rangle = 0.$$

Veranschaulichung im Fall $n = 2$: Sei $\vec{x} = (x_1, x_2)^T$ ein beliebiger Vektor. Geometrisch kann man sich überlegen, dass dann der Vektor $\vec{y} := (-x_2, x_1)^T$ senkrecht zu \vec{x} steht, und in der Tat ist (wenn $\langle \cdot, \cdot \rangle$ das Euklidische Skalarprodukt bezeichnet) $\langle \vec{x}, \vec{y} \rangle = x_1(-x_2) + x_2 x_1 = 0$, also \vec{x} und \vec{y} orthogonal.

Zum Nullvektor ist jeder Vektor orthogonal (bzgl. beliebigem Skalarprodukt):

$$\langle \vec{0}, \vec{x} \rangle = \langle 0 \cdot \vec{0}, \vec{x} \rangle = 0 \cdot \langle \vec{0}, \vec{x} \rangle = 0$$

⁶⁸Im reellen Fall kann man den Konjugiert-Komplex-Strich natürlich weglassen.

Satz (Matrizen im Euklidischen Skalarprodukt). Ist $A \in \mathbb{C}^{n \times n}$, so ist

$$\langle \vec{x}, A\vec{y} \rangle = \langle \overline{A}^T \vec{x}, \vec{y} \rangle;$$

im Fall $A \in \mathbb{R}^{n \times n}$ also

$$\langle \vec{x}, A\vec{y} \rangle = \langle A^T \vec{x}, \vec{y} \rangle.$$

Beweis. $\langle \vec{x}, A\vec{y} \rangle = \vec{x}^T \overline{A\vec{y}} = (\vec{x}^T \overline{A}) \vec{y} = (\overline{A}^T \vec{x})^T \vec{y} = \langle \overline{A}^T \vec{x}, \vec{y} \rangle$

Längenmessung, Normen. Bei der Längenmessung von Vektoren geht es darum, jedem Vektor $\vec{x} \in V$ eine 'Länge' $\|\vec{x}\| \in \mathbb{R}_0^+$ zuzuordnen; eine Abbildung $\|\cdot\| : V \rightarrow \mathbb{R}_0^+$, die so etwas leistet, nennt man *Norm*. Möchte man für $V = \mathbb{K}^n$ den anschaulichen Längenbegriff haben, so wählt man die Norm

$$\|\vec{x}\| := \sqrt{|x_1|^2 + \dots + |x_n|^2}$$

zur Längenmessung.⁶⁹ Dies ist die sogenannte *Euklidische Norm* im \mathbb{R}^n bzw. im \mathbb{C}^n . Die Euklidische Norm hat folgende Eigenschaften:

N1: $\|\vec{x}\| \geq 0 \quad \forall \vec{x} \in \mathbb{K}^n$

N2: $\|\vec{x}\| = 0 \Leftrightarrow \vec{x} = \vec{0}$

N3: $\|\alpha \vec{x}\| = |\alpha| \|\vec{x}\| \quad \forall \vec{x} \in \mathbb{K}^n$

N4: $\|\vec{x} + \vec{y}\| \leq \|\vec{x}\| + \|\vec{y}\| \quad \forall \vec{x}, \vec{y} \in \mathbb{K}^n$ (Dreiecksungleichung)

Eigenschaften N1 und N2 sind unmittelbar klar; auch N3 ist elementar, nur N4 ist nicht so trivial; der Beweis wird nachgeliefert.

Man sieht, dass folgender Zusammenhang zwischen Euklidischer Norm und Euklidischem Skalarprodukt gilt:

$$\boxed{\|\vec{x}\| = \sqrt{\langle \vec{x}, \vec{x} \rangle}}$$

Wenn man nun, statt des Euklidischen, ein *beliebiges* Skalarprodukt in einem Vektorraum V nimmt, so kann man mittels $\|\vec{x}\| := \sqrt{\langle \vec{x}, \vec{x} \rangle}$ ebenfalls eine Längenmessung bekommen, die ebenfalls obige Eigenschaften N1-N4 erfüllt: Dass die Eigenschaften N1-N4 erfüllt sind, folgert man aus den Eigenschaften S1-S5 des Skalarprodukts, so ist z.B. N1-N2 eine unmittelbare Folge von S1-S2, nur N4 ist nicht ganz trivial, s.u.. Man sagt: $\|\vec{x}\| := \sqrt{\langle \vec{x}, \vec{x} \rangle}$ ist die vom Skalarprodukt $\langle \cdot, \cdot \rangle$ erzeugte Norm.

⁶⁹Im Fall $\mathbb{K} = \mathbb{R}$ kann man hier wieder die Betragsstriche weglassen. Die Längenmessung mit der Euklidischen Norm im Fall $n=2$ entspricht dem Satz des Pythagoras im rechtwinkligen Dreieck mit den Ecken $(0,0)^T$, $(x_1,0)^T$, $(x_1,x_2)^T$: Die Länge der Verbindungslinie der Punkte $(0,0)^T$ und $(x_1,x_2)^T$ ist die Wurzel aus der Summe der Quadrate der Längen der Verbindungslinien zwischen $(0,0)^T$ und $(x_1,0)^T$ sowie $(x_1,0)^T$ und $(x_1,x_2)^T$ (Skizze).

Man legt fest:

Def. (Norm). Ist V ein \mathbb{K} -Vektorraum, so heißt jede Abbildung $\|\cdot\| : V \rightarrow \mathbb{R}$, die obige Eigenschaften N1-N4 erfüllt (dabei ' \mathbb{K}^n ' immer durch ' V ' ersetzt),⁷⁰ Norm auf dem Vektorraum V . $(V, \|\cdot\|)$ heißt *normierter Vektorraum*.

Dabei ist zu beachten, dass nicht alle Normen mittels $\|\vec{x}\| = \sqrt{\langle \vec{x}, \vec{x} \rangle}$ aus einem Skalarprodukt hervorgehen müssen.

Beispiele für Normen im \mathbb{K}^n (also Abbildungen $\|\cdot\| : \mathbb{K}^n \rightarrow \mathbb{R}$, die die obigen Eigenschaften N1-N4 haben), die nicht aus einem Skalarprodukt konstruiert werden können, sind $\|\vec{x}\|_1 := |x_1| + \dots + |x_n|$ und $\|\vec{x}\|_\infty := \max\{|x_1|, \dots, |x_n|\}$. Verwendet man mehrere Normen nebeneinander, so kennzeichnet man die Euklidische Norm oft mit einem Index '2': $\|\cdot\|_2$.

Ein Beispiel für eine Norm, die aus einem Skalarprodukt hervorgeht, und zwar aus dem Skalarprodukt $\langle f, g \rangle = \int_a^b f(x)g(x) dx$ im Vektorraum V auf S. 109, ist die Norm $\|f\| = \sqrt{\langle f, f \rangle} = (\int_a^b f(x)^2 dx)^{\frac{1}{2}}$.

Für das Euklidische Skalarprodukt und die von ihm erzeugte Euklidische Norm gilt folgender wichtiger Zusammenhang:

Satz (Cauchy-Schwarz'sche Ungleichung).⁷¹ Für das Euklidische Skalarprodukt und die von ihm erzeugte Euklidische Norm gilt

$$|\langle \vec{x}, \vec{y} \rangle| \leq \|\vec{x}\| \|\vec{y}\|$$

also

$$\left| \sum_{i=1}^n x_i \bar{y}_i \right| \leq \sqrt{\sum_{i=1}^n |x_i|^2} \sqrt{\sum_{i=1}^n |y_i|^2}$$

für alle $\vec{x}, \vec{y} \in \mathbb{K}^n$.

Im reellen Fall können natürlich wieder alle Konjugiert-Komplex-Striche sowie die Betragsstriche in den Quadraten weggelassen werden:

$$\boxed{\langle \vec{x}, \vec{y} \rangle \leq |\langle \vec{x}, \vec{y} \rangle| \leq \|\vec{x}\| \|\vec{y}\|}$$

also

$$\sum_{i=1}^n x_i y_i \leq \sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n y_i^2}$$

Beweis. Es wird bewiesen, dass $|\langle \vec{x}, \vec{y} \rangle|^2 \leq \|\vec{x}\|^2 \|\vec{y}\|^2$, woraus die Behauptung unmittelbar folgt. Wir wollen uns hier der Einfachheit halber auf den reellen Fall

⁷⁰Beachte: Selbst auf \mathbb{C} -Vektorräumen ist die Norm eines Vektors immer reell, anders als das Skalarprodukt.

⁷¹Augustin Louis Cauchy, 1789-1857, einer der wichtigsten Väter der modernen Analysis, siehe auch 2. Semester;

Hermann Amandus Schwarz, 1843-1921

beschränken:

Zunächst im Fall $n=1$ ist $|\langle \vec{x}, \vec{y} \rangle|^2 = |x_1 y_1|^2 = |x_1|^2 |y_1|^2 = \|\vec{x}\|^2 \|\vec{y}\|^2$; die Ungleichung ist sogar mit Gleichheit erfüllt.

Im Fall $n=2$: Es ist zu zeigen, dass $(x_1 y_1 + x_2 y_2)^2 \leq (x_1^2 + x_2^2)(y_1^2 + y_2^2)$.

Mittels Ausmultiplizieren ist dies äquivalent zu

$$x_1^2 y_1^2 + x_2^2 y_2^2 + 2x_1 y_1 x_2 y_2 \leq x_1^2 y_1^2 + x_2^2 y_2^2 + x_1^2 y_2^2 + x_2^2 y_1^2, \text{ also}$$

$$2x_1 y_1 x_2 y_2 \leq x_1^2 y_2^2 + x_2^2 y_1^2. \text{ Dies wiederum ist äquivalent zu}$$

$$0 \leq (x_1 y_2)^2 + (x_2 y_1)^2 - 2x_1 y_2 x_2 y_1. \text{ Die rechte Seite kann als Quadrat } (x_1 y_2 - x_2 y_1)^2 \text{ geschrieben werden, d.h. die Ungleichung ist erfüllt.}$$

Der allgemeine Fall $n \in \mathbb{N}$ folgt per Vollständiger Induktion (siehe Übung).⁷²

Die Anwendungen der Cauchy-Schwarz'schen Ungleichung sind vielfältig; eine ist: Aus der Ungleichung folgt, dass für alle $\vec{x}, \vec{y} \in \mathbb{R}^n$ der Quotient

$$\frac{\langle \vec{x}, \vec{y} \rangle}{\|\vec{x}\| \|\vec{y}\|} \in [-1, 1]$$

liegt. Man kann daher mittels

$$\text{Winkel}(\vec{x}, \vec{y}) := \arccos\left(\frac{\langle \vec{x}, \vec{y} \rangle}{\|\vec{x}\| \|\vec{y}\|}\right) \in [0, \pi]$$

den Winkel zwischen zwei Vektoren im \mathbb{R}^n erklären (ist vermutlich aus der Schule für den \mathbb{R}^3 oder \mathbb{R}^2 bekannt); \arccos ist die Umkehrfunktion von $\cos : [0, \pi] \rightarrow [-1, 1]$.

Ferner kann man mit der Cauchy-Schwarz'schen Ungleichung die Dreiecksungleichung $\|\vec{x} + \vec{y}\| \leq \|\vec{x}\| + \|\vec{y}\|$ beweisen; der Beweis orientiert sich an dem Beweis der Dreiecksungleichung für komplexe Zahlen, siehe S. 42:

$$\begin{aligned} \|\vec{x} + \vec{y}\|^2 &= \langle \vec{x} + \vec{y}, \vec{x} + \vec{y} \rangle = \langle \vec{x}, \vec{x} \rangle + \langle \vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{x} \rangle + \langle \vec{y}, \vec{y} \rangle \\ &= \|\vec{x}\|^2 + \|\vec{y}\|^2 + \underbrace{\langle \vec{x}, \vec{y} \rangle + \overline{\langle \vec{x}, \vec{y} \rangle}}_{=2\operatorname{Re}(\langle \vec{x}, \vec{y} \rangle) \leq 2|\langle \vec{x}, \vec{y} \rangle|} \\ &\leq \|\vec{x}\|^2 + \|\vec{y}\|^2 + 2|\langle \vec{x}, \vec{y} \rangle| \\ &\leq \|\vec{x}\|^2 + \|\vec{y}\|^2 + 2\|\vec{x}\| \|\vec{y}\| = (\|\vec{x}\| + \|\vec{y}\|)^2 \end{aligned}$$

wobei im vorletzten Schritt die Cauchy-Schwarz'sche Ungleichung verwendet wurde. Die Behauptung folgt durch Wurzelziehen.

3.7.1 Hyperebenen

Eine Anwendung des Skalarproduktes besteht in der Darstellung von (Hyper)-ebenen:

⁷²Dieser Beweis ist ein Beispiel für eine Induktion, bei der der Induktionsanfang bei $n=2$ gemacht werden muss, damit der Induktionsschritt funktioniert; vgl. die Übungsaufgabe 'alle Schafe haben die gleiche Farbe'.

Def. (Hyperebene). Ein $n-1$ -dimensionaler affiner Unterraum eines n -dimensionalen Vektorraums heißt *Hyperebene*.

Eine Hyperebene E im \mathbb{R}^n kann also dargestellt werden als

$$E = \{\vec{x}_0\} + \text{span}\{\vec{x}_1, \dots, \vec{x}_{n-1}\} = \left\{ \vec{x}_0 + \sum_{i=1}^n \alpha_i \vec{x}_i \mid \alpha_1, \dots, \alpha_{n-1} \in \mathbb{R} \right\},$$

wobei $\vec{x}_1, \dots, \vec{x}_{n-1}$ linear unabhängig sind.

Die Vektoren $\vec{x}_1, \dots, \vec{x}_{n-1}$ sind also die aufspannenden Vektoren der Hyperebene, und \vec{x}_0 ist ein Punkt der Hyperebene. Im Fall $n=3$ ist eine Hyperebene also nichts anderes als eine Ebene, im Fall $n=2$ ist eine Hyperebene eine Gerade.

Es ist jedoch gar nicht nötig, so viele Daten anzugeben, um eine einzige Hyperebene festzulegen: Es reicht, neben einem in der Hyperebene liegenden Vektor \vec{x}_0 lediglich einen einzigen, auf der Ebene senkrecht stehenden Vektor, einen sogenannten *Normalenvektor* $\vec{n} \neq \vec{0}$, anzugeben, anstelle der $n-1$ aufspannenden Vektoren: Eine Hyperebene besteht genau aus denjenigen Punkten \vec{x} , für die der Differenzvektor $\vec{x} - \vec{x}_0$ senkrecht zu \vec{n} steht:

$$E = \{ \vec{x} \in \mathbb{K}^n \mid \langle \vec{x} - \vec{x}_0, \vec{n} \rangle = 0 \}$$

Diese Darstellungsform für Hyperebenen wird auch *Normalenform* genannt, die Darstellung mittels aufspannender Vektoren wird auch *Parameterform* genannt. In der Normalenform *kann* man verlangen, dass der Normalenvektor 'normiert' ist, d.h. die Länge 1 hat. Das erreicht man durch setzen von

$$\vec{n}_0 := \frac{\vec{n}}{\|\vec{n}\|},$$

denn dann ist $\|\vec{n}_0\| = \left\| \frac{\vec{n}}{\|\vec{n}\|} \right\| = \frac{1}{\|\vec{n}\|} \cdot \|\vec{n}\| = 1$. Man bezeichnet \vec{n}_0 als *Normaleneinheitsvektor*. Für eine vorgegebene Hyperebene gibt es genau zwei Normaleneinheitsvektoren, aber unendlich viele Normalenvektoren (die alle einem eindimensionalen Unterraum des \mathbb{R}^n angehören).

Beispiel für die Umrechnung zwischen Normalen- und Parameterform:

Sei

$$E = \left\{ \begin{pmatrix} 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} \right\} + \text{span} \left\{ \begin{pmatrix} 1 \\ 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 2 \end{pmatrix} \right\}.$$

Wie findet man einen Normalenvektor \vec{n} , also einen Vektor, der orthogonal zu den obigen Vektoren $\vec{x}_1, \vec{x}_2, \vec{x}_3$ ist? \vec{n} soll die Bedingungen $\vec{x}_1^T \vec{n} = 0, \dots, \vec{x}_3^T \vec{n} = 0$ erfüllen. Wir können diese 3 Gleichungen zusammenfassen zu einem (homogenen) LGS, bei

dem die Zeilen der Systemmatrix gerade die Vektoren \vec{x}_i^T sind:

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Mit Gauß-Elimination:

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

$$\implies \vec{n} \in \text{span} \left\{ \begin{pmatrix} 4 \\ -2 \\ 1 \\ -1 \end{pmatrix} \right\}$$

also z.B. $\vec{n} := (4, -2, 1, -1)^T$ (oder auch $\vec{n}_0 = \frac{1}{\sqrt{22}} \vec{n}$). Eine Normalenform von E lautet also

$$\left\langle \vec{x} - \begin{pmatrix} 2 \\ 3 \\ 4 \\ 5 \end{pmatrix}, \begin{pmatrix} 4 \\ -2 \\ 1 \\ -1 \end{pmatrix} \right\rangle = 0.$$

Das kann man schreiben als

$$\left\langle \vec{x}, \begin{pmatrix} 4 \\ -2 \\ 1 \\ -1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 2 \\ 3 \\ 4 \\ 5 \end{pmatrix}, \begin{pmatrix} 4 \\ -2 \\ 1 \\ -1 \end{pmatrix} \right\rangle = 1$$

also

$$4x_1 - 2x_2 + x_3 - x_4 = 1$$

Dies ist die sogenannte *Koordinatenform* der Ebene E .

Und in umgekehrter Richtung: Ist die Koordinatenform (oder die Normalenform) gegeben, so kann man sich n Vektoren $\vec{x}_i \in E$ leicht verschaffen, indem man alle bis auf eine Komponente von \vec{x}_i frei wählt (z.B. = 0) und die letzte aus der Koordinatenform berechnet, also z.B. $\vec{x}_0 = (0, 0, 0, -1)^T \in E$, $\vec{x}_1 = (0, 0, 1, 0)^T$, $\vec{x}_2 = (0, -\frac{1}{2}, 0, 0)^T$, $\vec{x}_3 = (\frac{1}{4}, 0, 0, 0)^T$, und sich durch Differenzbildung $n-1$ aufspannende Vektoren verschafft, z.B. $\vec{x}_1 - \vec{x}_0 = (0, 0, 1, 1)^T$, $\vec{x}_2 - \vec{x}_0 = (0, -\frac{1}{2}, 0, 1)^T$, $\vec{x}_3 - \vec{x}_0 = (\frac{1}{4}, 0, 0, 1)^T$, somit

$$E = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix} \right\} + \text{span} \left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -\frac{1}{2} \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{4} \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Vektorprodukt ('Kreuzprodukt'). Im Fall $n = 3$ kann man die Konstruktion eines Vektors $\vec{n} \in \mathbb{R}^3$, der orthogonal auf zwei linear unabhängigen Vektoren $\vec{x} = (x_1, x_2, x_3)^T, \vec{y} = (y_1, y_2, y_3)^T$ stehen soll, explizit bestimmen: Die Lösungsmenge des zugehörigen LGS

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

ist der von dem Vektor $\vec{n} = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)^T$ aufgespannte (eindimensionale) Raum (siehe Übung).

Dies motiviert die folgende Definition:

Für alle Vektoren $\vec{x}, \vec{y} \in \mathbb{R}^3$ heißt der Vektor

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} := \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix}$$

Vektorprodukt oder *Kreuzprodukt* (oder *äußeres Produkt*) von \vec{x} und \vec{y} .

Nach Konstruktion ist also $\vec{x} \times \vec{y}$ ein auf \vec{x} und \vec{y} orthogonal stehender Vektor, also $\langle \vec{x}, \vec{x} \times \vec{y} \rangle = 0, \langle \vec{y}, \vec{x} \times \vec{y} \rangle = 0$. Ferner ist, was unmittelbar aus der Definition folgt, $\vec{y} \times \vec{x} = -\vec{x} \times \vec{y}$, und $(\alpha\vec{x}) \times \vec{y} = \alpha(\vec{x} \times \vec{y}), \vec{x} \times (\alpha\vec{y}) = \alpha(\vec{x} \times \vec{y})$, sowie $\vec{x} \times \vec{x} = \vec{0}$, also auch $\vec{x} \times (\alpha\vec{x}) = \alpha(\vec{x} \times \vec{x}) = \vec{0}$, d.h. das Kreuzprodukt von zwei linear abhängigen Vektoren (der eine lässt sich als α -faches des anderen darstellen) ist immer null.

Beachte: Das Vektorprodukt ist nicht allgemein im \mathbb{R}^n , sondern nur im \mathbb{R}^3 definiert (denn für größere n wäre die Lösung des LGS extrem kompliziert allgemein aufzuschreiben). Für $n > 3$ konstruiert man also einen Normalenvektor, so wie oben geschehen, durch Lösen eines homogenen LGS.

3.7.2 Symmetrische Matrizen, Orthogonalmatrizen

Def. (Orthogonalsystem, Orthonormalsystem). Vektoren $\vec{x}_1, \dots, \vec{x}_m \in \mathbb{K}^n$ bilden ein *Orthogonalsystem* wenn

$$\langle \vec{x}_i, \vec{x}_j \rangle = \begin{cases} = 0 & , \text{ falls } i \neq j \\ \neq 0 & , \text{ falls } i = j \end{cases}$$

wenn also die Vektoren paarweise orthogonal sind (und keines der \vec{x}_i der Nullvektor ist).

Vektoren $\vec{x}_1, \dots, \vec{x}_m \in \mathbb{K}^n$ bilden ein *Orthonormalsystem* wenn

$$\langle \vec{x}_i, \vec{x}_j \rangle = \begin{cases} = 0 & , \text{ falls } i \neq j \\ = 1 & , \text{ falls } i = j \end{cases}$$

gilt, wenn also die Vektoren paarweise orthogonal sind und alle die Länge eins haben.

Aus einem Orthogonalsystem kann man also leicht ein Orthonormalsystem machen, indem man jeden Vektor durch seine Norm teilt.

Man kann leicht zeigen (s. Übung): Die Vektoren eines Orthogonalsystems (insbesondere also eines Orthonormalsystems) sind linear unabhängig. Insbesondere besteht ein Orthogonalsystem (Orthonormalsystem) im \mathbb{K}^n also aus höchstens n Vektoren. Falls es genau n sind, spricht man auch von einer *Orthogonalbasis/Orthonormalbasis* des \mathbb{K}^n .

Beispiel: Die Vektoren der Standardbasis im \mathbb{K}^n bilden ein Orthonormalsystem bzgl. des Euklidischen Skalarprodukts.

Def. (Symmetrische Matrix, Orthogonalmatrix). Eine Matrix $A \in \mathbb{R}^{n \times n}$ heißt *symmetrisch*, wenn $A^T = A$, also wenn $a_{ij} = a_{ji} \forall i, j = 1, \dots, n$.

Eine Matrix $X \in \mathbb{R}^{n \times n}$ heißt *Orthogonalmatrix*, wenn ihre Spalten ein Orthonormalsystem (also eine Orthonormalbasis des \mathbb{R}^n) bilden.⁷³

(Sprachlich ist das etwas seltsam: Sind die Spalten orthonormal, so spricht man von einer Orthogonalmatrix.)

Geometrische Anschauung: Die Spalten einer Matrix sind ja nichts anderes als die Bilder der Standardbasisvektoren unter der zu der Matrix gehörenden linearen Abbildung. Die zu einer Orthogonalmatrix gehörende lineare Abbildung überführt also die Standardbasis in eine Orthonormalbasis. (Man kann sogar zeigen: Die zu einer Orthogonalmatrix gehörende lineare Abbildung überführt beliebige Orthonormalsysteme wieder in Orthonormalsysteme.) Also: Drehungen und Spiegelungen sowie Hintereinanderschaltungen von Drehungen und Spiegelungen sind Orthogonalmatrizen.

Orthogonalmatrizen haben die schöne Eigenschaft, dass man ihr Inverses ohne Rechnung angeben kann:

Satz (Eigenschaften von Orthogonalmatrizen). Für Orthogonalmatrizen X gilt: X ist invertierbar, und es ist

$$X^{-1} = X^T, \quad \det(X) = \pm 1.$$

Ferner bilden auch die *Zeilen* von X ein Orthonormalsystem.

Beweis. Nach Definition der Orthogonalmatrix ist $X^T X = E_n$ unmittelbar klar. Mit Anwendung von 'det' folgt

$$1 = \det(E_n) = \det(X^T X) = \det(X^T) \det(X) = \det(X) \det(X),$$

also $\det(X) = \pm 1$.

Wegen $\det(X) \neq 0$ ist X invertierbar, wir können also die Gleichung $X^T X = E_n$ mit

⁷³Es gibt Verallgemeinerungen dieser Begriffe für $\mathbb{C}^{n \times n}$ -Matrizen: Eine komplexe Matrix, die $a_{ij} = \overline{a_{ji}}$, also $A^T = \overline{A}$, erfüllt, heißt *hermitesch*, eine komplexe Matrix, deren Spalten ein Orthonormalsystem bilden, heißt *unitär*. Wir wollen uns jedoch auf den reellen Fall beschränken.

X^{-1} von rechts malnehmen. Es folgt $X^T = X^{-1}$.⁷⁴ Daraus wiederum folgt, dass auch $XX^T = E_n$ gilt, was bedeutet, dass die Zeilen von X ein Orthonormalsystem bilden.⁷⁵

Das Wissen um Orthogonalmatrizen erlaubt es, den Satz über die Diagonalisierbarkeit noch einmal genauer anzuschauen; und zwar können wir nun zeigen, dass *alle symmetrischen Matrizen diagonalisierbar sind*:

Satz (Eigenschaften von symmetrischen Matrizen). Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch. Dann gilt:

- a) Alle Eigenwerte $\lambda \in \mathbb{C}$ von A sind reell.
- b) Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal zueinander (im Euklidischen Skalarprodukt). (Die Eigenräume stehen also senkrecht zueinander.)
- c) Es gibt eine Orthonormalbasis des \mathbb{R}^n , die aus Eigenvektoren von A besteht.
- d) A ist diagonalisierbar, und zwar gibt es eine Darstellung $A = X LX^{-1}$ derart, dass L eine (nach a)) *reelle* Diagonalmatrix ist, und X eine *Orthogonalmatrix* ist; es gilt also, wegen $X^{-1} = X^T$,

$$A = X L X^T.$$

Also: Alle symmetrischen Matrizen sind diagonalisierbar, haben reelle Eigenwerte, und die Eigenräume einer symmetrischen Matrix stehen paarweise orthogonal aufeinander. Bemerkung: Die Zerlegung einer symmetrischen Matrix in ein solches Produkt heißt *Hauptachsentransformation*; die Spalten von X (=Richtungen der Eigenvektoren von A) heißen *Hauptachsen* von A (stehen senkrecht aufeinander). Was die Veranschaulichung angeht, gilt also das gleiche, was am Ende von Kap. 3.6.2 allgemein über die Veranschaulichung von diagonalisierbaren Matrizen gesagt wurde; es kommt jedoch hinzu, dass für symmetrische Matrizen die Hauptachsen, also die Richtungen der Eigenräume, senkrecht aufeinander stehen.

(Teilweiser) Beweis des Satzes.

- a) Sei $\lambda \in \mathbb{C}$ Eigenwert von A und $\vec{x} \in \mathbb{C}^n$ zugehöriger Eigenvektor. Wir wollen $\lambda = \bar{\lambda}$ zeigen, da dies gleichbedeutend mit $\lambda \in \mathbb{R}$ ist.
Es ist

$$\langle A\vec{x}, \vec{x} \rangle = \langle \lambda\vec{x}, \vec{x} \rangle = \lambda \langle \vec{x}, \vec{x} \rangle$$

⁷⁴Dies ist allgemeingültig: Gilt $AB = E_n$ und ist zusätzlich bekannt, dass A invertierbar ist, so folgt $A^{-1} = B$ (d.h. es muss $BA = E_n$ nicht mehr geprüft werden).

⁷⁵Das Vorzeichen der Determinante drückt aus, ob sich die 'Händigkeit' des Orthogonalsystems bei Anwendung von X ändert: Ist $\det(X) = +1$, so ist das Bild eines Rechts(bzw. Links)-Systems wieder ein Rechts(Links)-System (\rightarrow Drehungen). Falls $\det(X) = -1$, wo werden Rechts- in Linkssysteme überführt und umgekehrt (\rightarrow Spiegelungen an Hyperebenen).

aber auch

$$\langle A\vec{x}, \vec{x} \rangle = \langle \vec{x}, \overline{A}^T \vec{x} \rangle \stackrel{(1)}{=} \langle \vec{x}, A^T \vec{x} \rangle \stackrel{(2)}{=} \langle \vec{x}, A\vec{x} \rangle = \langle \vec{x}, \lambda\vec{x} \rangle = \overline{\lambda} \langle \vec{x}, \vec{x} \rangle,$$

wobei in (1) verwendet wurde, dass A reell ist, und in (2), dass A symmetrisch ist.

Division durch $\langle \vec{x}, \vec{x} \rangle \neq 0$ liefert die Behauptung.⁷⁶

- b) Es sei $A\vec{x}_1 = \lambda_1\vec{x}_1$ und $A\vec{x}_2 = \lambda_2\vec{x}_2$ mit $\lambda_1 \neq \lambda_2$. Mit Hilfe der Rechenregeln fürs komplexe Skalarprodukt bekommen wir

$$\lambda_1 \langle \vec{x}_1, \vec{x}_2 \rangle = \langle \lambda_1\vec{x}_1, \vec{x}_2 \rangle = \langle A\vec{x}_1, \vec{x}_2 \rangle \stackrel{(*)}{=} \langle \vec{x}_1, A\vec{x}_2 \rangle = \langle \vec{x}_1, \lambda_2\vec{x}_2 \rangle \stackrel{(**)}{=} \lambda_2 \langle \vec{x}_1, \vec{x}_2 \rangle,$$

wobei in (*) verwendet wurde, dass A reell und symmetrisch ist, und in (**), dass λ_2 reell ist. Also ist

$$\underbrace{(\lambda_1 - \lambda_2)}_{\neq 0} \langle \vec{x}_1, \vec{x}_2 \rangle = 0$$

woraus die Orthogonalität von \vec{x}_1 und \vec{x}_2 folgt.

- c) Als nächsten muss man zeigen, dass für alle EW von A die geometrische gleich der algebraischen Vielfachheit; auf diesen Beweisschritt wollen wir verzichten. Daraus folgt, dass es eine Basis des \mathbb{R}^n von Eigenvektoren gibt. Dass es sogar eine *Orthonormalbasis* von Eigenvektoren gibt, sieht man wie folgt ein. Man wählt zunächst für jeden einzelnen Eigenraum $\text{Eig}(\lambda_i)$ eine Orthonormalbasis. (Dass dies möglich ist, ist zumindest anschaulich klar/plausibel; ein exakter Beweis verwendet das sog. Schmidt'sche Orthogonalisierungsverfahren, siehe Literatur). Setzt man alle diese Orthonormalbasen der Eigenräume zusammen, so bekommt man wegen b) eine Orthonormalbasis des \mathbb{R}^n .
- d) Nach dem Satz über Diagonalisierbarkeit aus Kap. 3.6.2 folgt daraus, dass es eine Basis aus Eigenvektoren gibt, dass A diagonalisierbar ist; $A = X LX^{-1}$, wobei die Diagonaleinträge von L die Eigenwerte von A sind und die Spalten von X zugehörige Eigenvektoren. Nach a) enthält die Diagonalmatrix L nur reelle Einträge. Nach c) können die Spalten von X orthonormal gewählt werden, dann ist X Orthogonalmatrix.

⁷⁶Eigenvektoren können dann immer reell gewählt werden, wenn der Eigenwert einer reellen Matrix reell ist. Das sieht man wie folgt: Aus $A\vec{x} = \lambda\vec{x}$ folgt durch Konjugiert-Komplex-Bildung unter den gegebenen Voraussetzungen $A\vec{\bar{x}} = \lambda\vec{\bar{x}}$, also neben \vec{x} ist auch $\vec{\bar{x}}$ ein EV zum EW λ . Da der Eigenraum ein Vektorraum ist, ist dann auch $\vec{x} + \vec{\bar{x}}$ ein Eigenvektor, und $\vec{x} + \vec{\bar{x}}$ ist immer reell.

Ausblick (auf die kommenden Semester des C-Kurses):

Im **zweiten Semester** wird die *Analysis* im Zentrum stehen. Grob gesprochen kann man darunter den Bereich der Mathematik auffassen, der auf *Grenzwerten* beruht. Wichtige Objekte werden sein: Folgen, Reihen, Funktionen von \mathbb{R} nach \mathbb{R} und deren Eigenschaften wie Stetigkeit, Differenzierbarkeit, sowie das Berechnen von Integralen/Stammfunktionen. Am Ende des zweiten Semesters beschäftigen wir uns auch mit Funktionen von \mathbb{R}^n nach \mathbb{R} oder von \mathbb{R}^n nach \mathbb{R}^m ; hier werden wir wieder auf unsere Vektoren und Matrizen aus der Linearen Algebra treffen.

Das **dritte Semester** kann von allen drei Anfangssemestern als das anwendungsorientierteste bezeichnet werden, denn es geht um Probleme, die bei anwendungsorientierten Fragestellungen (Fragestellungen aus anderen Wissenschaften) häufig auftreten: (1) Bestimmung von Extremwerten von Funktionen von \mathbb{R}^n nach \mathbb{R} (auch als *Optimierung* bezeichnet), (2) *gewöhnliche Differentialgleichungen* (diese beschreiben viele Naturvorgänge, die zeitliche Evolution von 'Systemen'), (3) *Algebra* (hier werden wir uns wieder mit Körpern und Ringen und Gruppen beschäftigen, sowie Anwendungen der Algebra im Bereich der Kodierungstheorie (wie erkennt man Fehler bei der Datenübermittlung mittels Prüfsummen) und der Kryptographie (RSA-Verschlüsselung, beruhend auf großen Primzahlen)). Bei den Themen (1) und (2) werden wir auf unser Wissen über Matrizen und Vektoren aus dem ersten Semester zurückgreifen.

Das **vierte Semester** ist der *Stochastik* und der *Statistik* gewidmet.

Ich bedanke mich ganz herzlich bei Prof. D. Kuzmin, bei Dr. M. Neuss-Radu, bei B. Reuter, sowie bei mehreren Hörern meiner Vorlesung für die Hilfe bei der Eliminierung diverser Tippfehler in diesem Skript.