Skript zur Vorlesung

Lineare Algebra 1 (BA/GYM)

(Wintersemester 2016/17)

Dieses Geheft enthält in kompakter Form die wesentlichen Inhalte, wie sie in der Vorlesung ,,Lineare Algebra 1 (BA/GYM)" vorgestellt werden.

Es ist zum Gebrauch neben der Vorlesung gedacht und erhebt nicht den Anspruch, ,,in sich selbst verständlich" oder vollständig zu sein.

S. Hilger

Inhaltsverzeichnis

1 Aussagen, Mengen, Relationen und Abbildungen

Wir können uns hier nicht ausführlich mit den feinen und tiefen mathematischen Einsichten in zwei der grundlegenden Teilgebiete abgeben, die Aussagenlogik und Mengenlehre. Nichtsdestoweniger müssen wir einige elementare Begriffe und Fakten bereitstellen.

1.1 Aussagen

1.1.1 Naive Beschreibung

> Eine *Aussage* ist ein sprachliches Gebilde, das — innerhalb eines vereinbarten Kontexts — prinzipiell als *wahr* (w) oder *falsch* (f) erkannt werden kann.

Ist eine Aussage wahr, so sagt man auch sie *gilt*.

1.1.2 Nicht–Beispiele

- Bleib hier! (Grammatik)
- Wie geht es Dir? (Grammatik)
- Die Resteverwertung ist bunt. (Sinngehalt)
- „Rot" ist eine schöne Farbe. (Wertung, Subjektivität)
- Harald ist rothaarig. (Kontext)
- $x \geq 0$ (Kontext)
- „Der Satz, den Sie gerade lesen (hören), ist falsch".
- Der älteste Mann der Welt ist tot. (Schlagzeile im Eichstätter Kurier)

1.1.3 Beispiele

„Gute" Beispiele erhält man im allgemeinen dadurch, dass man als Kontext einfache klare Sachverhalte wählt (Quiz-Show) oder — eben — die „Mathematik".

Ist beispielweise $X = \{1, 2, 3\}$, so kann man von den folgenden Aussagen sofort sagen, ob sie wahr oder falsch sind.

- $1 \in X$. (w)
- $3 \notin X$. (f)
- $5 \in X$.(f)
- 5 ist ungerade. (w)

1.1.4 Andere berühmte Beispiele

- Für $n \geq 3$ hat die Gleichung $x^n + y^n = z^n$ keine ganzzahlige nichttriviale Lösung. (trivial heißt „für jeden sofort zu sehen" oft ist es die Null–Lösung). Seit 1992 ist die Wahrheit dieser Aussage bewiesen.
- Es gibt unendlich viele Primzahlen (Bekannt seit 300 v. Chr., Euklid / Siehe Abschnitt 1.3.6).
- Es gibt unendlich viele Primzahlzwillinge (Bis heute nicht entschieden).
- Jede gerade Zahl größer als 2 ist Summe zweier Primzahlen (Goldbach-Vermutung, bis heute nicht entschieden).

1.2 Logische Operationen

1.2.1 Einstieg — Überblick

Aussagen können zu neuen verknüpft werden. Der Wahrheitswert der neuen Aussage bestimmt sich aus denen der vorgegebenen Aussagen nach bestimmten Regeln, den „formalen Gesetzen der Logik".

Auf der linken Seite der folgenden Tabelle sind Operationen mit Aussagen aufgelistet, die wir in den folgenden Abschnitten noch genauer besprechen. Auf der rechten Seite ist die Zuordnung der Wahrheitswerte angegeben.

Name:	Sprechweise:	Symbol:				
Eine Aussage vorgegeben:		$\mathcal{A}$	w		f	
Negation	NICHT $\mathcal{A}$	$\neg\mathcal{A}$	f		w	
Zwei Aussagen vorgegeben:		$\mathcal{A}, \mathcal{B}$	(w, w)	(w, f)	(f, w)	(f, f)
Konjunktion	$\mathcal{A}$ UND (ZUGLEICH) $\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	w	f	f	f
Disjunktion	$\mathcal{A}$ ODER $\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	w	w	w	f
Disjunktion (ausschl.)	ENTWEDER $\mathcal{A}$ ODER $\mathcal{B}$		f	w	w	f
Implikation	$\mathcal{A}$ IMPLIZIERT $\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	w	f	w	w
Bijunktion	$\mathcal{A}$ ÄQUIVALENT $\mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$	w	f	f	w

1.2.2 Die Negation

Name:	Sprechweise:	Symbol:				
Eine Aussage vorgegeben:		$\mathcal{A}$	w		f	
Negation	NICHT $\mathcal{A}$	$\neg\mathcal{A}$	f		w	

Auf sprachlicher Ebene wird die Negation einer Aussage meist durch das Wörtchen NICHT beschrieben. Auch die Vorsilben UN, IN bzw. IR oder die wechselweise Ersetzung von EIN durch KEIN sind üblich. Manchmal gibt es auch Begriffspaare, die gegenteilig zueinander sind.

Die Negation kehrt den Wahrheitswert einer Aussage um.

Beispiele:

$\mathcal{A}$	$\neg\mathcal{A}$
Jedes LGS lässt sich durch Zeilen-Äquivalenzumformungen in Dreiecksform überführen.	Nicht jedes LGS lässt sich durch Zeilen-Äquivalenzumformungen in Dreiecksform überführen.
Es gibt endlich viele Primzahlzwillinge.	Es gibt unendlich viele Primzahlzwillinge.
$\sqrt{2}$ ist eine rationale Zahl.	$\sqrt{2}$ ist eine irrationale Zahl.

1.2.3 Die Konjunktion

Name:	Sprechweise:	Symbol:				
Zwei Aussagen vorgegeben:		$\mathcal{A},\mathcal{B}$	(w,w)	(w,f)	(f,w)	(f,f)
Konjunktion	$\mathcal{A}$ UND (ZUGLEICH) $\mathcal{B}$	$\mathcal{A}\wedge\mathcal{B}$	w	f	f	f

Auf sprachlicher Ebene wird die Konjunktion zweier Aussagen meist durch das zwischengestellte Wörtchen UND, manchmal UND ZUGLEICH beschrieben. Auf symbolischer Ebene bedeutet auch oft das zwischengestellte Komma ein UND. Der sprachliche Hinweis auf UND wird oft ganz weggelassen.

Beispiele:

- In einem achsensymmetrischen Viereck sind zwei Seiten gleich lang UND zwei Winkel gleich groß.
- Die Symmetrieachse halbiert senkrecht die Verbindungsstrecke von Punkt und Bildpunkt. (Das Schlüsselwort UND ist implizit enthalten.)
- Bei dem Girokonto sind Adalbert UND Adelheid zeichnungsberechtigt.

Die Aussage $\mathcal{A}\wedge\neg\mathcal{A}$ ist falsch für alle Aussagen $\mathcal{A}$.

1.2.4 Die Disjunktion

Name:	Sprechweise:	Symbol:				
Zwei Aussagen vorgegeben:		$\mathcal{A}, \mathcal{B}$	(w, w)	(w, f)	(f, w)	(f, f)
Disjunktion	$\mathcal{A}$ ODER $\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	w	w	w	f

Sprachlich wird die Disjunktion durch das zwischengestellte ODER ausgedrückt.

Im mathematischen Kontext beinhaltet die Gültigkeit einer durch ODER hergestellten Verknüpfung zweier Aussagen immer auch die Gültigkeit beider Teilaussagen. Im Alltagssprachgebrauch ist dies nicht genau geklärt, oft wird das ODER ausschließend aufgefasst.

Beispiele:

- Zwei Geraden sind parallel ODER sie schneiden sich.
  (wahr im $\mathbb{R}^2$, falsch im $\mathbb{R}^n$, $n \geq 3$. Kann beides wahr sein?)
- ,,Geld ODER Leben" sagte der Raubmörder noch vorher.
- Der Mathematiklehrer sagt zur Klasse: Ihr dürft bei der heute gestellten Hausaufgabe die Aufgabe 3 ODER die Aufgabe 5 weglassen.
- Bei dem Girokonto ist Edelbert ODER Edeltraut zeichnungsberechtigt.

Die Aussage $\mathcal{A} \vee \neg\mathcal{A}$ ist wahr für alle Aussagen $\mathcal{A}$. Das Zusammenspiel dieser Aussage mit der oben angegebenen dualen Aussage kommt in dem klassischen philosophischen Grundsatz ,,Tertium non datur" zum Ausdruck.

1.2.5 Die ausschließende Disjunktion

Name:	Sprechweise:	Symbol:				
Zwei Aussagen vorgegeben:		$\mathcal{A}, \mathcal{B}$	(w, w)	(w, f)	(f, w)	(f, f)
Disjunktion (ausschl.)	ENTWEDER $\mathcal{A}$ ODER $\mathcal{B}$		f	w	w	f

Sprachlich wird die ausschließende Disjunktion durch die Paarung eines vorangestellten ENTWEDER und eines zwischengestellten ODER ausgedrückt.

Beispiele:

- Für zwei verschiedene natürliche Zahlen m, n gilt ENTWEDER $m < n$ ODER $n < m$.
  (wahr)
- Für zwei verschiedene natürliche Zahlen m, n gilt ENTWEDER $m|n$ ODER $n|m$. (falsch)
- Die Lateinlehrerin sagt zur Klasse: Ihr dürft bei der heute gestellten Hausaufgabe ENTWEDER die Aufgabe 3 ODER die Aufgabe 5 weglassen.

1.2.6 Die Implikation

Name:	Sprechweise:	Symbol:				
Zwei Aussagen vorgegeben:		$\mathcal{A}, \mathcal{B}$	(w, w)	(w, f)	(f, w)	(f, f)
Implikation	$\mathcal{A}$ IMPLIZIERT $\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	w	f	w	w

Anstelle von „$\mathcal{A}$ IMPLIZIERT $\mathcal{B}$" spricht man auch:

- Aus $\mathcal{A}$ folgt $\mathcal{B}$.
- Wenn $\mathcal{A}$, dann $\mathcal{B}$.
- $\mathcal{B}$, wenn $\mathcal{A}$.
- $\mathcal{A}$ ist hinreichend für $\mathcal{B}$.
- $\mathcal{B}$ ist notwendig für $\mathcal{A}$.
- (Engl.) If $\mathcal{A}$, then $\mathcal{B}$.

Beispiele:

- WENN heute Montag ist, DANN beginnt der Werktagsname von morgen mit D.
  (An jedem Wochentag wahr.)
- WENN Du im Abitur 3,5 schaffst, bekommst Du ein Auto.
  (Diese Aussage ist nur dann falsch, wenn das Versprechen nicht eingelöst wird. Sie ist insbesondere wahr, wenn „trotz Scheiterns" ein Auto geschenkt wird.)
- WENN $3 + 4 = 8$, DANN $5 = 0$. (wahr. Diese Aussage kann auch arithmetisch bewiesen werden: Zieht man auf beiden Seiten der ersten Gleichung 7 ab, so stellt sich heraus: $0 = 1$. Beide Seiten dieser Gleichung werden dann mit 5 multipliziert. Solche Spitzfindigkeiten werden nicht Ihr mathematischer Alltag sein.)
- WENN eine natürliche Zahl mit gerader Stellenzahl (im 10er System) eine Spiegelzahl ist, DANN ist sie ohne Rest durch 11 teilbar.

1.2.7 Die Bijunktion

Name:	Sprechweise:	Symbol:				
Zwei Aussagen vorgegeben:		$\mathcal{A}, \mathcal{B}$	(w, w)	(w, f)	(f, w)	(f, f)
Bijunktion	$\mathcal{A}$ ÄQUIVALENT $\mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$	w	f	f	w

Anstelle von „$\mathcal{A}$ ÄQUIVALENT $\mathcal{B}$" sagt man auch:

- $\mathcal{A}$ ist hinreichend und notwendig für $\mathcal{B}$.
- $\mathcal{A}$ genau dann, wenn $\mathcal{B}$.
- (Engl.) $\mathcal{A}$, if and only if $\mathcal{B}$, in Kurzform oft mit dem Kunstwort: $\mathcal{A}$ iff $\mathcal{B}$.

Beispiele

- Ein Kreis mit $[AB]$ als Durchmesser geht genau dann durch C, wenn der Innenwinkel des Dreiecks ABC bei C das Maß $90\,^\circ$ hat (Satz von Thales).

- Eine natürliche Zahl ist genau dann eine Quadratzahl, wenn die Zahl ihrer Teiler ungerade ist.
- Eine natürliche Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Ein Vergleich der Wahrheitswerte zeigt, dass

$$(\mathcal{A} \Leftrightarrow \mathcal{B}) \quad \Leftrightarrow \quad \Big((\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\mathcal{B} \Rightarrow \mathcal{A})\Big).$$

Das bedeutet, dass der Beweis einer Äquivalenz durch Beweis der beiden Implikationen $\mathcal{A} \Rightarrow \mathcal{B}$ und $\mathcal{B} \Rightarrow \mathcal{A}$ bewerkstelligt werden kann.

1.2.8 Aussagenalgebra Die Gesetze der Operationen $\neg, \wedge, \vee$ und der aus ihnen abgeleiteten Operationen wie $\Rightarrow, \Leftrightarrow$ innerhalb eines Systems von Aussagen lassen sich in einem ,,Axiomensystem" zusammenfassen, das die Struktur eines ,,BOOLE'schen Verbandes" trägt. Alle ,,Rechenregeln" für Aussagen lassen sich aus diesem Axiomen herleiten. Wir werden einige Boole'sche Rechenregeln in den Übungen behandeln. Hier nur ein Beispiel:

$$\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \quad \Longleftrightarrow \quad (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C}) \qquad (\wedge\text{–Distributivgesetz})$$

Zur Veranschaulichung ein Beispiel:

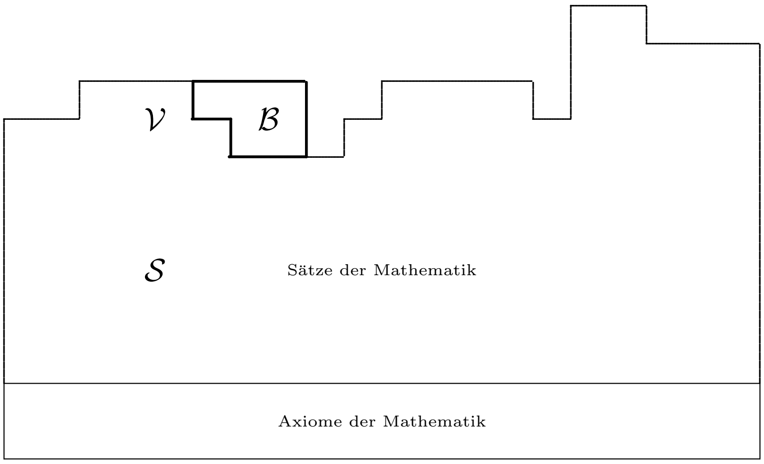
$\mathcal{A}$: Ich kaufe Papier
$\mathcal{B}$: Ich kaufe einen Bleistift
$\mathcal{C}$: Ich kaufe einen Kugelschreiber

Beweis durch Wahrheitswerttabelle: Für alle acht Kombinationen der Wahrheitswerte von $\mathcal{A}, \mathcal{B}, \mathcal{C}$ wird nachgeprüft, dass die Wahrheitswerte von $\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C})$ und $(\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$ übereinstimmen.

$\mathcal{A}$	w	w	w	w	f	f	f	f
$\mathcal{B}$	w	w	f	f	w	w	f	f
$\mathcal{C}$	w	f	w	f	w	f	w	f
$\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C})$	w	w	w	f	f	f	f	f
$(\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$	w	w	w	f	f	f	f	f

1.3 Mathematik als Aussagennetz im Kontext der Mengenlehre

1.3.1 Axiome Sehr stark vereinfacht kann das Programm der wissenschaftlichen Mathematik so in einem Diagramm dargestellt werden:



Ausgangspunkt ist eine Sammlung von einigen grundlegenden Aussagen im Kontext der Mengenlehre, die nicht auf andere Aussagen zurückgeführt werden können. Man nennt diese grundlegenden Aussagen die *Axiome*. Sie werden als wahr gesetzt.

Ausgehend davon werden weitere wahre Aussagen abgeleitet, die in diesem Zusammenhang dann *Sätze* (oder Theoreme, Korollare, Folgerungen, Präpositionen, Hilfssätze, Lemmata,. . .) heißen.

Die zeitlose Aktivität eines Mathematikers oder einer Mathematikerin besteht darin, das System der Sätze zu erlernen, sich darin zu bewegen und — vor allem — neue Sätze zu erschließen und zu beweisen. Dieses Programm unterliegt einerseits einem historischen Ablauf und andererseits der individuellen Entwicklung.

1.3.2 Mathematische Sätze bestehen letztlich aus Aussagen der Form

$$\underset{\text{Voraussetzung}}{\mathcal{V}} \quad \Longrightarrow \quad \underset{\text{Behauptung.}}{\mathcal{B}}$$

Die *Voraussetzung* $\mathcal{V}$ wird dabei dem System der bereits abgeleiteten Sätze entnommen. die *Behauptung* $\mathcal{B}$ ist die aktuell zu beweisende neue Aussage.

Bei Formulierungen von Sätzen ist es meist so, dass die Voraussetzung $\mathcal{V}$ nur die aktuell wesentliche Information enthält. Viele weitere Anteile der Voraussetzung beinhalten unausgesprochen bisher behandelte Axiome oder Sätze oder den gerade aktuellen Kontext des Satzes.

Beispiel eines Satzes:

> Zwei Geraden sind parallel oder sie schneiden sich.

Der unausgesprochene Kontext besteht in der ,,Geometrie der Zeichenebene", die die Begriffsbildungen ,,Gerade, parallel, sich schneiden" bereitstellt. Ein guter Beweis erfordert weiter die Klärung, welche Sätze und Axiome aus der ebenen Geometrie als Voraussetzung vorgegeben sind.

1.3.3 Beweisen Der Beweis eines mathematischen Satzes besteht also darin, die Implikation $\mathcal{V} \Rightarrow \mathcal{B}$ als wahr zu erweisen. Dies geschieht dadurch, dass man die Voraussetzung $\mathcal{V}$ als wahr betrachtet und dann in kleinen ,,allgemein nachvollziehbaren" Schritten die Behauptung $\mathcal{B}$ herleitet. Was dabei ,,allgemein nachvollziehbar" heißt, entzieht sich einer genaueren mathematischen Definition, die mathematische Praxis weltweit zeigt aber, dass darüber i.a. Übereinkunft erzielt werden kann.

1.3.4 Widerspruchsbeweis

Mithilfe einer Wahrheitswerttabelle überlegen wir zunächst, dass für zwei gegebene Aussagen $\mathcal{V}$ und $\mathcal{B}$ die vier Aussagen

$$\mathcal{V} \Rightarrow \mathcal{B} \qquad \neg\mathcal{B} \Rightarrow \neg\mathcal{V} \qquad \neg\mathcal{V} \vee \mathcal{B} \qquad \neg(\mathcal{V} \wedge \neg\mathcal{B})$$

äquivalent sind. Das geschieht dadurch, dass für alle vier Kombinationen der Wahrheitswerte von $\mathcal{V}, \mathcal{B}$ getestet wird, ob die Wahrheitswerte der vier Aussagen übereinstimmen:

$\mathcal{V}$	w	w	f	f
$\mathcal{B}$	w	f	w	f
$\neg\mathcal{V}$	f	f	w	w
$\neg\mathcal{B}$	f	w	f	w
$\mathcal{V} \Rightarrow \mathcal{B}$	w	f	w	w
$\neg\mathcal{B} \Rightarrow \neg\mathcal{V}$	w	f	w	w
$\neg(\mathcal{V} \wedge \neg\mathcal{B})$	w	f	w	w
$\neg\mathcal{V} \vee \mathcal{B}$	w	f	w	w

Das bedeutet, dass man den Beweis der Implikation $\mathcal{V} \Rightarrow \mathcal{B}$ durch den Beweis jeder der anderen äquivalenten Aussagen aus den letzten drei Zeilen ersetzen kann.

Sprachlich lassen sich die drei Spielarten so beschreiben:

$\boxed{\neg\mathcal{B} \Rightarrow \neg\mathcal{V}}$ Man nimmt an, dass die Behauptung $\mathcal{B}$ falsch ist und schließt daraus (unter strenger Anwendung der Logik), dass die Voraussetzung $\mathcal{V}$ falsch ist. Man spricht hier vom *Beweisen durch Annahme der gegenteiligen Behauptung*.

$\boxed{\neg(\mathcal{V} \wedge \neg\mathcal{B})}$ Nehme die Aussage $\mathcal{V}$ und die Aussage $\neg\mathcal{B}$ als wahr an und leite daraus irgendeine falsche Aussage $\mathcal{F}$ (einen Widerspruch) her. Man hat also $\mathcal{V} \wedge \neg\mathcal{B} \Rightarrow \mathcal{F}$ bewiesen. Die Wahrheitswertzuordnung durch $\Rightarrow$ zeigt dann, dass $\mathcal{V} \wedge \neg\mathcal{B}$ falsch ist und somit $\neg(\mathcal{V} \wedge \neg\mathcal{B})$ wahr. Diese Methode heißt *Beweisen durch Herstellen eines Widerspruchs*, kurz *Widerspruchsbeweis*.

$\boxed{\neg\mathcal{V} \vee \mathcal{B}}$ Man beweist (unabhängig vom Wahrheitswert für $\mathcal{V}$), dass die Behauptung $\mathcal{B}$ stimmt oder die Voraussetzung $\mathcal{V}$ falsch ist.

Ein Widerspruchsbeweis wird typischerweise verwendet als Beweis dafür, dass etwas **nicht** existiert. Beispiele dafür sind die folgenden beiden ,,Sätzchen", deren Beweise fast schon für Schüler/innen erreichbar sind:

1.3.5 Sätzchen Ist s eine rationale Zahl, so ist $s^2 \neq 2$.

Um dies zu beweisen, isolieren wir Voraussetzung und Behauptung aus diesem Satz:

$\mathcal{V}$: s ist eine rationale Zahl.

$\mathcal{B}$: Es ist $s^2 \neq 2$.

Wir nehmen $\mathcal{V}$ und das Gegenteil von $\mathcal{B}$ als wahr an.

Ohne **B**eschränkung **d**er **A**llgemeinheit (O.B.d.A) können wir annehmen, dass s positiv ist.

Aufgrund von $\mathcal{V}$ hat s die Form $s = \frac{m}{n}$ mit $m, n \in \mathbb{N}$. Der Bruch kann gekürzt werden, so dass $s = \frac{p}{q}$ mit $p, q \in \mathbb{N}$, teilerfremd.

Aufgrund von $\neg\mathcal{B}$ gilt dann weiter

$$\begin{aligned}
& s^2 = 2 \\
\Longrightarrow \quad & \frac{p^2}{q^2} = 2 \\
\Longrightarrow \quad & p^2 = 2q^2 \\
\Longrightarrow \quad & 2 \text{ ist Primteiler von } p. \\
\Longrightarrow \quad & 4 \text{ teilt } p^2 \\
\Longrightarrow \quad & 2 \text{ teilt } q^2 \quad \text{{\scriptsize (Dieser Schluss gründet sich auch auf $p^2 = 2q^2$ drei Zeilen weiter oben.)}} \\
\Longrightarrow \quad & 2 \text{ ist Primteiler von } q.
\end{aligned}$$

Wir haben bewiesen, dass 2 sowohl ein Teiler von p als auch ein Teiler von q ist. Das stellt einen WIDERSPRUCH dazu dar, dass p und q teilerfremd sind.

1.3.6 Sätzchen Es gibt unendlich viele Primzahlen (Euklid).

Voraussetzung und Behauptung können hier wie folgt dargestellt weden:

$\mathcal{V}$: „Teilbarkeitslehre" inkl. Satz über die eindeutige Primfaktorzerlegung

$\mathcal{B}$: Es gibt unendlich viele Primzahlen

Wir nehmen $\mathcal{V}$ und das Gegenteil von $\mathcal{B}$ als wahr an.

Aufgrund von $\neg\mathcal{B}$ können wir das Produkt aller Primzahlen hinschreiben:

$$m = 2 \cdot 3 \cdot 5 \cdot \ldots\ldots \cdot p_{\max}.$$

$m + 1$ ist keine Primzahl, besitzt also aufgrund des Satzes von der Primzahlzerlegung einen Primteiler p.

Da die Primzahl p ein Teiler von m und von $m + 1$ ist, teilt sie auch die Differenz $= 1$. WIDERSPRUCH.

1.4 Mengen

1.4.1 Cantor'sche Auffassung über Mengen, Naive Mengenlehre

> Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche die Elemente von M genannt werden, zu einem Ganzen.
> [Gesammelte Abhandlungen, ed E. Zermelo, Berlin 1932]
>
> **Georg Cantor** (1845 – 1918, Begründer der Mengenlehre)

1.4.2 Elemente von Mengen

Zentral wichtig, letztlich aber undefiniert, ist die Beobachtung, dass zwischen zwei mathematischen Objekten a und M die Beziehung

a ist Element der Menge M, symbolisch: $a \in M$

bestehen kann.

Innerhalb der Mathematik, wie wir sie kennenlernen werden, ist es für zwei Objekte i.a. prinzipiell klar entscheidbar, ob

$a \in M$ oder $a \notin M$.

1.4.3 Schreibweise Eine Menge wird — zunächst — durch Aufzählung aller ihrer Elemente beschrieben. Beispiele

$$M = \left\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\right\} = \left\{0, 1, 2, \dots, 9\right\},$$

oder

$$M = \left\{x, y, z, g, e, b, a\right\}.$$

Beachte dabei:

- In der wissenschaftlichen Mathematik werden zur Trennung Kommata gesetzt, in der Schule Strichpunkte.
- Eine bestimmte Reihenfolge ist mathematisch ohne Belang, manchmal ist sie zweckmäßig. Bei Vorliegen einer ,,bekannten, selbstverständlichen" Reihenfolge kann man eine längere Liste durch Punkte abkürzen.

- Mehrfachnennungen sind möglich:

$$\Big\{1,4,12,20\Big\} \quad = \quad \Big\{12,4,20,1\Big\} = \Big\{1,12,4,20,1,12,20\Big\}.$$

- Auch Mengen können Elemente sein.

$$M \quad = \quad \Big\{1,2,3,\{1,2\}\Big\}, \qquad \text{Beachte dabei } 2 \neq \{2\}.$$

- Mit Hilfe von Punkten kann man auch bestimmte unendliche Mengen kennzeichnen:

$$\Big\{1,3,5,\dots\Big\}, \qquad \Big\{2,3,5,7,11,\dots\Big\}, \qquad \Big\{\dots,-4,-2,0,+2,+4,\dots\Big\}$$

1.4.4 Die leere Menge

Die Menge, die kein Element enthält, wird *leere Menge* genannt.

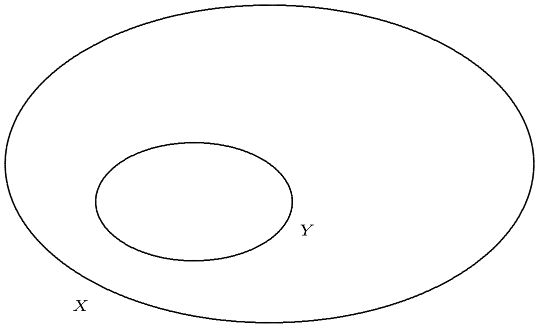
Als Symbol wird weltweit das $\varnothing$ oder $\emptyset$ verwendet. In der Schule ist das bildsprachliche $\{\ \}$ üblich.

1.5 Operieren mit Mengen

1.5.1 Gleichheit Zwei Mengen sind (per definitionem, Cantor) gleich, wenn sie in ihren Elementen übereinstimmen:

$$X = Y \iff (a \in X \iff a \in Y).$$

1.5.2 Teilmenge Es seien zwei Mengen X, Y gegeben.



Venn-Diagramm

- Y heißt *Teilmenge* von X,

  $$Y \subseteq X,$$

  wenn gilt: Aus $x \in Y$ folgt $x \in X$.

- Y heißt *echte Teilmenge* von X, wenn zusätzlich $Y \neq X$ gilt. Symbolisch kann dies mit $Y \subsetneqq X$ zum Ausdruck gebracht werden.

- Die Verwendung von $Y \subset X$ als Zeichen für eine der obigen Beziehungen ist wegen der Missverständlichkeit nicht so günstig.

Folgerungen:

1. Für jede Menge X gilt:

   $$\emptyset \subseteq X.$$

2. Für zwei Mengen X und Y sind die beiden Aussagen

   $$X = Y, \qquad (X \subseteq Y) \text{ und } (Y \subseteq X)$$

äquivalent. Der Beweis der Gleichheit zweier Mengen geschieht oft durch den Nachweis dieser wechselweisen Teilmengenbeziehung.

1.5.3 Aussagen definieren Teilmengen Es sei X eine Menge. Für jedes $x \in X$ sei eine Aussage $\mathcal{A}(x)$ vorgegeben[1]. Dann kann die Teilmenge

$$Y = \{x \in X \mid \mathcal{A}(x) \text{ ist wahr}\} \overset{\text{kürzer}}{=} \{x \in X \mid \mathcal{A}(x)\}$$

gebildet werden. Der senkrechte Strich ist als ,,mit der Eigenschaft, dass" zu lesen.

Beispiel: $\{n \in \mathbb{N} | n \text{ ist eine Quadratzahl}\} = \{1, 4, 9, 16, 25, 36, \dots\}.$

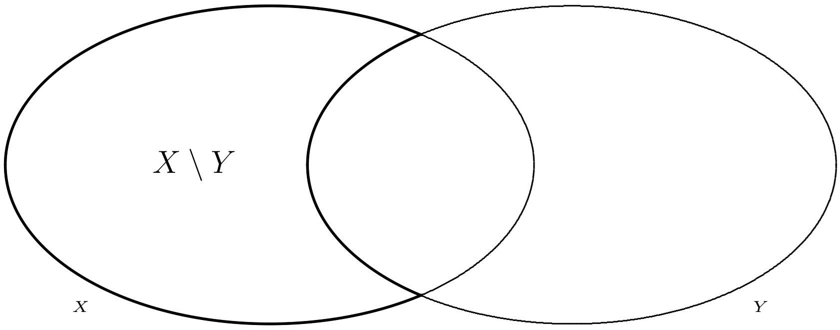
[1]Man nennt dies auch eine Aussageform.

1.5.4 Differenzmenge und Komplement

Für zwei vorgegebene Mengen X, Y heißt

$$X \setminus Y \;:=\; \left\{ x \in X \;\middle|\; x \notin Y \right\}$$

die *Differenzmenge*. (Der Doppelpunkt steht auf der Seite des zu definierenden Objekts.)



Venn-Diagramm

Beispiel:

$$X \;=\; \{0,1,4,7,9\} \qquad Y \;=\; \{0,2,3,4,5\} \qquad X \setminus Y \;=\; \{1,7,9\}$$

Wir haben dabei nicht vorausgesetzt, dass Y eine Teilmenge von X ist. Falls dies der Fall ist, so heißt die Differenzmenge $X \setminus Y$ auch das *Komplement* oder *Komplementärmenge* von Y in X. Beispiel:

$X \;=\; \{0,1,4,7,9\}$ $\qquad Y \;=\; \{0,7,9\}$ $\qquad \{1,4\}$ ist das Komplement von Y in X

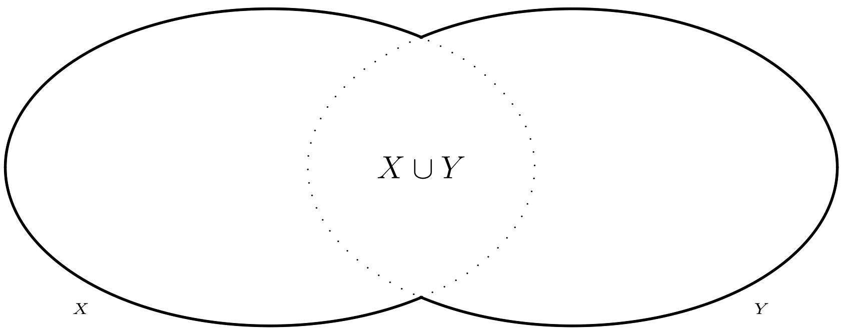
Ist die Obermenge X durch den Kontext fixiert, so schreibt man symbolisch einfach

$$Y^c \;=\; X \setminus Y$$

1.5.5 Vereinigungsmenge Für zwei vorgegebene Mengen X, Y heißt

$$X \cup Y \;:=\; \{z | z \in X \text{ oder } z \in Y\}$$

die *Vereinigung(-smenge)* von X und Y.



Venn-Diagramm

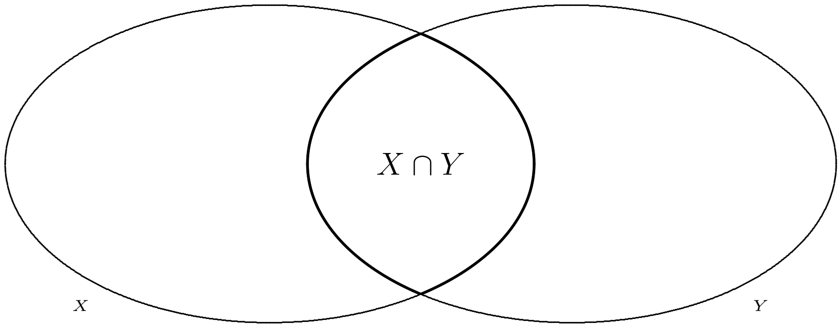
Beispiel:

$$X \;=\; \{0,1,4,7,9\} \qquad Y \;=\; \{0,2,3,4,5\} \qquad X \cup Y \;=\; \{0,1,2,3,4,5,7,9\}$$

1.5.6 Schnittmenge Für zwei vorgegebene Mengen X, Y heißt

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

die *Schnittmenge* oder der *Durchschnitt* von X und Y.



Venn-Diagramm

Beispiel:

$$X \ = \ \{0, 1, 4, 7, 9\} \qquad Y \ = \ \{0, 2, 3, 4, 5\} \qquad X \cap Y \ = \ \{0, 4\}$$

Zwei Mengen X und Y, für die $X \cap Y = \varnothing$ gilt, heißen *disjunkt*.

1.5.7 Potenzmenge Ist eine Menge X gegeben, so heißt die Menge aller Teilmengen von X die *Potenzmenge* von X. Sie wird mit $\mathcal{P}(X)$ bezeichnet. Beispiele:

$$\begin{aligned} \mathcal{P}(\{1,2,3\}) \ &= \ \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\Big\}, \quad \text{(dann:)} \\ & \{1,3\} \subseteq \{1,2,3\} \qquad \text{äquivalent:} \qquad \{1,3\} \in \mathcal{P}(\{1,2,3\}). \end{aligned}$$

Die Menge aller Teilmengen von $\mathbb{N}$ ist $\mathcal{P}(\mathbb{N})$. Sie lässt sich nicht in aufzählender Form darstellen.

$$\begin{aligned} &\{1\} \in \mathcal{P}(\mathbb{N}) \\ &\{2, 34, 93821, 39237\} \in \mathcal{P}(\mathbb{N}) \\ &\{\text{gerade Zahlen}\} \in \mathcal{P}(\mathbb{N}) \\ &\{\text{Primzahlen}\} \in \mathcal{P}(\mathbb{N}) \end{aligned}$$

1.5.8 Mengenalgebra Die Gesetze der Operationen $\setminus, \cap, \cup$ und der aus ihnen abgeleiteten Operationen wie $\subseteq$ innerhalb eines Systems von Mengen lassen sich ebenfalls in einem ,,Axiomensystem" zusammenfassen, das die Struktur eines BOOLE'schen Verbandes trägt.

Ein Beispiel:

$$X \cap (Y \cup Z) \quad = \quad (X \cap Y) \cup (X \cap Z) \qquad (\cap\text{–Distributivgesetz})$$

Beweis (Variante 1): Übertragung in eine Wahrheitstabelle. Betrachte ein Element a bzgl. X, Y, Z.

X	$\in$	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$
Y	$\in$	$\in$	$\notin$	$\notin$	$\in$	$\in$	$\notin$	$\notin$
Z	$\in$	$\notin$	$\in$	$\notin$	$\in$	$\notin$	$\in$	$\notin$
$X \cap (Y \cup Z)$	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$
$(X \cap Y) \cup (X \cap Z)$	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$

Das bedeutet, dass ein beliebiges Element a genau dann in $X \cap (Y \cup Z)$ enthalten ist, wenn es in $(X \cap Y) \cup (X \cap Z)$ enthalten ist.

Beweis (Variante 2): Wir zeigen zunächst, dass $X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z)$:

$$\begin{aligned}
& \text{Es sei } a \in X \cap (Y \cup Z) \\
\Longrightarrow \quad & a \in X \text{ und } (a \in Y \text{ oder } a \in Z) \\
\Longrightarrow \quad & (a \in X \text{ und } a \in Y) \text{ oder } (a \in X \text{ und } a \in Z) \\
\Longrightarrow \quad & a \in (X \cap Y) \cup (X \cap Z)
\end{aligned}$$

Dann muss noch die umgekehrte Richtung gezeigt werden:

$$\begin{aligned}
& \text{Es sei } a \in (X \cap Y) \cup (X \cap Z) \\
\Longrightarrow \quad & (a \in X \text{ und } a \in Y) \text{ oder } (a \in X \text{ und } a \in Z) \\
\Longrightarrow \quad & a \in X \text{ und } (a \in Y \text{ oder } a \in Z) \\
\Longrightarrow \quad & a \in X \cap (Y \cup Z)
\end{aligned}$$

Beweis (Variante 3): Es sei $a \in X \cup Y \cup Z$. Wir betrachten die drei Aussagen:

$$\mathcal{A} : a \in X, \qquad \mathcal{B} : a \in Y, \qquad \mathcal{C} : a \in Z.$$

Dann gilt

$$\begin{aligned}
& a \in X \cap (Y \cup Z) \quad \Longleftrightarrow \quad \mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \\
\overset{\wedge\text{–DG}}{\Longleftrightarrow} \quad & (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C}) \quad \Longleftrightarrow \quad a \in (X \cap Y) \cup (X \cap Z)
\end{aligned}$$

Die in diesem Beweis zum Ausdruck kommende Entsprechung zwischen Aussagenalgebra und Mengenalgebra kann man innerhalb der ,,Verbandstheorie" genauer untersuchen. Wir können und wollen uns damit hier nicht aufhalten.

1.5.9 Aussageformen Es gibt noch ein anderes Wechselspiel zwischen einer gegebenen Menge (*Grundmenge*) M und Aussagen.

Man spricht von einer *Aussageform*, wenn die Elemente x der Menge M als Variable innerhalb einer Aussage $\mathcal{A}(x)$ auftreten. Beispiele

- $n \in \mathbb{N}$, n ist eine Quadratzahl.
- $n \in \mathbb{N}$, n besitzt eine eindeutige Primzahlzerlegung.
- $q \in \mathbb{Q}$, q besitzt eine Quadratwurzel.
- $x \in \mathbb{R}$, $3x^2 - 5x + 7 = 0$

Je nach dem, welches Element aus der Grundmenge eingesetzt wird, ergibt sich eine wahre oder falsche Aussage.

1.5.10 Quantoren

Aus einer Aussageform lassen sich durch besondere *Quantoren* Aussagen herstellen:

- All–Quantor: ,,Für alle $x \in M$ gilt $\mathcal{A}(x)$".

  Symbolisch: $\underset{x \in M}{\forall} \mathcal{A}(x)$ oder $\forall x \in M \;\; \mathcal{A}(x)$

- Existenz–Quantor: Es gibt (mindestens) ein $x \in M$, für das $\mathcal{A}(x)$ gilt.

  Symbolisch: $\underset{x \in M}{\exists} \mathcal{A}(x)$ oder $\exists x \in M \;\; \mathcal{A}(x)$

- Es gibt genau ein $x \in M$, für das $\mathcal{A}(x)$ gilt.

  Symbolisch: $\underset{x \in M}{\exists !} \mathcal{A}(x)$ oder $\exists !\, x \in M \;\; \mathcal{A}(x)$

1.5.11 Satz: Dualität von All- und Existenzquantor unter Negation

Es gelten die beiden Äquivalenzen

$$\neg\Big(\underset{x \in M}{\forall} \mathcal{A}(x) \Big) \iff \underset{x \in M}{\exists} \Big(\neg\mathcal{A}(x) \Big)$$

$$\neg\Big(\underset{x \in M}{\exists} \mathcal{A}(x) \Big) \iff \underset{x \in M}{\forall} \Big(\neg\mathcal{A}(x) \Big)$$

Die obere Zeile bedeutet, dass eine All–Aussage genau dann falsch ist, wenn sie für irgendein Beispiel (,,Gegenbeispiel") falsch ist.

In der unteren Zeile steht, dass es kein einziges x mit der Eigenschaft ,,$\mathcal{A}(x)$ wahr" gibt genau dann, wenn für alle x die Aussage $\mathcal{A}(x)$ falsch ist.

1.5.12 Beispiel

Betrachte die Aussage

Wenn p eine Primzahl ist, so ist auch $2^p - 1$ eine Primzahl.

Zum Beweis, dass der Satz falsch ist, genügt die Angabe eines einzigen Gegenbeispiels: $2^{11} - 1 = 2047 = 23 \cdot 89$.

1.5.13 Mengenalgebra mit unendlich vielen Mengen wird durch Verwendung von Quantoren möglich.

Sind X_i unendlich viele Mengen, die durch einen Index i (aus einer Indexmenge I) gekennzeichnet sind, so definiert man

$$\bigcap_{i \in I} X_i \quad := \quad \{a \,|\, a \in X_i \text{ für alle } i \in I\}$$

$$\bigcup_{i \in I} X_i \quad := \quad \{a \,|\, a \in X_i \text{ für (mindestens) ein } i \in I\}$$

Sind zum Beispiel die Mengen X_i reelle Intervalle

$$X_i \;=\; [-i, +i] \;\subseteq\; \mathbb{R},$$

so ergibt sich

$$\bigcap_{i \in I} X_i \quad = \quad [-1, +1]$$

$$\bigcup_{i \in I} X_i \quad = \quad \mathbb{R}$$

1.6 Relationen

1.6.1 Definition: Geordnetes Paar

Für zwei vorgegebene Mengen X, Y und Elemente $x \in X$, $y \in Y$ heißt

$$(x, y) \quad := \quad \Big\{\{x, y\}, \{x\}\Big\}$$

das durch x und y gebildete *(geordnete) Paar* oder 2–*Tupel*. x und y heißen in diesem Zusammenhang die *erste* bzw. *zweite Koordinate* des Paares.

1.6.2 Satz: Gleichheit von Paaren

Sind X, Y zwei Mengen mit $x_1, x_2 \in X$ und $y_1, y_2 \in Y$ so gilt:

$$(x_1, y_1) \;=\; (x_2, y_2) \quad \Longleftrightarrow \quad x_1 \;=\; x_2 \text{ und } y_1 \;=\; y_2.$$

Dieser Satz wäre mit Mengen anstelle geordneter Paare falsch.

Ist der Satz 1.6.2 akzeptiert, so kann die zugrundeliegende „umständliche" Definition 1.6.1 wieder in den Hintergrund treten.

1.6.3 Beweis Die eine Richtung $\Leftarrow$ ist trivial. Die andere Richtung $\Rightarrow$ muss bewiesen werden.

$$\begin{aligned}
& (x_1, y_1) = (x_2, y_2) \\
\Longrightarrow \quad & \Big\{\{x_1, y_1\}, \{x_1\}\Big\} = \Big\{\{x_2, y_2\}, \{x_2\}\Big\} \\
\Longrightarrow \quad & (\{x_1\} = \{x_2\} \text{ und } \{x_1, y_1\} = \{x_2, y_2\}) \quad \text{oder} \\
& (\{x_1\} = \{x_2, y_2\} \text{ und } \{x_2\} = \{x_1, y_1\}).
\end{aligned}$$

Wir betrachten diese zwei Fälle:
1. Fall:

$$\begin{aligned}
& \{x_1\} = \{x_2\} \text{ und } \{x_1, y_1\} = \{x_2, y_2\} \\
\Longrightarrow \quad & x_1 = x_2 \text{ und } y_1 \in \{x_2, y_2\} \text{ und } y_2 \in \{x_1, y_1\} \\
\Longrightarrow \quad & x_1 = x_2 \text{ und } (y_1 = x_2 = x_1 \text{ oder } y_1 = y_2) \text{ und } (y_2 = x_1 = x_2 \text{ oder } y_2 = y_1) \\
\Longrightarrow \quad & x_1 = x_2 \text{ und } y_1 = y_2.
\end{aligned}$$

2. Fall:

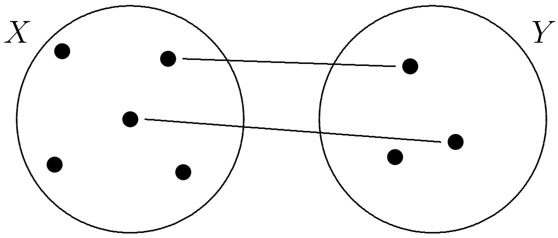
$$\begin{aligned}
& \{x_1\} = \{x_2, y_2\} \text{ und } \{x_2\} = \{x_1, y_1\} \\
\Longrightarrow \quad & x_1 = x_2 = y_2 = y_1.
\end{aligned}$$

1.6.4 Das kartesische Produkt Das *Kartesische Produkt* (René Descartes, fr, 1596 – 1650) der Mengen X und Y ist die Menge der durch die Elemente von X und die Elemente von Y gebildeten geordneten Paare:

$$X \times Y \;:=\; \Big\{(x, y) \Big| \, x \in X, y \in Y\Big\}.$$

1.6.5 Relationen Eine *Relation R zwischen X und Y* ist eine beliebige Teilmenge von $X \times Y$.

Gut kann man das mit Hilfe eines *Liniendiagramms* oder *Pfeildiagramms* veranschaulichen:



Zwischen einem Element $x \in X$ und einem Element $y \in Y$ wird genau dann eine Linie gezogen, wenn $(x, y) \in R$.

1.6.6 Spiegelrelation

Ist R eine Relation, so heißt

$$R^{-1} \;:=\; \Big\{(y, x) \;\Big|\; (x, y) \in R\Big\}$$

die zu R *gespiegelte* Relation oder *Spiegelrelation*.

1.6.7 Definition: Eigenschaften einer Relation

Eine Relation zwischen X und Y heißt

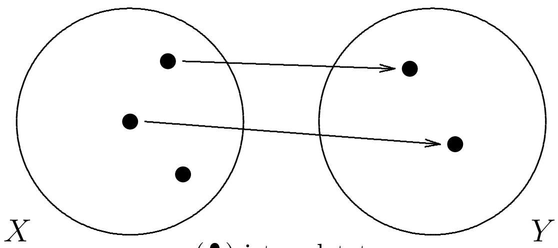
$$\left\{\begin{array}{l} (\clubsuit)\ \textit{links–total}, \\ (\spadesuit)\ \textit{rechts–eindeutig}, \\ (\heartsuit)\ \textit{rechts–total}, \\ (\diamondsuit)\ \textit{links–eindeutig}, \end{array}\right. \quad \text{wenn für jedes} \quad \left\{\begin{array}{l} x \in X \text{ mindestens ein } y \in Y \\ x \in X \text{ höchstens ein } y \in Y \\ y \in Y \text{ mindestens ein } x \in X \\ y \in Y \text{ höchstens ein } x \in X \end{array}\right.$$

existiert, so dass $(x, y) \in R$. Im Diagramm veranschaulicht heißt dies:

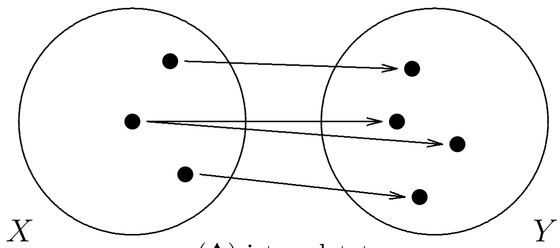
$$\text{In} \left\{\begin{array}{l} x \in X \text{ startet mindestens} \\ x \in X \text{ startet höchstens} \\ y \in Y \text{ endet mindestens} \\ y \in Y \text{ endet höchstens} \end{array}\right. \quad \text{ein Pfeil.}$$

(Sie müssen diese Begriffe nicht auswendig lernen.)

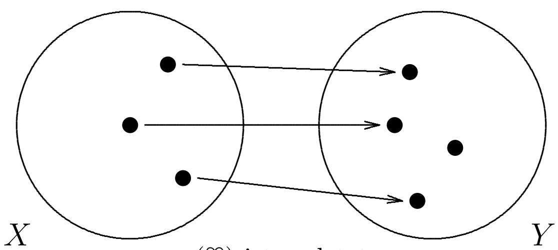
1.6.8 Diagramm: Bedingungen verletzt



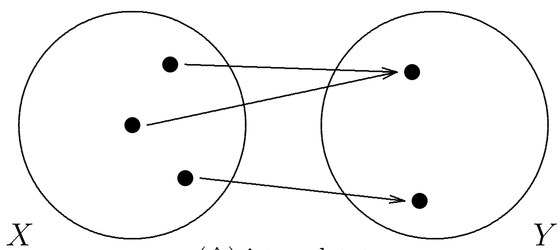
($\clubsuit$) ist verletzt



($\spadesuit$) ist verletzt



($\heartsuit$) ist verletzt

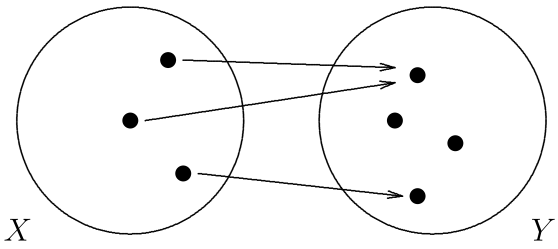


($\diamondsuit$) ist verletzt

1.7 Abbildungen

1.7.1 Definition: Abbildung

Eine Relation zwischen X und Y heißt *Abbildung von X nach Y*, wenn sie links–total (♣) und rechts–eindeutig (♠) ist.



1.7.2 Erläuterungen

- Eine Relation $R \subseteq X \times Y$ ist also genau dann eine Abbildung, wenn es zu jedem $x \in X$ genau ein $y \in Y$ gibt, so dass $(x, y) \in R$. Im Venn-Diagramm veranschaulicht heißt das, dass bei **jedem** Element $x \in X$ auf der linken Seite **genau ein** Pfeil nach rechts startet.
- Die beiden Begriffe ,,Abbildung" und *Funktion* sind synonym. In der Linearen Algebra ist der erste gebräuchlich.
- In diesem Zusammenhang heißt X *Definitionsmenge* und Y *Wertemenge* der Abbildung.
- Abbildungen werden oft mit kleinen Buchstaben bezeichnet: $f, g, h, \ldots$

1.7.3 Veranschaulichende Fassung des Abbildungsbegriffs

Die soeben gegebene Definition des Begriffs ,,Abbildung" ist mathematisch befriedigend, für das praktische Arbeiten aber zu abstrakt, umständlich und zu statisch. Oft ist daher eine andere Beschreibung des Begriffs Abbildung anzutreffen, die nicht in der Mengenlehre verankert ist. Sie unterstreicht den eher dynamischen Charakter dieses Begriffs:

Es seien zwei Mengen X und Y gegeben. Eine Funktion von X nach Y ist eine Vorschrift, die **jedem** $x \in X$ **genau ein** $y \in Y$ zuordnet. Dies wird auch in einer gänzlich veränderten Notation deutlich:

$$f : \begin{cases} X & \to & Y \\ x & \mapsto & f(x) \end{cases}$$

$f(x)$ ist dabei ein irgendwie gearteter mathematisch sinnvoller Ausdruck (Term, Textdefinition, auch per Fallunterscheidung,...), der das ,,genau ein" sicherstellen muss.

1.7.4 Graph einer Abbildung

Geht man von der veranschaulichenden Beschreibung von ,,Abbildung" aus, so wird die zugehörige Relation oft als Graph G_f der Abbildung bezeichnet:

$$G_f \;:=\; \Big\{ (x, y) \in X \times Y \;\Big|\; y = f(x) \Big\}.$$

1.7.5 Zuordnung von Teilmengen Auch Teilmengen $X' \subseteq X$ bzw. $Y' \subseteq Y$ werden durch eine Funktion $f : X \to Y$ zugeordnet:

$$\begin{aligned} f(X') &:= \Big\{ y \in Y \;\Big|\; \text{Es ex. } x \in X' \text{ mit } f(x) = y \Big\} \\ f^{-1}(Y') &:= \Big\{ x \in X \;\Big|\; f(x) \in Y' \Big\} \end{aligned}$$

Die Menge $f(X)$ heißt *Bild(–menge)* der Funktion f. Unterscheide Bild- und Wertemenge!

1.7.6 Beispiel Ist

$$\begin{cases} f : & \mathbb{R} \to \mathbb{R} \\ & x \mapsto x^2 \end{cases}$$

die Quadratfunktion, so ist

$$\begin{aligned} f([-2,5]) &= [0,25] \\ f^{-1}([1,7]) &= [-\sqrt{7},-1] \cup [1,\sqrt{7}] \end{aligned}$$

1.7.7 Identische Abbildung Ist X eine Menge, so heißt die Abbildung (Begründung)

$$\mathrm{id}_X := \Big\{ (x,x) \in X \times X \;\Big|\; x \in X \Big\}$$

die *identische Abbildung* oder *Identität auf* X. Innerhalb der Zuordnungsauffassung schreibt man oft kurz $x \mapsto x$.

1.7.8 Komposition von Abbildungen Sind $f : X \to Y$ und $g : Y \to Z$ Abbildungen, so heißt die Abbildung (Begründung)

$$g \circ f := \Big\{ (x,z) \in X \times Z \;\Big|\; \text{Es ex. } y \in Y \text{ mit } f(x) = y \text{ und } g(y) = z \Big\}$$

die *Hintereinanderausführung* oder *Komposition* der Abbildungen f und g. Da f eine Abbildung ist, ist das y in der Definition eindeutig bestimmt.

Innerhalb der Zuordnungsauffassung schreibt man $x \mapsto (g \circ f)(x) = g(f(x))$. Im Pfeil-Diagramm kann dies so veranschaulicht werden:

$$\begin{array}{ccccc} & \overbrace{\hphantom{\xrightarrow{\quad f \quad} \; Y \; \xrightarrow{\quad g \quad}}}^{g \circ f} & & & \\ X & \xrightarrow{\quad f \quad} & Y & \xrightarrow{\quad g \quad} & Z \\ x & \longmapsto & f(x) & \longmapsto & g(f(x)) \end{array}$$

Ohne Beweis halten wir fest, dass für die Komposition von Abbildungen das Assoziativgesetz gilt. Sind $f : X \to Y$, $g : Y \to Z$ und $h : Z \to W$ drei Abbildungen, so gilt

$$(f \circ g) \circ h = f \circ (g \circ h) \quad : \quad X \to W$$

1.7.9 Beispiel Bei Komposition der beiden Funktionen

$$f : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2, \end{cases} \qquad g : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x+1 \end{cases}$$

entstehen die beiden Funktionen

$$g \circ f : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2+1, \end{cases} \qquad f \circ g : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & (x+1)^2. \end{cases}$$

1.7.10 Definition und Satz: Injektive Abbildungen

Für eine Abbildung $f : X \to Y$ sind die folgenden Aussagen äquivalent:

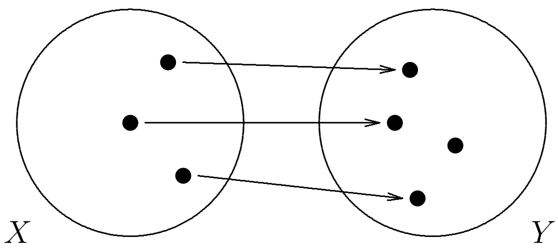
(A) (Def) Die Abbildung heißt *injektiv*.

(B) Als Relation ist f links-eindeutig.

(C) Zu jedem $y \in Y$ gibt es höchstens ein $x \in X$ mit $f(x) = y$.

(D) Im Venn-Diagramm: Bei jedem $y \in Y$ endet höchstens ein Pfeil.

(E) Es existiert eine Abbildung $g : Y \to X$, so dass $g \circ f = \mathrm{id}_X$ (Links-Inverse).



1.7.11 Beweis Die Aussagen (B) – (D) sind nur Umformulierungen des jeweils gleichen Sachverhalts.

Wir beweisen die Implikation $(C) \Rightarrow (E)$: Fixiere dazu ein $a \in X$ und definiere die Funktion g durch

$$g(y) \;:= \begin{cases} x, & \text{falls } x \text{ (dann wegen (C) eindeutig) existiert, so dass } f(x) = y, \\ a, & \text{sonst.} \end{cases}$$

Für alle $x \in X$ gilt dann $g(f(x)) = x$.

Wir beweisen die Implikation $(E) \Rightarrow (C)$: Es seien $x_1, x_2 \in X$ beliebig mit $f(x_1) = f(x_2)$. Dann gilt aufgrund der Eigenschaft (E):

$$x_1 \;=\; g(f(x_1)) = g(f(x_2)) = x_2.$$

Also ist f injektiv.

1.7.12 Definition und Satz: Surjektive Abbildungen

Für eine Abbildung $f : X \to Y$ sind die folgenden Aussagen äquivalent:

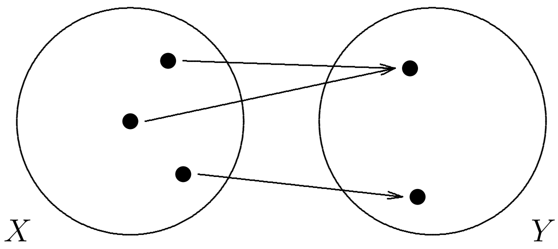
(A) (Def) Die Abbildung heißt *surjektiv*.

(B) Als Relation ist f rechts-total.

(C) Zu jedem $y \in Y$ gibt es mindestens ein $x \in X$ mit $f(x) = y$.

(D) Im Venn-Diagramm: Bei jedem $y \in Y$ endet mindestens ein Pfeil.

(E) Es existiert eine Abbildung $g : Y \to X$, so dass $f \circ g = \mathrm{id}_Y$ (Rechts-Inverse).



1.7.13 Beweis Die Aussagen (B) – (D) sind nur Umformulierungen des jeweils gleichen Sachverhalts.

Wir beweisen die Implikation $(C) \Rightarrow (E)$:

Zu jedem $y \in Y$ wähle ein $x \in X$, so dass $f(x) = y$. Es gibt mindestens ein solches x, da f surjektiv. Definiere g durch $g(y) = x$. Dann gilt für alle $y \in Y$: $f(g(y)) = f(x) = y$.

Wir beweisen die Implikation $(E) \Rightarrow (C)$: Sei $y \in Y$. Dann existiert zu jedem $y \in Y$ ein x, nämlich $x = g(y)$, so dass

$$f(x) \quad = \quad f(g(y)) = y.$$

Also ist f surjektiv.

1.7.14 Definition und Satz: Bijektive Abbildungen

Für eine Abbildung $f : X \to Y$ sind die folgenden Aussagen äquivalent:

(A) (Def) Die Abbildung heißt *bijektiv* (oder *invertierbar* oder *umkehrbar*).

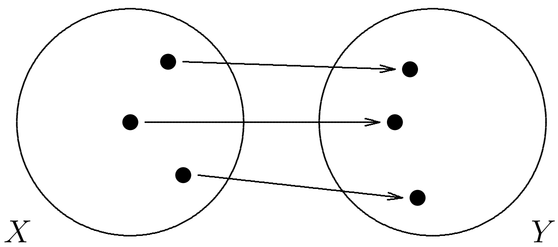
(B) Die Abbildung ist injektiv und surjektiv.

(C) Als Relation ist f links-eindeutig und rechts-total.

(D) Zu jedem $y \in Y$ gibt es genau ein $x \in X$ mit $f(x) = y$.

(E) Im Venn-Diagramm: Bei jedem $y \in Y$ endet genau ein Pfeil.

(F) Es existiert eine Abbildung $g : Y \to X$, so dass $f \circ g = \mathrm{id}_Y$ und $g \circ f = \mathrm{id}_X$.



1.7.15 Beweis Die Aussagen (A) bis (F) fassen nur die entsprechenden Aussagen über injektive bzw. surjektive Abbildungen zusammen.

1.7.16 Definition: Umkehrabbildung Die in (E) angegebene Abbildung ist durch die im Satz angegebenen Eigenschaften eindeutig bestimmt, sie heißt die *Umkehrabbildung* und wird mit dem Symbol f^{-1} angegeben. Als Relation ist f^{-1} die Spiegelrelation zu f.

Zusammengefasst haben wir also die beiden Abbildungen

$$f : \begin{cases} X & \to & Y \\ x & \mapsto & f(x) \end{cases} \qquad f^{-1} : \begin{cases} Y & \to & X \\ y & \mapsto & f^{-1}(y) \end{cases}$$

die durch die Eigenschaften

$$f^{-1} \circ f \;=\; \mathrm{id}_X \qquad f \circ f^{-1} = \mathrm{id}_Y$$

aufeinander bezogen sind.

1.7.17 Beispiel Abhängig von Definitions- und Wertemenge weist die aus der Schule bekannte Quadratfunktion $x \mapsto x^2$ die folgenden Eigenschaften auf:

	surjektiv	injektiv	bijektiv
$\mathbb{R} \to \mathbb{R}$	–	–	–
$\mathbb{R} \to \mathbb{R}_0^+$	✓	–	–
$\mathbb{R}_0^+ \to \mathbb{R}$	–	✓	–
$\mathbb{R}_0^+ \to \mathbb{R}_0^+$	✓	✓	✓

Im Fall der letzten Zeile sind Funktion und Umkehrfunktion gegeben durch:

$$f : \begin{cases} \mathbb{R}_0^+ & \to & \mathbb{R}_0^+ \\ x & \mapsto & x^2 \end{cases} \qquad f^{-1} : \begin{cases} \mathbb{R}_0^+ & \to & \mathbb{R}_0^+ \\ x & \mapsto & \sqrt{x}. \end{cases}$$

1.7.18 Bemerkungen

1. Die Äquivalenzen (A) $\Leftrightarrow$ (B) $\Leftrightarrow$ (F) zeigen, dass man die Umkehrbarkeit einer Abbildung dadurch beweisen kann, dass man Injektivität und Surjektivität zeigt. Die Umkehrabbildung muss nicht angegeben werden.

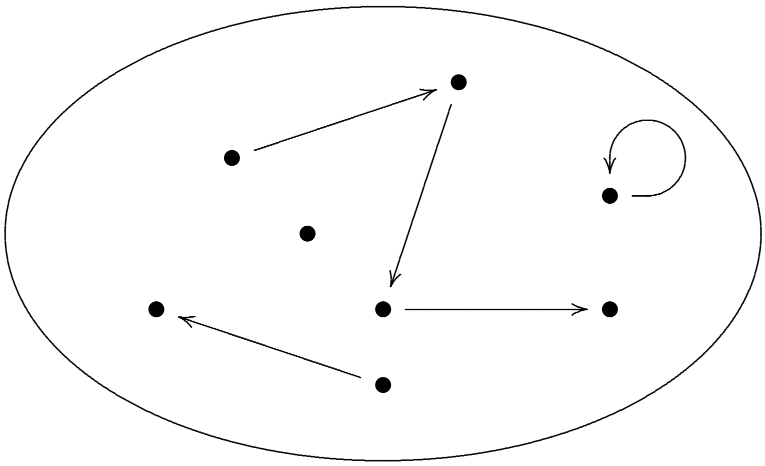
2. Die Aussage (F) zeigt, dass die Umkehrabbildung f^{-1} einer umkehrbaren Abbildung bei beidseitiger Komposition mit der Originalabbildung f die Identität hervorbringt.

1.8 Relationen auf einer Menge

1.8.1 Definition Eine *Relation* ***auf einer*** *Menge* X ist eine Relation zwischen X und X, also eine beliebige Teilmenge von $X \times X$.

1.8.2 Veranschaulichung

Eine Relation auf einer endlichen Menge X kann dadurch veranschaulicht werden, dass die Menge als Venn-Diagramm gezeichnet wird,



und die Tatsache $(x, y) \in R$ durch einen Pfeil von x nach y dargestellt wird. Beachte, dass Linien in diesem Fall nicht ausreichen, da dann eine Unterscheidung $(x, y) \in R$ oder $(y, x) \in R$ nicht möglich wäre.

1.8.3 Eigenschaften von Relationen auf einer Menge

Wir listen mögliche Eigenschaften von solchen Relationen auf:

Die Relation heißt ...	wenn ...	Diagramm-Beschreibung
reflexiv	für alle $x \in X$ gilt: $(x, x) \in R$	Von jedem Punkt führt ein Pfeil zu sich selbst.
transitiv	für alle $x, y, z \in X$ gilt: $(x, y) \in R$ und $(y, z) \in R \Rightarrow (x, z) \in R$	Wenn eine Pfeilkette von x über y nach z führt, dann gibt es einen direkten Pfeil von x nach z
symmetrisch	für alle $x, y \in X$ gilt: $(x, y) \in R \Rightarrow (y, x) \in R$	Wenn ein Pfeil von x nach y führt, dann führt auch ein Pfeil von y nach x.
antisymmetrisch	für alle $x, y \in X$ mit $x \neq y$ gilt: $(x, y) \in R \Rightarrow (y, x) \notin R$	Wenn ein Pfeil von x nach $y \neq x$ führt, dann führt kein Pfeil von y nach x.
total	für alle $x, y \in X$ mit $x \neq y$ gilt: $(x, y) \in R$ oder $(y, x) \in R$	Zwischen x und $y \neq x$ muss mindestens ein Pfeil existieren
Äquivalenzrelation	sie reflexiv, transitiv und symmetrisch ist	
Halbordnung	sie reflexiv, transitiv und antisymmetrisch ist	
lineare (= totale) Ordnung	sie eine Halbordnung und total ist	

Ist R eine Halbordnung, so benutzt man die viel suggestiveren Schreibweisen

$$\begin{array}{rcccc} (x, y) \in R & \Longleftrightarrow & x \preceq y & \Longleftrightarrow & y \succeq x \\ (x, y) \in R \text{ und } x \neq y & \Longleftrightarrow & x \prec y & \Longleftrightarrow & y \succ x. \end{array}$$

Je nach Konkretisierung treten ähnliche andere Zeichen $(\leq, \subseteq, \sqsubseteq, \trianglelefteq, \dots)$ auf. Die Ausschließung der Gleichheit, wie sie in der zweiten Zeile angegeben ist, wird durch Wörter wie „echt”, „streng” oder „strikt” umschrieben.

1.8.4 Beispiele

$$R_1 = \Big\{(x,y) \in \mathbb{Q} \times \mathbb{Q} \,\Big|\, x \le y\Big\}$$

$$R_2 = \Big\{(x,y) \in \mathbb{Q} \times \mathbb{Q} \,\Big|\, x < y\Big\}$$

$$R_3 = \Big\{(x,y) \in \mathbb{N} \times \mathbb{N} \,\Big|\, x|y\Big\} \qquad \text{(ist Teiler von)}$$

$$R_4 = \Big\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \,\Big|\, x = y \bmod k\Big\},$$

Dabei ist k eine fest gewählte Zahl in $\mathbb{N}$. $x = y \bmod k$ bedeutet:
x und y haben bei der Division durch k den gleichen Rest.

$$R_5 = \Big\{(X,Y) \in \mathcal{P}(M) \times \mathcal{P}(M) \,\Big|\, X \subseteq Y\Big\}, \qquad (M \text{ ist eine beliebige Menge})$$

$$R_6 = \Big\{(x,y) \in X \times X \,\Big|\, x \text{ parallel zu } y\Big\}, \qquad X = \{\text{Geraden in der Zeichenebene}\},$$

$$R_7 = \Big\{(x,y) \in H \times H \,\Big|\, x \text{ ist nicht jünger als } y\Big\},$$

(H ist die Menge der Gäste auf einer Hochzeit),

$$R_8 = \Big\{(x,y) \in H \times H \,\Big|\, x = y \text{ oder } x \text{ ist mit } y \text{ verheiratet}\Big\},$$

$$R_9 = \Big\{(x,y) \in H \times H \,\Big|\, x = y \text{ oder } x \text{ ist ein Ahne von } y\Big\},$$

$$R_{10} = \Big\{(x,y) \in H \times H \,\Big|\, x \text{ ist ,,Elter'' von } y\Big\},$$

$$R_{11} = \Big\{(x,y) \in H \times H \,\Big|\, x \text{ und } y \text{ haben Vater und Mutter gemeinsam}\Big\},$$

$$R_{12} = \Big\{(x,y) \in H \times H \,\Big|\, x \text{ und } y \text{ haben Vater oder Mutter gemeinsam}\Big\}.$$

	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}
re	$\surd$		$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$		$\surd$	$\surd$
tr	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$		$\surd$	
sy				$\surd$		$\surd$		$\surd$			$\surd$	$\surd$
as	$\surd$	$\surd$	$\surd$		$\surd$		$\surd$		$\surd$	$\surd$		
to	$\surd$	$\surd$					$\surd$					
ÄR				$\surd$		$\surd$		$\surd$			$\surd$	
HO	$\surd$		$\surd$		$\surd$		$\surd$		$\surd$			
LO	$\surd$						$\surd$					

1.9 Peano-Axiome und vollständige Induktion

1.9.1 Peano-Axiome Die Peano–Axiome legen die Eigenschaften der natürlichen Zahlen — ebenfalls in der Sprache und in dem System der Mengenlehre — beschreibend fest. Die Frage der Existenz einer solchen Menge bleibt dabei hier unbeantwortet. Tatsächlich lassen sich die Peano-Axiome aus tiefer liegenden Axiomen der Mengenlehre herleiten.

1.9.2 Definition: Die Menge der natürlichen Zahlen

Eine Menge $\mathbb{N}$ heißt *Menge der natürlichen Zahlen*, wenn eine Abbildung $\nu : \mathbb{N} \to \mathbb{N}$ (Nachfolger–Abbildung) existiert mit folgenden Eigenschaften:

P1 Es existiert genau eine Zahl in $\mathbb{N}$, die nicht im Bild von ν enthalten ist.

P2 Die Abbildung ν ist injektiv.

P3 Gilt für eine Teilmenge $A \subseteq \mathbb{N}$

$$1 \in A \text{ und } \Big(x \in A \Rightarrow \nu(x) \in A\Big),$$

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

Die eigentliche Bedeutung dieser drei Peano-Axiome offenbart sich in dem folgenden

1.9.3 Satz: Beweis-Prinzip der vollständigen Induktion

Es sei $\mathcal{A}(n)$ für jedes $n \in \mathbb{N}$ eine Aussage. Dann gilt das folgende *Prinzip der vollständigen Induktion*:

WENN $\mathcal{A}(1)$ wahr ist

UND für alle $n \in \mathbb{N}$ die Implikation $\mathcal{A}(n) \Rightarrow \mathcal{A}(n+1)$ gilt,

DANN ist $\mathcal{A}(n)$ wahr für alle $n \in \mathbb{N}$.

Die Aussage $\mathcal{A}(1)$ in der ersten Zeile heißt in diesem Zusammenhang auch *Induktionsanfang*. Die Aussage $\mathcal{A}(n)$ in der zweiten Zeile heißt *Induktionsvoraussetzung* oder *Induktionsannahme*. Die Implikation in der zweiten Zeile wird als *Induktionsschritt* oder *Induktionsschluss* bezeichnet.

Entscheidend an diesem Prinzip ist die Tatsache, dass unendlich viele Aussagen durch zwei Aussagen ,,mathematisch dingfest" gemacht sind.

1.9.4 Beweis Wende einfach die Peano–Eigenschaft P3 auf die Teilmenge

$$A \;=\; \{n \in \mathbb{N} \mid \mathcal{A}(n) \text{ ist wahr } \}$$

an.

1.9.5 Beispiel: Summe ungerader Zahlen

Wir zeigen mit Hilfe der vollständigen Induktion, dass für alle $n \in \mathbb{N}$

$$\mathcal{A}(n) \qquad 1 + 3 + 5 + \cdots + (2n-1) \;=\; n^2.$$

Induktionsanfang: Die Aussage ist wahr für $n = 1$, da

$$1 \;=\; 1^2.$$

Induktionsschluss: Wir nehmen jetzt an, dass die Aussage für ein (fixiertes) $n \in \mathbb{N}$ wahr ist und wollen daraus folgern, dass sie auch für $n+1$ wahr ist. Das geht so:

$$\begin{aligned}
& 1 + 3 + 5 + \cdots + (2(n+1)-1) \\
\text{(Abspaltung des letzten Summanden)} \quad = \;& 1 + 3 + 5 + \cdots + (2n-1) + (2n+1) \\
\text{(Induktionsvoraussetzung)} \quad = \;& n^2 + (2n+1) \\
\text{(Binomische Plus-Formel)} \quad = \;& (n+1)^2
\end{aligned}$$

Das ist genau die Aussage $\mathcal{A}(n+1)$.

Weitere hunderte Beispiele folgen — in Ihrer Mathematik-Ausbildung.

1.9.6 Prinzip der Rekursiven Definition

Mathematische Objekte M_n können für alle $n \in \mathbb{N}$ dadurch definiert werden, dass

1. das Objekt M_1 definiert wird und
2. für jedes $n \in \mathbb{N}$ angegeben wird, wie das Objekt M_{n+1} bei bekanntem M_n definiert ist.

Eine ,,Begründung” besteht darin, dass man das Axiom P3 auf die Teilmenge

$$A' \;=\; \{n \in \mathbb{N} | M_n \text{ ist definiert } \}$$

anwendet.

Immer, wenn in mathematischen Formeln die ominösen Dreipünktchen auftauchen, steckt eigentlich eine rekursive Definition dahinter.

1.9.7 Bemerkung Die beiden Prinzipien 1.9.3 und 1.9.6 können — entsprechend modifiziert — auch bei Zugrundelegung anderer Teilmengen von $\mathbb{Z}$ angewandt werden.

Beispiele zur vollständigen Induktion sind

$\mathbb{N}_0$ Der Induktionsanfang erfolgt bei $n = 0$ anstatt bei $n = 1$.

$\mathbb{N}_{\geq N}$ Der Induktionsanfang erfolgt bei einer fixierten natürlichen Zahl N anstatt bei $n = 1$.

$\mathbb{N}_{\leq N}$ Der Induktionsanfang erfolgt bei einer fixierten natürlichen Zahl N anstatt bei $n = 1$. Es wird dann der Induktionsschritt in Gegenrichtung $\mathcal{A}(n) \Rightarrow \mathcal{A}(n-1)$ durchgeführt.

$2\mathbb{N}$ Um Aussagen $\mathcal{A}(n)$ für alle geraden Zahlen inkl. Null zu beweisen, wird der Induktionsanfang $\mathcal{A}(0)$ und dann der Induktionsschritt $\mathcal{A}(n) \Rightarrow \mathcal{A}(n+2)$ gezeigt.

1.10 Beispiele

1.10.1 Definition: n-Tupel Wir definieren rekursiv höhere n–*Tupel*. Es sei für jedes $n \in \mathbb{N}$ eine Menge X_n und ein Element $x_n \in X_n$ gegeben. Definiere rekursiv

$$\begin{aligned} (x_1) &:= x_1 \\ (x_1, x_2, \ldots, x_n, x_{n+1}) &:= ((x_1, x_2, \ldots, x_n), x_{n+1}). \end{aligned}$$

Die Menge aller n-Tupel wird dann mit $X_1 \times \ldots \times X_n$ bezeichnet.

Wenn alle Mengen übereinstimmen,

$$X = X_1 = \cdots = X_n,$$

so schreibt man kürzer

$$X^n = \underbrace{X \times X \times \ldots \times X}_{n \text{ Faktoren im kartesischen Produkt}} .$$

1.10.2 Summenschreibweise Es sei für jedes $k \in \{1, \ldots, n\}$ eine Zahl a_k gegeben. Dann sind durch

$$S_1 = a_1, \qquad S_{k+1} = S_k + a_{k+1}$$

die abschnittsweisen Summen definiert. Um den Aufwand in der Definition geringer zu halten, schreibt man kürzer und suggestiver:

$$S_n = a_1 + a_2 + \cdots + a_n \quad \text{oder} \quad S_n = \sum_{k=1}^{n} a_k.$$

1.10.3 Gauß'sche Summenformel Wir definieren

$$s_0 = 0, \qquad s_{k+1} = (k+1) + s_k$$

für $k \in \mathbb{N}_0$, das heißt also

$$s_n = n + (n-1) + \cdots + 1 = \sum_{k=0}^{n} k.$$

Wir zeigen durch Induktion:

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

Induktionsanfang: $s_0 = 0 = \frac{0 \cdot 1}{2}$

Induktionsschluss: Wir nehmen an, dass die Behauptung für $n \geq 2$ gezeigt ist. Dann gilt:

$$\begin{aligned} s_{n+1} &\overset{\text{def}}{=} (n+1) + s_n \overset{\text{IndV}}{=} (n+1) + \tfrac{n \cdot (n+1)}{2} \\ &= \tfrac{2(n+1) + n \cdot (n+1)}{2} = \tfrac{(n+2) \cdot (n+1)}{2} = \tfrac{(n+1) \cdot (n+2)}{2}. \end{aligned}$$

Also gilt die Behauptung auch für $n+1$.

Nach dem Induktionsprinzip ist die Aussage für alle $n \in \mathbb{N}_0$ richtig.

1.10.4 Geometrische Summe Für ein beliebiges $q \in \mathbb{Q} \setminus \{1\}$ gilt:

$$\sum_{k=0}^{n} q^k = 1 + q + q^2 + \cdots + q^n = \tfrac{1-q^{n+1}}{1-q}.$$

Beweis durch Induktion über n:

Induktionsanfang:

$$\sum_{k=0}^{0} q^k = q^0 = 1 = \tfrac{1-q^{0+1}}{1-q}$$

Induktionsschritt: Wir nehmen an, dass die Aussage für n gezeigt ist.

$$\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1} \overset{\text{IndV}}{=} \tfrac{1-q^{n+1}}{1-q} + q^{n+1} = \tfrac{1-q^{n+1}+(1-q)q^{n+1}}{1-q} = \tfrac{1-q^{n+2}}{1-q}.$$

1.10.5 Beispiel Wir beweisen durch Induktion, dass die Summe der ersten n Quadratzahlen gegeben ist durch

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

Induktionsanfang:

$$\sum_{k=0}^{0} k^2 = 0^2 = 0 = \tfrac{0(0+1)(2\cdot 0+1)}{6}.$$

Induktionsschritt: Wir nehmen an, dass die Aussage für n gezeigt ist. Dann folgt:

$$\begin{aligned}\sum_{k=0}^{n+1} k^2 &= \sum_{k=0}^{n} k^2 + (n+1)^2 \overset{\text{IndV}}{=} \tfrac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1)\cdot\frac{n(2n+1)+6(n+1)}{6} = (n+1)\cdot\frac{2n^2+7n+6}{6} \\ &= (n+1)\cdot\frac{(n+2)(2n+3)}{6} = \frac{(n+1)(n+2)(2(n+1)+1)}{6}.\end{aligned}$$

Die gesamte Gleichungskette zeigt auf, dass die Aussage für $n+1$ gezeigt ist.

1.10.6 Definition: Potenzfunktion

Für festes $n \in \mathbb{Z}$ und $a \neq 0$ ist die Potenzfunktion

$$\uparrow \begin{cases} \mathbb{Q} & \to & \mathbb{Q} \\ a & \mapsto & a^n \end{cases}$$

durch

$$a^0 = 1, \qquad a^{n+1} = a \cdot a^n, \qquad a^{n-1} = \tfrac{1}{a} \cdot a^n$$

(in beide Richtungen) rekursiv definiert. Mit Hilfe der Pünktchen kann man diese Definition auch suggestiver schreiben als

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ Faktoren}}, \quad n \in \mathbb{N}, \qquad a^n = \frac{1}{\underbrace{a \cdot a \cdot \ldots \cdot a}_{|n| \text{ Faktoren}}}, \quad n \in -\mathbb{N}.$$

Es gilt dann für $m, n \in \mathbb{Z}$:

$$a^m \cdot a^n = a^{m+n}, \qquad (a^m)^n = a^{m \cdot n}.$$

1.10.7 Produktschreibweise Es sei für jedes $k \in \{1, \ldots, n\}$ eine Zahl a_k gegeben. Dann sind durch

$$P_1 = a_1, \qquad P_{k+1} = a_{k+1} \cdot P_k$$

die abschnittsweisen Produkte rekursiv definiert.

Ähnlich wie bei Summen gibt es die Schreibweise

$$\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdot \ldots \cdot a_k.$$

1.10.8 Definition: Fakultäts-Funktion

Die Fakultät einer natürlichen Zahl ist als Funktion definiert

$$\begin{cases} \mathbb{N}_0 & \to & \mathbb{N} \\ n & \mapsto & n! \end{cases}$$

so rekursiv definiert:

$$0! = 1, \qquad (n+1)! = (n+1) \cdot n! \quad \text{für alle } n \geq 1.$$

Suggestiver:

$$n! = n \cdot (n-1) \cdot \ldots \cdot 1 = \prod_{k=1}^{n} k.$$

1.10.9 Definition: Binomialkoeffizienten

Wir definieren für zwei Zahlen $n \in \mathbb{N}_0, k \in \mathbb{Z}$, den *Binomialkoeffizienten*

$$\binom{n}{k} := \begin{cases} \frac{n!}{k!(n-k)!}, & \text{falls } 0 \leq k \leq n, \\ 0, & \text{falls } k > n \text{ oder } k < 0. \end{cases}$$

1.10.10 Satz: Eigenschaften der Binomialkoeffizienten

Wir notieren gleich zwei wichtige Eigenschaften: Für $n \in \mathbb{N}_0$ und $k \in \mathbb{Z}$ gilt

$$\binom{n}{k} = \binom{n}{n-k} \qquad \text{(Symmetrie bzgl. } k = \tfrac{n}{2})$$

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \qquad \text{(Pascal–Beziehung)}$$

1.10.11 Beweis Da für $k \notin \{0, \ldots, n\}$ die erste Beziehung trivial ist, braucht sie nur noch für den anderen Fall $0 \leq k \leq n$ überprüft zu werden:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)![n-(n-k)]!} = \binom{n}{n-k}.$$

Für $1 \leq k \leq n-1$ rechnen wir die zweite Beziehung so nach:

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= n! \cdot \frac{(n-k+1)+k}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}. \end{aligned}$$

Die Fälle $k = 0$ und $k = n$ sind leicht zu testen:

$$\begin{aligned} \binom{n}{0} + \binom{n}{-1} &= 1 + 0 = 1 = \binom{n+1}{0} \\ \binom{n}{n} + \binom{n}{n-1} &= 1 + n = \binom{n+1}{n}. \end{aligned}$$

In den anderen Fälle $k < 0$ oder $k > n$ sind alle in der Beziehung auftretenden Ausdrücke gleich 0.

1.10.12 Bemerkung: Pascalsches Dreieck Man kann die Binomialkoeffizienten im sogenannten Pascal'schen Dreieck anordnen. Die zweite Beziehung des Satzes besagt, dass sich ein Binomialkoeffizient als Summe der beiden über ihm stehenden ergibt.

$$\begin{array}{ccccccccccccc} &&&&&& 1 &&&&&& \\ &&&&& 1 && 1 &&&&& \\ &&&& 1 && 2 && 1 &&&& \\ &&& 1 && 3 && 3 && 1 &&& \\ && 1 && 4 && 6 && 4 && 1 && \\ & 1 && 5 && 10 && 10 && 5 && 1 & \\ 1 && 6 && 15 && 20 && 15 && 6 && 1 \\ && \vdots &&&& \vdots &&&& \vdots && \end{array}$$

1.11 Mächtigkeit von Mengen

1.11.1 Definitionen

- Zwei Mengen X, Y heißen *gleichmächtig*, wenn eine bijektive Abbildung $X \to Y$ existiert.
- Es sei $n \in \mathbb{N}$. Besteht zwischen einer Menge X und der Menge $\{1, 2, 3, \dots, n\}$ eine bijektive Abbildung, so sagt man: Die Menge X ...
  - hat die *Mächtigkeit* n oder
  - die *Anzahl* der Elemente ist n oder
  - ist eine n–Menge.

  Es sind verschiedene Symbole dafür im Gebrauch: $\#(X) = \text{card}(X) = |X| = n$.
- Die leere Menge hat die *Mächtigkeit* 0.
- Eine Menge der Mächtigkeit n, $n \in \mathbb{N}_0$, heißt *endlich*.
- Eine Menge, die nicht endlich ist, heißt *unendlich*.
- Besteht zwischen einer Menge X und der Menge $\mathbb{N}$ eine bijektive Abbildung, so sagt man, dass die Menge X *abzählbar unendlich* ist.
- Eine Menge heißt *(höchstens) abzählbar*, wenn sie endlich oder abzählbar unendlich ist.
- Eine Menge, die nicht abzählbar ist, heißt *überabzählbar*.

1.11.2 Satz: Arithmetik mit endlichen Mengen Wenn X und Y endlich sind, gelten die elementaren Beziehungen

$$\begin{aligned}
|X \cup Y| &= |X| + |Y|, && \text{falls } X \cap Y = \varnothing \\
|X \setminus Y| &= |X| - |Y|, && \text{falls } Y \subseteq X, \\
|X \cup Y| + |X \cap Y| &= |X| + |Y| \\
|X \times Y| &= |X| \cdot |Y|
\end{aligned}$$

1.11.3 Beweis Zum Beweis der ersten Beziehung müssen wir genau die Definition einer endlichen Mächtigkeit als Bijektion zu einem endlichen Anfangsintervall der natürlichen Zahlen heranziehen. Im Fall $|X| = n$, $|Y| = m$ bestehen die bijektive Abbildungen

$$\begin{aligned}
X &\leftrightarrow \{1, \dots, n\}, \\
Y &\leftrightarrow \{1, \dots, m\} \leftrightarrow \{n+1, \dots, n+m\},
\end{aligned}$$

die sich zu einer bijektiven Abbildung

$$X \cup Y \leftrightarrow \{1, \dots, n, n+1, \dots, n+m\}$$

zusammensetzen lassen. Die zweite Beziehung ist eine ,,Umdeutung" der ersten:

$$|X \setminus Y| + |Y| = |(X \setminus Y) \cup Y| = |X|.$$

Weiter ist

$$\begin{aligned} |X \cup Y| &= |(X \setminus Y) \cup (Y \setminus X) \cup (X \cap Y)| \\ &= (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) + |X \cap Y| \\ &= |X| + |Y| - |X \cap Y| \end{aligned}$$

Zum Beweis der letzten Beziehung nehmen wir an, dass

$$X = \{x_1, \ldots, x_n\}, \qquad |Y| = m.$$

Dann können wir wie folgt eine disjunkte Vereinigung aufschreiben:

$$X \times Y = \{(x,y) | x \in X, y \in Y\} = \{(x_1, y) | y \in Y\} \cup \cdots \cup \{(x_n, y) | y \in Y\}$$

Deshalb

$$|X \times Y| = \underbrace{m + \cdots + m}_{n \text{ Summanden}} = n \cdot m.$$

Die letzte Gleichheit müssten wir eigentlich auch noch genauer unter die Lupe nehmen. Wir wollen uns aber nicht zu sehr in diese Feinheiten verlieren und beschränken uns auf den Hinweis, dass das Distributivgesetz diese Beziehung absichert.

1.11.4 Satz: Mächtigkeit der Potenzmenge

Es sei X eine Menge mit n Elementen, $n \in \mathbb{N}_0$.

(i) Es sei $0 \leq k \leq n$. Die Anzahl der k–Teilmengen von X ist gleich $\binom{n}{k}$.

$$\left| \left\{ Y \in \mathcal{P}(X) \middle| |Y| = k \right\} \right| = \binom{n}{k}.$$

(ii) Die Anzahl aller Teilmengen von X ist gleich 2^n:

$$\left| \mathcal{P}(X) \right| = 2^n.$$

1.11.5 Beweis Wir fixieren $k \in \mathbb{N}_0$ und führen eine Induktion über $n \geq k$ durch.

Induktionsanfang: Für $n = 0$ ist die Behauptung klar: Eine k–elementige Menge X (es ist dann die leere Menge) besitzt genau eine k–Teilmenge Y, nämlich sich selbst:

$$Y = X = \varnothing$$

und es ist ja in diesem Fall: $1 = \binom{n}{k}$.

Induktionsschluss: Es sei X eine Menge mit $n+1$ Elementen. Wir dürfen die Aussage des Satzes für n als bewiesen voraussetzen. Wir wählen ein Element z aus X und schreiben X als

$$X = \{x_1, x_2, \ldots, x_n, z\}.$$

Wie viele k–Teilmengen besitzt X?

1. Fall: Für $k = n+1$ ist die Frage leicht zu beantworten: $1 = \binom{n+1}{n+1}$.

2. Fall: Es sei also $0 \leq k \leq n$. Wit zählen getrennt die k–Teilmengen Y von X, ...

- die z enthalten: Diese haben genau die Form

  $$Y = X' \cup \{z\},$$

  wobei X' eine $(k-1)$–Teilmenge von X ist. Davon gibt es gemäß Induktionsvoraussetzung $\binom{n}{k-1}$ Stück.

- und die, die z nicht enthalten: Das sind genau die k–Teilmengen von $\{x_1, \ldots, x_n\}$. Nach Induktionsvoraussetzung sind dies $\binom{n}{k}$ Stück.

Die Anzahl aller k–Teilmengen von X ist also gemäß der Pascal–Beziehung, vgl. Satz 1.10.10

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

Die Aussage (ii) ist Gegenstand der Übung. Sie folgt aber auch direkt aus dem so genannten Binomischen Lehrsatz.

2 Matrizen

2.1 Die Matrix-Menge $\mathbb{K}^{m\times n}$

Es sei $\mathbb{K}$ ein Körper, beispielsweise der Körper $\mathbb{Q}$ der rationalen Zahlen oder der Körper $\mathbb{R}$ der reellen Zahlen. Was ein Körper ist, werden wir noch sehr genau kennenlernen.

2.1.1 Definition Ist ein rechteckiges Schema von Zahlen aus $\mathbb{K}$ mit m Zeilen (erster Index) und n Spalten (zweiter Index) gegeben, so sprechen wir von einer $m \times n$*–Matrix* A. Man schreibt

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

Der Eintrag an der j–ten Zeile und der k–ten Spalte einer Matrix A wird mit

$$a_{jk} = a_{j,k} = (A)_{jk}$$

bezeichnet.

Wir bezeichnen die Menge der $m \times n$–Matrizen mit $\mathbb{K}^{m\times n}$.

Genauer mathematisch ist eine Matrix eine Abbildung

$$A : \begin{cases} \{1,\ldots,m\} \times \{1,\ldots,n\} & \to \mathbb{K} \\ (i,j) & \mapsto a_{ij} \end{cases}$$

2.1.2 Beispiele
Hier eine 3×2 Matrix und eine 2×5 Matrix:

$$\begin{pmatrix} 3 & -2 \\ \frac{2}{3} & \sqrt{3} \\ -1 & 2 \end{pmatrix} \in \mathbb{R}^{3\times 2} \qquad \begin{pmatrix} 3 & -2 & \frac{2}{5} & 0 & 2,3 \\ \frac{1}{2} & 3\sqrt{2} & -3 & 1 & 13 \end{pmatrix} \in \mathbb{R}^{2\times 5}$$

2.1.3 Spalten- und Zeilenvektoren

Eine Matrix mit einer Spalte und m Zeilen heißt auch m*-Spaltenvektor*.
Eine Matrix mit einer Zeile und n Spalten heißt auch n*-Zeilenvektor*.

$$\begin{pmatrix} 2 \\ 4 \\ -3 \end{pmatrix} \in \mathbb{R}^{3\times 1} \qquad \begin{pmatrix} 2 & 4 & -3 \end{pmatrix} \in \mathbb{R}^{1\times 3}$$

Die Menge der m-Spaltenvektoren wird kürzer geschrieben als $\mathbb{K}^m := \mathbb{K}^{m\times 1}$.

Eine 1×1 Matrix wird einfach als Zahl aufgefasst:

$$\begin{pmatrix} 7 \end{pmatrix} = 7$$

2.2 Addition und skalare Multiplikation von Matrizen

2.2.1 Addition von Matrizen Man kann zwei Matrizen des gleichen Typs addieren, indem man einfach ihre Einträge addiert:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} =$$

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

Als Beispiel

$$\begin{pmatrix} 4 & -1 & 0 & 6 \\ 2 & -3 & 7 & -1 \\ 1 & 2 & -6 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & -6 & -3 \\ -7 & -2 & -7 & 0 \\ 2 & 1 & 4 & 0 \end{pmatrix} = \begin{pmatrix} 5 & -1 & -6 & 3 \\ -5 & -5 & 0 & -1 \\ 3 & 3 & -2 & 0 \end{pmatrix}$$

2.2.2 Skalare Multiplikation von Matrizen Man kann Matrizen mit einem Skalar, das heißt einer Zahl aus $\mathbb{K}$, multiplizieren, indem man einfach alle ihre Einträge mit dieser Zahl multipliziert:

$$\alpha \cdot \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = \begin{pmatrix} \alpha\cdot a_{11} & \alpha\cdot a_{12} & \cdots & \alpha\cdot a_{1n} \\ \alpha\cdot a_{21} & \alpha\cdot a_{22} & \cdots & \alpha\cdot a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha\cdot a_{m1} & \alpha\cdot a_{m2} & \cdots & \alpha\cdot a_{mn} \end{pmatrix}$$

Als Beispiel

$$3 \cdot \begin{pmatrix} 1 & 0 & -6 & -3 \\ -7 & -2 & -7 & 0 \\ 2 & 1 & 4 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 & -18 & -9 \\ -21 & -6 & -21 & 0 \\ 6 & 3 & 12 & 0 \end{pmatrix}$$

2.3 Multiplikation von Matrizen

2.3.1 Fehl-Idee

Man könnte natürlich auch zwei Matrizen gleichen Typs miteinander multiplizieren, indem man jeweils die Einträge der gleichen Position multipliziert. Die Mathematik/er/innen haben aber festgestellt, dass diese Idee kaum verwertbar ist, in der linearen Algebra spielt sie keine Rolle. Nichtsdestoweniger gibt es eine andere Art, Matrizen zu multiplizieren, die fundamental für die ganze lineare Algebra ist.

2.3.2 Definition: Matrix-Multiplikation

Sind zwei Matrizen $A \in \mathbb{K}^{\ell \times m}$ und $B \in \mathbb{K}^{m \times n}$ gegeben, so ist ihr Matrixprodukt definiert als die Matrix $C \in \mathbb{K}^{\ell \times n}$ mit den folgenden Einträgen

$$c_{jk} \;=\; \sum_{i=1}^{m} a_{ji} b_{ik} \;=\; a_{j1}b_{1k} + a_{j2}b_{2k} + \cdots + a_{jm}b_{mk}$$

Diese Definition mutet einem Neuling unheimlich an. Man kann sie aber mit Hilfe des folgenden Diagramms (Hakentrick) anschaulicher machen.

$$
\begin{array}{ccccc|cccccc}
 & & & & & b_{11} & \cdots & \cdots & b_{1k} & \cdots & b_{1n} \\
 & & & & & \vdots & & & \vdots & & \vdots \\
 & & & & & \vdots & & & \vdots & & \vdots \\
 & & & & & \vdots & & & \vdots & & \vdots \\
 & & & & & b_{m1} & \cdots & \cdots & b_{mk} & \cdots & b_{mn} \\
\hline
a_{11} & \cdots & \cdots & \cdots & a_{1m} & c_{11} & \cdots & \cdots & \cdots & \cdots & c_{1n} \\
\vdots & & & & \vdots & \vdots & & & \downarrow & & \vdots \\
a_{j1} & \cdots & \cdots & \cdots & a_{jm} & \vdots & & \rightarrow & c_{jk} & & \vdots \\
\vdots & & & & \vdots & \vdots & & & & & \vdots \\
a_{\ell 1} & \cdots & \cdots & \cdots & a_{\ell m} & c_{\ell 1} & \cdots & \cdots & \cdots & \cdots & c_{\ell n}
\end{array}
$$

Der Eintrag c_{jk} in der Produktmatrix $C = A \cdot B$ ergibt sich, indem man den ersten, zweiten, $\ldots$, m–ten Eintrag der j–ten Zeile von A jeweils mit dem ersten, zweiten, $\ldots$, m–ten Eintrag der k–ten Spalte von B multipliziert und dann alle Produkte aufaddiert.

2.3.3 Beispiele

$$\begin{pmatrix} 3 & -2 & 5 \\ 1 & -3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 4 & -1 & 0 & 6 \\ 2 & -3 & 7 & -1 \\ 1 & 2 & -6 & 0 \end{pmatrix} = \begin{pmatrix} 13 & 13 & -44 & 20 \\ 0 & 12 & -39 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ -2 \\ 3 \end{pmatrix} = 39$$

$$\begin{pmatrix} 7 \\ -2 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 35 & 7 & 14 \\ -10 & -20 & -40 \\ 15 & 3 & 6 \end{pmatrix}$$

2.3.4 Nullmatrix

Die $n \times m$-Matrix, die nur Nullen als Einträge hat, heißt *Nullmatrix*. Es ist normalerweise kein Problem, sie einfach mit

$$(0) \quad \text{oder} \quad 0$$

zu bezeichnen.

2.3.5 Einheitsmatrix

Die Matrix in $\mathbb{K}^{n\times n}$, die in der Hauptdiagonale als Einträge 1 hat und sonst nur Nullen, heißt *Einheitsmatrix*. Sie wird meist mit I bezeichnet

$$I = I_n = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Gleichbedeutend ist die Bedingung an die Einträge der Matrix, dass an der Position (j,k) die Zahl

$$(I)_{jk} = \delta_{jk} = \begin{cases} 1, & \text{falls } j = k, \\ 0, & \text{falls } j \neq k. \end{cases}$$

hat. Das so definierte Symbol δ_{jk} heißt das *Kronecker–Delta–Symbol*.

2.4 Eigenschaften der Matrixmultiplikation

2.4.1 Satz: Eigenschaften der Matrixmultiplikation

(i) Für eine beliebige Matrix $A \in \mathbb{K}^{m \times n}$ gilt

$$I_m \cdot A \;=\; A \qquad \text{und} \qquad A \cdot I_n = A.$$

(ii) Die Matrixmultiplikation ist assoziativ, d.h. für drei Matrizen $A \in \mathbb{K}^{m \times n}, B \in \mathbb{K}^{n \times \ell}, C \in \mathbb{K}^{\ell \times p}$ gilt:

$$(A \cdot B) \cdot C \;=\; A \cdot (B \cdot C).$$

Deshalb kann dieses Matrixprodukt auch ohne Klammern als $A \cdot B \cdot C$ angegeben werden.

(iii) Die Matrixmultiplikation ist linear: Für ,,passende" Matrizen A, B, C und Skalare $\alpha, \beta, \gamma \in \mathbb{K}$ gilt:

$$\begin{aligned}(\alpha A + \beta B) \cdot C &= \alpha\, A \cdot C + \beta\, B \cdot C \\ A \cdot (\beta B + \gamma C) &= \beta\, A \cdot B + \gamma\, A \cdot C\end{aligned}$$

Für $\alpha = \beta = \gamma = 1$ sind hier die so genannten Distributivgesetze enthalten.

(iv) Bei der Matrixmultiplikation gibt es Nullteiler, d.h. es existieren ,,passende" Matrizen

$$A \neq 0, \quad B \neq 0 \quad \text{mit} \quad A \cdot B \;=\; 0.$$

(v) Besteht eine Matrix $B = (B_1|B_2)$ aus zwei vertikal abgetrennten Teilmatrizen, so gilt

$$A \cdot (B_1|B_2) \;=\; (A \cdot B_1|A \cdot B_2)$$

Insbesondere können die Spaltenvektoren von B einzeln von links mit A multipliziert werden.

(vi) Besteht eine Matrix $A = \left(\frac{A_1}{A_2}\right)$ aus zwei horizontal abgetrennten Teilmatrizen, so gilt

$$\left(\frac{A_1}{A_2}\right) \cdot B \;=\; \left(\frac{A_1 \cdot B}{A_2 \cdot B}\right)$$

Insbesondere können die Zeilenvektoren von A einzeln von rechts mit B multipliziert werden.

2.4.2 Beweis

Zu (i),(iii), (v) und (vi): Nachrechnen.

Zu (ii): Es seien drei Matrizen

$$A \in \mathbb{K}^{m\times n}, \quad B \in \mathbb{K}^{n\times \ell}, \quad C \in \mathbb{K}^{\ell\times p}$$

gegeben. Wir fixieren jetzt eine Position (j,k), $j = 1,\ldots,p$ und $k = 1,\ldots,m$, und betrachten den Eintrag in der Matrix $(A\cdot B)\cdot C$ an dieser Position.

$$\begin{aligned}
& [(A\cdot B)\cdot C]_{jk} \\
& \text{(Definition der Multiplikation } (AB)\cdot C) \\
= & \sum_{i=1}^{\ell} (A\cdot B)_{ji} c_{ik} \\
& \text{(Definition der Multiplikation } A\cdot B) \\
= & \sum_{i=1}^{\ell} \left(\sum_{h=1}^{n} a_{jh} b_{hi} \right) c_{ik} \\
= & \text{(Distributivgesetz: } c_{ik} \text{ wird in die Summe hineinmultipliziert)} \\
= & \sum_{i=1}^{\ell} \left(\sum_{h=1}^{n} a_{jh} b_{hi} c_{ik} \right) \\
= & \text{(Kommutativgesetz der Addition: Vertauschung der Summanden)} \\
= & \sum_{h=1}^{n} \left(\sum_{i=1}^{\ell} a_{jh} b_{hi} c_{ik} \right) \\
= & \text{(Distributivgesetz: Ausklammern von } a_{jh}) \\
= & \sum_{h=1}^{n} a_{jh} \left(\sum_{i=1}^{\ell} b_{hi} c_{ik} \right) \\
& \text{(Definition der Multiplikation } B\cdot C) \\
= & \sum_{h=1}^{n} a_{jh} (B\cdot C)_{hk} \\
& \text{(Definition der Multiplikation } A\cdot (BC)) \\
= & [A\cdot (B\cdot C)]_{jk}
\end{aligned}$$

Für jedes (j,k) stimmen also die Einträge der Matrizen $(A\cdot B)\cdot C$ und $A\cdot(B\cdot C)$ überein. Das bedeutet, dass die Matrizen übereinstimmen.

Zu (iv) geben wir einfach ein Beispiel an:

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

2.5 Anwendung von Matrizen

2.5.1 Lineare Gleichungssysteme Unter einem *linearen Gleichungssystem mit m Gleichungen und n Unbekannten* versteht man eine Zusammenstellung von Gleichungen wie folgt:

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array}$$

Die *Koeffizienten* a_{ij} und b_i der *Rechten Seite* entstammen einem fest gegebenem Körper (später!). Die gesuchten Zahlen x_j sollen ebenfalls diesem Körper angehören.

2.5.2 Umwandlung in Matrix-Schreibweise

Man kann nun die einzelnen Zahlen in dem Gleichungssystem geeignet zu Matrizen bzw. Spaltenvektoren zusammenfassen:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \qquad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

und dann das Gleichungssystem in kompakter Form als Matrixgleichung schreiben:

$$A \cdot x = b.$$

Bei gegebener $m \times n$-Matrix A und gegebenem m-Spaltenvektor b ist der n-Spaltenvektor x gesucht.

Bei der Matrixumschreibung eines linearen Gleichungssystems handelt sich nicht um großartige Mathematik, nichtsdestoweniger erleichtert die neue abstraktere Schreibweise die rechnerische und theoretische Aufarbeitung der Theorie der Linearen Gleichungssysteme.

2.5.3 Geometrische Abbildung Betrachten Sie die Zeichenebene mit einem rechtwinkligen Koordinatensystem. Die Projektion entlang der NW-SO-Richtung auf die Gerade

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \;\middle|\; x_2 = \tfrac{1}{2}x_1 \right\}$$

lässt sich mit Hilfe einer Matrix beschreiben. Ein beliebiger Punkt $\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ wird so abgebildet:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \mapsto \begin{pmatrix} \frac{2}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

2.5.4 Pausenverkauf

Eine Bäckerei verkauft an m Tagen aus einem Sortiment von n Waren. Bezeichnet man die Stückzahl der am Tag j verkauften Waren von Typ k mit s_{jk}, so lässt sich der Gesamtverkauf in einer Matrix

$$S = \begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \vdots & \vdots & & \vdots \\ s_{m1} & s_{m2} & \cdots & s_{mn} \end{pmatrix}$$

zusammenfassen. Die Preise p_k für die einzelnen Warentypen k lassen sich in einem Spaltenvektor

$$p = \begin{pmatrix} p_1 \\ \vdots \\ \vdots \\ p_n \end{pmatrix}$$

anordnen. Der Vektor der Tageseinnahmen

$$t = \begin{pmatrix} t_1 \\ \vdots \\ \vdots \\ t_m \end{pmatrix}$$

ergibt sich dann zu

$$t = S \cdot p.$$

Am Tag j werden (wegen Jubiläumsrabatt, Preiserhöhung o.ä.) alle Preise mit einem Faktor f_j multipliziert. Schreibt man diese Faktoren in den Zeilenvektor

$$f = \begin{pmatrix} f_1 & \cdots & \cdots & f_m \end{pmatrix},$$

so ergeben sich die Gesamteinnahmen über die Verkaufsperiode hinweg zu

$$g = f \cdot t = f \cdot S \cdot p.$$

2.6 Transponierung einer Matrix

2.6.1 Definition: Transponierung Es sei A eine $m \times n$–Matrix. Vertauscht man die Rollen von Zeilen und Spalten, so entsteht die $n \times m$–Matrix $A^T = {}^tA$ mit den Einträgen

$$(A^T)_{jk} = a_{kj}, \qquad j = 1, \ldots, n,\ k = 1, \ldots, m.$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & & a_{m2} \\ \vdots & & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

Sie heißt die zu A *transponierte* Matrix. Beachte, dass auf der rechten Seite die Merkregel ,,linker Index $\sim$ Zeilennummer / rechter Index $\sim$ Spaltennummer” nicht mehr gilt.

2.6.2 Beispiel

$$\begin{pmatrix} 5 & \frac{3}{2} & 4 & -2 \\ 8 & -12 & 0,5 & 7 \\ 6 & -5 & 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 5 & 8 & 6 \\ \frac{3}{2} & -12 & -5 \\ 4 & 0,5 & 0 \\ -2 & 7 & 1 \end{pmatrix}$$

2.6.3 Satz: Transponierung bei Matrixoperationen

Es seien A, B zwei Matrizen mit jeweils zueinander passenden Zeilen- und Spaltenzahlen. Es gilt

$$\begin{aligned} (A+B)^T &= A^T + B^T \\ (\alpha A)^T &= \alpha A^T \\ (A \cdot B)^T &= B^T \cdot A^T \end{aligned}$$

2.6.4 Beweis der dritten Aussage: Für den Eintrag an der Position (j, k) von $(A \cdot B)^T$ gilt:

$$((A \cdot B)^T)_{jk} = (A \cdot B)_{kj} = \sum_{i=1}^{n} (A)_{ki}(B)_{ij} = \sum_{i=1}^{n} (B^T)_{ji}(A^T)_{ik} = (B^T \cdot A^T)_{jk}.$$

2.7 Quadratische Matrizen

2.7.1 Definition: Quadratische Matrizen

Eine Matrix, bei der Zeilenzahl m und Spaltenzahl n übereinstimmen, heißt *quadratisch*.

Wie gehabt wird die Menge der $n \times n$-Matrizen mit $\mathbb{K}^{n \times n}$ bezeichnet.

2.7.2 Matrixmultiplikation nicht-kommutativ

Für $n \geq 2$ ist innerhalb von $\mathbb{K}^{n \times n}$ die Matrixmultiplikation nicht kommutativ. Dies sieht man am Beispiel

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

2.7.3 Definition: Symmetrische und schiefsymmetrische Matrizen

Eine quadratische Matrix heißt *symmetrisch*, wenn

$$A^T = A.$$

Eine quadratische Matrix heißt *schiefsymmetrisch*, wenn

$$A^T = -A.$$

Insbesondere sind alle Diagonaleinträge einer schiefsymmetrischen Matrix Null.

Beispiele sind:

$$\begin{pmatrix} 2 & 3 & -1 \\ 3 & -4 & \frac{3}{2} \\ -1 & \frac{3}{2} & \pi \end{pmatrix} \qquad \text{bzw.} \qquad \begin{pmatrix} 0 & 3 & -1 \\ -3 & 0 & \frac{3}{2} \\ 1 & -\frac{3}{2} & 0 \end{pmatrix}$$

2.7.4 Definition: Invertierbarkeit einer quadratischen Matrix

Eine Matrix $A \in \mathbb{K}^{n \times n}$ heißt *invertierbar*, wenn es eine andere Matrix $B \in \mathbb{K}^{n \times n}$ gibt, so dass

$$A \cdot B = I \qquad \text{und} \qquad B \cdot A = I. \qquad (*)$$

Durch diese beiden Gleichungen ist bei gegebenem A die Matrix B eindeutig bestimmt. Wäre nämlich $\widetilde{B}$ eine weitere Matrix, die $(*)$ erfüllt, so würde gelten:

$$\widetilde{B} = I \cdot \widetilde{B} = B \cdot A \cdot \widetilde{B} = B \cdot I = B.$$

Deshalb wird im Falle der Invertierbarkeit von A die Matrix B mit A^{-1} bezeichnet. Sie heißt die *zu A inverse* Matrix. Es gilt dann also

$$A \cdot A^{-1} = I \qquad \text{und} \qquad A^{-1} \cdot A = I.$$

Wir werden später (Abschnitt 4.2.7) sehen, dass eine der beiden Gleichungen in $(*)$ bereits die andere impliziert.

2.7.5 Beispiele invertierbarer Matrizen

$$\begin{pmatrix} 5 & 6 \\ 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & -3 \\ -\frac{3}{2} & \frac{5}{2} \end{pmatrix}$$

$$\begin{pmatrix} 4 & 0 & 3 \\ -1 & 1 & 0 \\ 5 & -2 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & -6 & -3 \\ 2 & -7 & -3 \\ -3 & 8 & 4 \end{pmatrix}.$$

2.7.6 Definition: Diagonalmatrix

Eine $n \times n$-Matrix, deren Einträge außerhalb der Diagonale Null sind, d.h.

$$a_{jk} = 0, \quad \text{falls } j \neq k,$$

heißt *Diagonalmatrix*. Sie hat die Gestalt und Schreibweise

$$\begin{pmatrix} a_{11} & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & a_{nn} \end{pmatrix} = \operatorname{diag}(a_{11}, \ldots, a_{nn}).$$

Man mache sich folgendes klar:

- Wird eine Matrix $A \in \mathbb{K}^{m\times n}$ von links mit der Diagonalmatrix $\operatorname{diag}(a_{11}, \ldots, a_{mm}) \in \mathbb{K}^{m\times m}$ multipliziert, so wird für alle $j = 1, \ldots, m$ die j-te Zeile von A mit a_{jj} multipliziert.
- Wird eine Matrix $A \in \mathbb{K}^{m\times n}$ von rechts mit der Diagonalmatrix $\operatorname{diag}(a_{11}, \ldots, a_{nn}) \in \mathbb{K}^{n\times n}$ multipliziert, so wird für alle $k = 1, \ldots, n$ die k-te Spalte von A mit a_{kk} multipliziert.
- Es ist $\operatorname{diag}(a_{11}, \ldots, a_{nn}) \cdot \operatorname{diag}(b_{11}, \ldots, b_{nn}) = \operatorname{diag}(a_{11}b_{11}, \ldots, a_{nn}b_{nn})$.
- Eine Diagonalmatrix ist genau dann invertierbar, wenn alle Diagonaleinträge ungleich Null sind. Es ist dann

$$\operatorname{diag}(a_{11}, \ldots, a_{nn})^{-1} = \operatorname{diag}(a_{11}^{-1}, \ldots, a_{nn}^{-1}).$$

2.7.7 Definition: Dreiecksmatrizen

Eine $n \times n$-Matrix, deren Einträge unterhalb der Diagonale Null sind, d.h.

$$a_{jk} = 0, \quad \text{falls } j > k,$$

heißt *obere Dreiecksmatrix*.

Dual dazu heißt eine $n \times n$-Matrix, deren Einträge oberhalb der Diagonale Null sind, d.h.

$$a_{jk} = 0, \quad \text{falls } j < k,$$

eine *untere Dreiecksmatrix*. Sie haben die Gestalt

$$\begin{pmatrix} * & \cdots & \cdots & \cdots & * \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & * \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} * & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ * & \cdots & \cdots & \cdots & * \end{pmatrix}$$

Es ist üblich, mit Hilfe des Sterns anzudeuten, dass da ,,irgendeine" Zahl (ungleich Null oder gleich Null) aus dem Körper steht.

Enthält zusätzlich die Diagonale ausschließlich Nullen, so spricht man von *strengen* oberen bzw. unteren Dreiecksmatrizen

$$\begin{pmatrix} 0 & * & \cdots & \cdots & * \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & * \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ * & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ * & \cdots & \cdots & * & 0 \end{pmatrix}.$$

2.7.8 Definition: Einzel-Diagonalmatrix

Zur späteren Verwendung legen wir noch eine Bezeichnung fest.

$$Q_{j|\alpha} \quad = \quad \operatorname{diag}(1,\ldots,1,\alpha,1,\ldots,1) \;=\; \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \alpha & & \\ & & & & 1 & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

Die Zahl α steht an der Position (j,j).
Alle nicht vorhandenen Einträge sind Null.

Man mache sich folgendes klar:

- Wird eine Matrix $A \in \mathbb{K}^{m\times n}$ von links mit $Q_{j|\alpha} \in \mathbb{K}^{m\times m}$ multipliziert, so wird die j-te Zeile von A mit α multipliziert.
- Wird eine Matrix $A \in \mathbb{K}^{m\times n}$ von rechts mit $Q_{j|\alpha} \in \mathbb{K}^{n\times n}$ multipliziert, so wird die j-te Spalte von A mit α multipliziert.
- Es ist $\operatorname{diag}(a_{11},\ldots,a_{nn}) = Q_{1|\alpha_{11}} \cdot \ldots \cdot Q_{n|\alpha_{nn}}$.
- Wenn $\alpha \neq 0$, dann ist $Q_{j|\alpha}$ invertierbar mit $(Q_{j|\alpha})^{-1} = Q_{j|\frac{1}{\alpha}}$.

2.7.9 Definition: Vertauschungsmatrix

Eine quadratische Matrix der Form

$$T_{jk} \quad = \quad \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & & 1 & & \\ & & & & 1 & & & & \\ & & & \vdots & & \ddots & \vdots & & \\ & & & & & & 1 & & \\ & & & 1 & \cdots & & 0 & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}$$

Die Nullen stehen an den Positionen (j,j) und (k,k).
Die beiden extra Einsen stehen an den Positionen (j,k) und (k,j).
Alle nicht vorhandenen Einträge sind Null.

mit $k \neq j$ heißt *Vertauschungsmatrix.*

Beachte, dass T_{jk} eine ganze Matrix bezeichnet und nicht etwa den Eintrag $(T)_{jk}$ einer Matrix T.

Man mache sich folgendes klar:

- Wird eine Matrix $A \in \mathbb{K}^{m \times n}$ von links mit der Vertauschungsmatrix $T_{jk} \in \mathbb{K}^{m \times m}$ multipliziert, so werden dabei die j-te und k-te Zeile von A vertauscht.
- Wird eine Matrix $A \in \mathbb{K}^{m \times n}$ von rechts mit der Vertauschungsmatrix $T_{jk} \in \mathbb{K}^{n \times n}$ multipliziert, so werden dabei die j-te und k-te Spalte von A vertauscht.
- T_{jk} ist invertierbar mit $(T_{jk})^{-1} = T_{jk}$.

2.7.10 Definition: Addierer-Matrix

Zur späteren Verwendung führen wir für $j \neq k$ die folgende Matrix ein:

$$R_{jk} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & \vdots & \ddots & \\ & & 1 \cdots & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}$$

Die zusätzliche 1 steht an der Position (j, k).
Alle nicht vorhandenen Einträge sind Null.

Man mache sich folgendes klar:

- Wird eine Matrix $A \in \mathbb{K}^{m \times n}$ von links mit der Matrix $R_{jk} \in \mathbb{K}^{m \times m}$ multipliziert, so wird die j-te Zeile in A durch die Summe der j-ten und k-ten Zeile ersetzt.

  Kürzer: Die k-te Zeile wird zur j-ten addiert.
- Wird eine Matrix $A \in \mathbb{K}^{m \times n}$ von rechts mit der Matrix $R_{jk} \in \mathbb{K}^{n \times n}$ multipliziert, so wird die k-te Spalte in A durch die Summe der k-ten und j-ten Spalte ersetzt.

  Kürzer: Die j-te Spalte wird zur k-ten addiert.

2.7.11 Definition: α-Addierer-Matrix

Für $j \neq k$ definieren wir noch die Matrix

$$R_{jk|\alpha} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & \vdots & \ddots & \\ & & \alpha & \cdots & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

Die Zahl α steht an der Position (j, k).
Alle nicht vorhandenen Einträge sind Null.

Man mache sich folgendes klar:

- Wird eine Matrix $A \in \mathbb{K}^{m\times n}$ von links mit der Matrix $R_{jk|\alpha} \in \mathbb{K}^{m\times m}$ multipliziert, so wird die j-te Zeile in A durch die Summe aus j-ter und ver-α-fachter k-ter Zeile ersetzt.

  Kürzer: Das α-fache der k-ten Zeile wird zur j-ten addiert.

- Wird eine Matrix $A \in \mathbb{K}^{m\times n}$ von rechts mit der Matrix $R_{jk|\alpha} \in \mathbb{K}^{n\times n}$ multipliziert, so wird die k-te Spalte in A durch die Summe aus k-ter und ver-α-fachter j-ter Spalte ersetzt.

  Kürzer:Das α-fache der j-ten Spalte wird zur k-ten addiert.

- Die Matrizen $R_{jk|\alpha}$ und $R_{jk|-\alpha}$ sind invertierbar mit $(R_{jk|\alpha})^{-1} = R_{jk|-\alpha}$.

- Die Matrix R^{α}_{jk} kann wie folgt als Produkt der vorherigen Matrizen geschrieben werden:

$$\begin{aligned} R_{jk|\alpha} &= Q_{j|\alpha^{-1}} \cdot R_{jk} \cdot Q_{j|\alpha} \\ &= Q_{k|\alpha} \cdot R_{jk} \cdot Q_{k|\alpha^{-1}}. \end{aligned}$$

  Wir werden später noch sehen, dass sich alle quadratischen Matrizen als Produkte von Matrizen der Form $Q_{j|\alpha}$, T_{jk} und R_{jk} darstellen lassen.

3 Lineare Gleichungssysteme

3.1 Einführung

Wir betrachten ein LGS

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \quad\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{array}$$

das in Matrixform so geschrieben werden kann:

$$A \cdot x = b.$$

INPUT: Gegeben sind dabei die $m \times n$–Matrix A und der m-Spaltenvektor b. Es ist gelegentlich günstig bzw. für Programmierzwecke sehr zweckmäßig, diese Daten in der $m \times (n+1)$-Matrix

$$A|b = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array} \right)$$

zusammenzufassen. Sie heißt die *erweiterte Matrix* zum LGS.

OUTPUT: Gesucht ist der n-Spaltenvektor x. Wir bezeichnen die Menge aller n-Spaltenvektor x, die das obige LGS lösen, mit $\mathcal{L}(A|b)$. Formal:

$$\mathcal{L}(A|b) := \left\{ x \in \mathbb{K}^n \,\middle|\, Ax = b \right\}$$

3.1.1 Beispiele

Wir wollen an Beispielen aufzeigen, dass dann die folgenden Fälle auftreten können:

- Die Lösungsmenge ist leer:

$$0 \cdot x = 3 \qquad \begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- Die Lösungsmenge enthält genau ein Element:

$$2 \cdot x = 3 \qquad \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

- Die Lösungsmenge enthält unendlich viele Elemente:

$$0 \cdot x = 0 \qquad \begin{pmatrix} 0 & 3 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Dabei gibt es unterschiedliche Qualitäten von „Unendlich“.

3.2 Äquivalenzumformungen

3.2.1 Definition: Äquivalenz/Umformung

Zwei Lineare Gleichungssysteme $A|b$ und $\widetilde{A}|\widetilde{b}$ heißen *äquivalent*, wenn ihre Lösungsmengen übereinstimmen.

Eine Umformung, die ein gegebenes LGS $A|b$ in ein anderes äquivalentes LGS $\widetilde{A}|\widetilde{b}$ überführt, heißt *Äquivalenzumformung*.

3.2.2 Zeilenumformung: Invertierbare Matrix von links

Wird ein gegebenes LGS von links mit einer invertierbaren $m \times m$-Matrix T multipliziert, so geht es in ein äquivalentes LGS über. Für ein $x \in \mathbb{K}^n$ gilt nämlich (ganz ausführlich)

$$\begin{array}{rrclcl} & Ax & = & b & \text{bzw.} & x \in \mathcal{L}(A|b) \\ \stackrel{T \text{ von links}}{\Longrightarrow} & T \cdot Ax & = & T \cdot b & \text{bzw.} & x \in \mathcal{L}(TA|Tb) \\ \stackrel{T^{-1} \text{ von links}}{\Longrightarrow} & Ax & = & b & \text{bzw.} & x \in \mathcal{L}(A|b), \end{array}$$

also ist $x \in \mathcal{L}(A|b)$ genau dann, wenn $x \in \mathcal{L}(TA|Tb) = \mathcal{L}(T(A|b))$.

Wir nennen eine solche Äquivalenzumformung einfach *Zeilenumformung*.

3.2.3 Elementare Zeilenumformungen

Insbesondere gibt es die folgenden *elementaren Zeilenumformungen*:

- Linksmultiplikation mit $Q_{j|\alpha}$, $\alpha \neq 0$: Die j-te Zeile des LGS wird mit α multipliziert.
- Linksmultiplikation mit T_{jk}: Die j-te und k-te Zeile des LGS werden getauscht.
- Linksmultiplikation mit R_{jk}: Die k-te Zeile des LGS wird zur j-ten Zeile addiert.

3.2.4 Zusätzliche Beobachtung

Man mache sich folgendes klar:

Stehen in den beteiligten (ein oder zwei) Zeilen von $A|b$ in der gleichen Spalte Nullen, so ist dies auch nach einer elementaren Zeilenumformung der Fall.

Für eine beliebige Spaltennummer $\ell \in \{1, \ldots, n+1\}$ gilt:

$$(A|b)_{j\ell} = 0 = (A|b)_{k\ell} \quad \Longrightarrow \quad (\widetilde{A}|\widetilde{b})_{j\ell} = 0 = (\widetilde{A}|\widetilde{b})_{k\ell}.$$

3.2.5 Kombinierte Zeilenumformung

Wie wir in Abschnitt 2.7.11 gesehen haben, können diese elementaren Zeilenumformungen zu einer weiteren Zeilenumformung kombiniert werden:

- Linksmultiplikation mit $R_{jk|\alpha}$: Die ver-α-fachte k-te Zeile des LGS wird zur j-ten Zeile addiert.

3.2.6 Einträge zu Null machen

Ist bei einer gegebenen erweiterten Matrix $A|b$ ein Diagonalelement $a_{\ell\ell}$ ungleich Null, so lassen sich alle anderen Einträge in der Spalte ℓ durch Zeilenumformungen ,,zu Null machen".

Steht dabei an der Position (ℓ, k) (gleiche Zeile wie $a_{\ell\ell}$, andere Spalte k) eine Null, so bleiben dabei alle Einträge dieser Spalte unverändert.

$$\left(\begin{array}{ccccccccccc|c} * & \cdots & * & * & * & \cdots & * & * & * & \cdots & * & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & * & \vdots & & \vdots & * & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & 0 & \vdots & & \vdots & a_{\ell\ell} & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & * & \vdots & & \vdots & * & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots & \vdots \\ * & \cdots & * & * & * & \cdots & * & * & * & \cdots & * & * \end{array}\right) \rightsquigarrow \left(\begin{array}{ccccccccccc|c} \widetilde{*} & \cdots & \widetilde{*} & * & \widetilde{*} & \cdots & \widetilde{*} & 0 & \widetilde{*} & \cdots & \widetilde{*} & \widetilde{*} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & * & \vdots & & \vdots & 0 & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & 0 & \vdots & & \vdots & a_{\ell\ell} & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & * & \vdots & & \vdots & 0 & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots & \vdots \\ \widetilde{*} & \cdots & \widetilde{*} & * & \widetilde{*} & \cdots & \widetilde{*} & 0 & \widetilde{*} & \cdots & \widetilde{*} & \widetilde{*} \end{array}\right)$$

Wie geht das? Führe für alle Zeilen $j = 1, \ldots, m$, $j \neq \ell$ die folgende Operation aus:

> Multipliziere von links mit der $m \times m$ Matrix $R_{j\ell|-\frac{a_{j\ell}}{a_{\ell\ell}}}$.
> Gleichbedeutend damit ist, dass von der j-ten Zeile das $\frac{a_{j\ell}}{a_{\ell\ell}}$ -fache der Zeile ℓ subtrahiert wird.
>
> Es ist dann
>
> $$\widetilde{a}_{j\ell} \;=\; a_{j\ell} - \tfrac{a_{j\ell}}{a_{\ell\ell}} \cdot a_{\ell\ell} \;=\; 0.$$

3.2.7 Beispiel

$$\left(\begin{array}{cccc|c} -2 & 4 & 5 & -3 & -2 \\ 0 & 2 & 1 & 6 & 7 \\ 7 & -1 & 5 & 3 & 9 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{cccc|c} -2 & 0 & 3 & -15 & -16 \\ 0 & 2 & 1 & 6 & 7 \\ 7 & 0 & 5\,\frac{1}{2} & 6 & 12\,\frac{1}{2} \end{array}\right)$$

Es ist $a_{22} \neq 0$. Also lassen sich alle Einträge der Spalte 2 zu Null machen.
Weiter ist $a_{21} = 0$. Deshalb bleibt Spalte 1 unverändert.

3.3 Äquivalenzumformung in obere Dreiecksform

3.3.1 Obere Dreiecksfrom

Ein LGS $A|b$ heißt in *oberer Dreiecksform*, wenn alle Einträge von A unterhalb der Diagonale gleich Null sind:

$$a_{jk} \;=\; 0, \quad \text{falls } j > k.$$

Es hat also die Gestalt

$$\begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{nn} \\ \vdots & & & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}, \quad \begin{pmatrix} a_{11} & \cdots & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & a_{nn} \end{pmatrix}, \quad \begin{pmatrix} a_{11} & \cdots & \cdots & \cdots & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & & & & \vdots \\ \vdots & \ddots & \ddots & & & & \vdots \\ \vdots & & \ddots & \ddots & & & \vdots \\ 0 & \cdots & \cdots & 0 & a_{mm} & \cdots & a_{mn} \end{pmatrix},$$

je nach dem die Zeilenzahl größer, gleich oder kleiner ist als die Spaltenzahl.

3.3.2 Satz: Äquivalenzumformung eines LGS in obere Dreiecksform

Durch eine Abfolge geeigneter Zeilenumformungen kann man ein gegebenes LGS $A|b$ in ein anderes äquivalentes LGS $\widetilde{A}|\widetilde{b}$ umformen,...

(i) das in oberer Dreiecksform ist,

(ii) dessen Diagonaleinträge $\widetilde{a}_{kk}$ gleich Null oder Eins sind,

(iii) und, falls ein Diagonaleintrag $\widetilde{a}_{kk} = 1$ ist, auch alle Einträge oberhalb dieses Eintrags gleich Null sind.

Das bedeutet, dass die k-te Spalte der Matrix $\widetilde{A}$ genau eine der beiden Formen

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \leftarrow \text{Zeile } k$$

hat.

3.3.3 Begründung

Führe für jede Spalte $k = 1, 2, \ldots, \min\{m, n\}$ (von links nach rechts) des gegebenen LGS die folgenden Schritte durch:

- Erreiche durch Vertauschung mit einer Zeile unterhalb, dass möglichst an der Diagonal-Position (k, k) ein Eintrag ungleich Null steht!
- Falls der Eintrag an der Diagonalposition (k, k) ungleich Null ist, multipliziere die Zeile k mit $\frac{1}{a_{kk}}$!
- Mache alle Einträge unterhalb (und wenn möglich und gewünscht: oberhalb) von (k, k) zu Null!
- Dabei bleiben alle Spalten $1, \ldots, k-1$ unverändert.
- Gehe zur nächsten Spalte $k + 1$.

3.3.4 Beispiel 1 Wir betrachten das LGS

$$\begin{array}{rcrcrcr} 2x_1 & + & 3x_2 & - & 2x_3 & = & -3 \\ 5x_1 & - & x_2 & + & 3x_3 & = & K \\ x_1 & + & x_2 & + & x_3 & = & 5 \\ -3x_1 & + & 4x_2 & - & 4x_3 & = & 2 \end{array}$$

in dem ein Parameter $K \in \mathbb{R}$ auftritt. Es soll in Abhängigkeit von K die Lösungsmenge $\mathcal{L}(A|b_K)$ bestimmt werden.

Die Zeilenumformungen laufen nun beispielsweise wie folgt ab. Es ist günstig zunächst die Zeilen so zu ordnen, dass Einsen weiter oben auftauchen und der Parameter ganz unten.

$$\begin{array}{rrr|r||r} 2 & 3 & -2 & -3 & \\ 5 & -1 & 3 & K & \\ 1 & 1 & 1 & 5 & \\ -3 & 4 & -4 & 2 & \\ \hline 1 & 1 & 1 & 5 & \\ 2 & 3 & -2 & -3 & -2\ \mathrm{I} \\ -3 & 4 & -4 & 2 & +3\ \mathrm{I} \\ 5 & -1 & 3 & K & -5\ \mathrm{I} \\ \hline 1 & 1 & 1 & 5 & -1\ \mathrm{II} \\ 0 & 1 & -4 & -13 & \\ 0 & 7 & -1 & 17 & -7\ \mathrm{II} \\ 0 & -6 & -2 & K-25 & +6\ \mathrm{II} \\ \hline 1 & 0 & 5 & 18 & \\ 0 & 1 & -4 & -13 & \\ 0 & 0 & 27 & 108 & :27 \\ 0 & 0 & -26 & K-103 & \\ \hline 1 & 0 & 5 & 18 & -5\ \mathrm{III} \\ 0 & 1 & -4 & -13 & +4\ \mathrm{III} \\ 0 & 0 & 1 & 4 & \\ 0 & 0 & -26 & K-103 & +26\ \mathrm{III} \\ \hline 1 & 0 & 0 & -2 & \\ 0 & 1 & 0 & 3 & \\ 0 & 0 & 1 & 4 & \\ 0 & 0 & 0 & K+1 & \\ \hline \end{array}$$

für $K \neq -1$ ist die Lösungsmenge leer. Für $K = -1$ ergibt sich die eindeutige Lösung

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -2 \\ 3 \\ 4 \end{pmatrix}.$$

3.3.5 Beispiel 2 Wir betrachten das LGS

$$\begin{array}{rcrcrcrcr} 6x_1 & + & 4x_2 & - & 4x_3 & + & 2x_4 & = & 12 \\ -x_1 & + & 2x_2 & - & 2x_3 & + & 3x_4 & = & -5 \\ 3x_1 & - & x_2 & - & x_3 & - & x_4 & = & 0 \end{array}$$

Die Zeilenumformungen laufen nun beispielsweise wie folgt ab.

$$\begin{array}{rrrr|r||r} 6 & 4 & -4 & 2 & 12 & :2 \to \ \mathrm{II} \\ -1 & 2 & -2 & 3 & -5 & \cdot(-1) \to \ \mathrm{I} \\ 3 & -1 & -1 & -1 & 0 & \\ \hline 1 & -2 & 2 & -3 & 5 & \\ 3 & 2 & -2 & 1 & 6 & -3\ \mathrm{I} \\ 3 & -1 & -1 & -1 & 0 & -3\ \mathrm{I} \\ \hline 1 & -2 & 2 & -3 & 5 & \\ 0 & 8 & -8 & 10 & -9 & :8 \\ 0 & 5 & -7 & 8 & -15 & \\ \hline 1 & -2 & 2 & -3 & 5 & +2\ \mathrm{II} \\ 0 & 1 & -1 & \frac{5}{4} & -\frac{9}{8} & \\ 0 & 5 & -7 & 8 & -15 & -5\ \mathrm{II} \\ \hline 1 & 0 & 0 & -\frac{1}{2} & \frac{11}{4} & \\ 0 & 1 & -1 & \frac{5}{4} & -\frac{9}{8} & \\ 0 & 0 & -2 & \frac{7}{4} & -\frac{75}{8} & :(-2) \\ \hline 1 & 0 & 0 & -\frac{1}{2} & \frac{11}{4} & \\ 0 & 1 & -1 & \frac{5}{4} & -\frac{9}{8} & +\ \mathrm{III} \\ 0 & 0 & 1 & -\frac{7}{8} & \frac{75}{16} & \\ \hline 1 & 0 & 0 & -\frac{1}{2} & \frac{11}{4} & \\ 0 & 1 & 0 & \frac{3}{8} & \frac{57}{16} & \\ 0 & 0 & 1 & -\frac{7}{8} & \frac{75}{16} & \\ \hline \end{array}$$

Damit ergibt sich als allgemeine Lösung

$$x(\lambda) \quad = \quad \begin{pmatrix} \frac{11}{4} \\ \frac{57}{16} \\ \frac{75}{16} \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} \frac{1}{2} \\ -\frac{3}{8} \\ \frac{7}{8} \\ 1 \end{pmatrix}.$$

4 Gruppen und Körper

4.1 Verknüpfungen

4.1.1 Definition Es sei X eine beliebige Menge. Eine Abbildung

$$v : \begin{cases} X \times X & \to & X \\ (a,b) & \mapsto & v(a,b) \end{cases}$$

heißt *Verknüpfung auf* X. Um die ,,Binarität" der Verknüpfung zu betonen, schreibt man meist

$$v(a,b) \quad = \quad a \star b.$$

Anstelle des Zeichens $\star$ werden vielfältige Symbole benutzt.

4.1.2 Beispiele

- Auf der Menge $X = \mathbb{N}$:
  - Addition $(a,b) \mapsto a + b$,
  - Multiplikation $(a,b) \mapsto a \cdot b = ab$,
  - Potenz $(a,b) \mapsto a^b$,
  - Größter gemeinsamer Teiler $(a,b) \mapsto a \sqcap b = \mathrm{ggT}(a,b)$,
  - Kleinstes gemeinsames Vielfaches $(a,b) \mapsto a \sqcup b = \mathrm{kgV}(a,b)$,
  - Minimum $\quad \min : (a,b) \mapsto \begin{cases} a, & \text{falls } a \leq b, \\ b, & \text{falls } a > b, \end{cases}$
- Auf der Menge $X = \mathbb{Q}$:
  - Addition, Subtraktion, Multiplikation, Minimum,
  - Arithmetisches Mittel $(a,b) \mapsto a \perp b \ := \frac{a+b}{2}$.
- Auf der Menge $X = \mathbb{R}^+ = \{x \in \mathbb{R} | x > 0\}$
  - Addition, Multiplikation, Potenz,
  - geometrisches Mittel $(a,b) \mapsto \sqrt{a \cdot b}$.
- Auf der Menge $X = \mathcal{P}(Y)$, wobei Y eine Menge:
  - Vereinigung, Durchschnitt, Differenz, Symmetrische Differenz
- Auf der Menge $X = \mathbb{R}^{n \times n}$
  - Addition, Subtraktion, Multiplikation
- Auf der Menge $X = \mathcal{F}(Y,Y)$ der Abbildungen $Y \to Y$ innerhalb einer Menge Y
  - Komposition $(f,g) \mapsto g \circ f$

4.2 Gruppen

4.2.1 Definition Eine Menge G zusammen mit einer Verknüpfung $\star$ heißt *Gruppe*, symbolisch $(G, \star)$, wenn folgende ,,Gesetze" erfüllt sind:

$\boxed{\text{AG}}$ (Assoziativgesetz) Für beliebige $a, b, c \in G$ gilt:

$$(a \star b) \star c = a \star (b \star c)$$

$\boxed{\text{NE}}$ (Existenz und Eindeutigkeit des neutralen Elements)
Es existiert genau ein Element $e \in G$, so dass für alle $a \in G$ gilt

$$a \star e = a \qquad \text{und} \qquad e \star a = a$$

$\boxed{\text{IE}}$ (Existenz und Eindeutigkeit der inversen Elemente)
Zu jedem $a \in G$ existiert genau ein Element $b \in G$, so dass für alle $a \in G$

$$b \star a = e \qquad \text{und} \qquad a \star b = e.$$

4.2.2 Beispiele Was ist jeweils das neutrale Element? Welches ist das inverse Element zu einem gegebenen Element?

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$
- $(\mathbb{K}^{m \times n}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$
- Die Menge der quadratischen Diagonalmatrizen mit Einträgen ungleich Null auf der Diagonalen

  $$\left\{ A \in \mathbb{K}^{n \times n} \middle| \begin{array}{ll} a_{jk} = 0, & \text{falls } j \neq k \\ a_{jk} \neq 0, & \text{falls } j = k \end{array} \right\}$$

  mit der Matrixmultiplikation als Verknüpfung.
- $(\mathcal{P}(X), \Delta)$.
- Definiere auf der Menge $\{g, u\}$ die Verknüpfung

$\oplus$	g	u
g	g	u
u	u	g

  Es handelt sich um eine Gruppe mit zwei Elementen, sie wird meist mit $\mathbb{Z}_2$ bezeichnet.
- Die sogenannte *triviale Gruppe* besteht aus einem einzigen Element: $G = \{e\}$.
- Die Menge der invertierbaren Matrizen

  $$\mathrm{GL}(n, \mathbb{K}) \quad := \quad \{A \in \mathbb{K}^{n \times n} | A \text{ invertierbar}\}$$

  ist bzgl. der Matrixmultiplikation eine Gruppe.
- Die Menge $X = \mathcal{F}^{\text{bij}}(Y, Y)$ der bijektiven Abbildungen $Y \to Y$ ist mit der Komposition als Verknüpfung eine Gruppe.

4.2.3 Abschwächung der Gruppenaxiome

Betrachte für eine Verknüpfung $\star$ auf einer Menge X die folgenden beiden Eigenschaften

$\boxed{\text{NE/IE}^{\text{links}}}$ Es gibt ein Element $e \in X$, so dass die beiden folgenden Aussagen gelten:

- Für alle $a \in X$ gilt: $e \star a = a$. Man sagt dazu, e sei *links-neutral*.
- Zu jedem $a \in X$ existiert ein Element $b \in X$, so dass $b \star a = e$. Man sagt, b ist zu a *links-invers* bzgl. e.

$\boxed{\text{NE/IE}^{\text{rechts}}}$ Es gibt ein Element $e \in X$, so dass die beiden folgenden Aussagen gelten:

- Für alle $a \in X$ gilt: $a \star e = a$ Man sagt dazu, e sei *rechts-neutral*.
- Zu jedem $a \in X$ gibt es ein Element $b \in X$, so dass $a \star b = e$. Man sagt, b ist zu a *rechts-invers* bzgl. e.

4.2.4 Satz: Schwache Gruppenaxiome → Starke Gruppenaxiome

Es sei $\star$ eine Verknüpfung auf einer Menge X, die $\boxed{\text{AG}}$ erfüllt. Dann sind die folgenden drei Aussagen äquivalent:

(A) Es gelten die Gesetze $\boxed{\text{NE}}$ und $\boxed{\text{IE}}$, d.h. $(X, \star)$ ist eine Gruppe.

(B) Es gilt $\boxed{\text{NE/IE}^{\text{links}}}$.

(C) Es gilt $\boxed{\text{NE/IE}^{\text{rechts}}}$.

4.2.5 Beweis

Die Implikationen (A) $\Rightarrow$ (B) und (A) $\Rightarrow$ (C) sind trivial.
Für (B) $\Rightarrow$ (A) braucht man mehrere Schritte. Es sei also das Axiom NE/IE$^{\text{links}}$ gegeben.

Wir nennen ein Element e, das den Aussagen NE/IE$^{\text{links}}$ bzw. NE/IE$^{\text{rechts}}$ genügt, innerhalb dieses Beweises *stark links-neutral* bzw. *stark rechts-neutral*.

1. Es sei e stark links-neutral und $a \in X$ beliebig. Wir zeigen, dass ein zu a bzgl. e links-inverses Element b auch rechts-invers bzgl. e ist. Dazu sei $c \in X$ links–invers zu b bzgl. e. Jetzt gilt:

$$\begin{aligned}
& a \star b \\
\text{\scriptsize (e ist links-neutral)} \quad &= e \star (a \star b) \\
\text{\scriptsize (c ist links-invers zu b bzgl. e)} \quad &= (c \star b) \star (a \star b) \\
\text{\scriptsize (Assoziativ-Gesetz)} \quad &= (c \star (b \star a)) \star b \\
\text{\scriptsize (b ist links-invers zu a bzgl. e)} \quad &= (c \star e) \star b \\
\text{\scriptsize (Assoziativ-Gesetz)} \quad &= c \star (e \star b) \\
\text{\scriptsize (e ist links-neutral)} \quad &= c \star b \\
\text{\scriptsize (c ist links-invers zu b bzgl. e)} \quad &= e
\end{aligned}$$

2. Es sei e stark links-neutral. Wir zeigen, dass e rechts–neutral ist. Dazu sei $a \in G$ beliebig und b zu a links-invers bzgl. e. Dann gilt:

$$\begin{aligned} & a \star e \\ \text{(}b\text{ ist links-invers zu }a\text{ bzgl. }e\text{)} \quad = \; & a \star (b \star a) \\ \text{(Assoziativ-Gesetz)} \quad = \; & (a \star b) \star a \\ \text{(Gemäß Schritt 1 ist }b\text{ rechts-invers zu }a\text{ bzgl. }e\text{)} \quad = \; & e \star a \\ \text{(}e\text{ ist links-neutral)} \quad = \; & a \end{aligned}$$

3. Angenommen, es gibt zwei stark links-neutrale Elemente e und $\tilde{e}$. Dann gilt

$$\begin{aligned} & \tilde{e} \\ \text{(Nach Schritt 2 ist }e\text{ rechts-neutral)} \quad = \; & \tilde{e} \star e \\ \text{(}\tilde{e}\text{ ist links-neutral)} \quad = \; & e. \end{aligned}$$

4. Angenommen, es gibt zu einem $a \in X$ zwei links-inverse Elemente b und $\tilde{b}$ (bzgl. des einzigen stark links-neutralen Elements e). Dann ist

$$\begin{aligned} & \tilde{b} \\ \text{(}e\text{ ist links-neutral)} \quad = \; & e \star \tilde{b} \\ \text{(}b\text{ ist links-invers zu }a\text{)} \quad = \; & (b \star a) \star \tilde{b} \\ \text{(Assoziativ-Gesetz)} \quad = \; & b \star (a \star \tilde{b}) \\ \text{(Nach Schritt 1 ist }\tilde{b}\text{ rechts-invers zu }a\text{)} \quad = \; & b \star e \\ \text{(Nach Schritt 2 ist }e\text{ rechts-neutral)} \quad = \; & b. \end{aligned}$$

   Also ist das links-inverse Element eindeutig.

Die andere Implikation (C) $\Rightarrow$ (A) wird völlig analog gezeigt.

4.2.6 Bezeichnung: Inverses Element

Da das inverse Element zu einem beliebiges $a \in G$ eindeutig ist, kann es symbolisch auf a bezogen werden: Man schreibt — je nach verwendetem — Verknüpfungssymbol:

$$a^{-1}, \qquad \tfrac{1}{a}, \qquad -a, \qquad \ominus a.$$

4.2.7 Beispiel: Inverse Matrix Die Äquivalenzen des letzten Satzes zeigen, dass zur Definition der Invertierbarkeit einer Matrix bereits eine der beiden Gleichungen in 2.7.4 $(*)$ ausreicht. Die eine Gleichung impliziert die andere.

4.2.8 Satz Existenz und Eindeutigkeit der Lösung

Es seien $(G, \star)$ eine Gruppe und $a, b \in G$.

(i) Die Gleichung $a \star x = b$ hat genau eine Lösung $x = a^{-1} \star b$.

(ii) Die Gleichung $x \star a = b$ hat genau eine Lösung $x = b \star a^{-1}$.

4.2.9 Beweis Existenz: Für gegebene $a, b \in G$ setze $x := a^{-1} \star b$. Dann gilt tatsächlich

$$a \star (a^{-1} \star b) \overset{\text{AG}}{=} (a \star a^{-1}) \star b \overset{\text{IE}}{=} e \star b \overset{\text{NE}}{=} b.$$

Eindeutigkeit: Es seien $x_1, x_2 \in G$, so dass

$$a \star x_1 = b \qquad \text{und} \qquad a \star x_2 = b.$$

Dann folgt:

$$a \star x_1 = a \star x_2.$$

Wir multiplizieren diese Gleichung von links mit a^{-1}

$$a^{-1} \star a \star x_1 = a^{-1} \star a \star x_2.$$

Daraus folgt mit (IE) und (NE) $x_1 = x_2$.

4.2.10 Definition

Eine Gruppe $(G, \star)$ heißt *abelsch* oder *kommutativ*, wenn das folgende ,,Gesetz" gültig ist:

$\boxed{\text{KG}}$ Für alle $a, b \in G$ gilt:

$$a \star b = b \star a.$$

4.2.11 Beispiele

- Die in Abschnitt 4.2.2 erwähnte Gruppe $\mathrm{GL}(\mathbb{K}, n)$ ist für $n \geq 2$ nicht-kommutativ.
- Die in Abschnitt 4.2.2 erwähnte Gruppe $\mathcal{F}^{\text{bij}}(Y, Y)$ ist für $|Y| \geq 3$ nicht-kommutativ.
- Alle anderen dort erwähnten Gruppen sind kommutativ.
- Die Menge $\left\{ A \in \mathbb{K}^{n \times n} \middle| \begin{smallmatrix} a_{jk} = 0, & \text{falls } j > k \\ a_{jk} \neq 0, & \text{falls } j = k \end{smallmatrix} \right\}$ der quadratischen oberen Dreiecksmatrizen mit Einträgen ungleich Null auf der Diagonalen ist Beispiel einer weiteren nicht–kommutativen Gruppe. Die Matrixmultiplikation ist die Verknüpfung. Neutrales Element ist die Einheitsmatrix. Das inverse Element zu einer gegebenen oberen Dreiecksmatrix A ist die eindeutige Lösung X des LGS (mit n^2 Gleichungen)

$$\begin{pmatrix} a_{11} & \cdots & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_{11} & \cdots & \cdots & \cdots & x_{1n} \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & x_{nn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Die Nicht-Kommutativität wird durch das Beispiel in Abschnitt 2.7.2 aufgezeigt.

4.3 Körper

4.3.1 Definition Eine Menge $\mathbb{K}$, auf der zwei Verknüpfungen

$$+ : \begin{cases} \mathbb{K} \times \mathbb{K} & \to & \mathbb{K} \\ (a,b) & \mapsto & a+b \end{cases} \qquad \text{und} \qquad \cdot : \begin{cases} \mathbb{K} \times \mathbb{K} & \to & \mathbb{K} \\ (a,b) & \mapsto & a \cdot b \end{cases}$$

(Addition und Multiplikation) definiert sind, heißt *(kommutativer) Körper* $(\mathbb{K}, +, \cdot)$, wenn folgendes gilt:

(1) $(\mathbb{K}, +)$ ist eine abelsche Gruppe (mit neutralem Element 0).

(2) $(\mathbb{K} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe (mit neutralem Element 1).

(3) Für alle $a, b, c \in \mathbb{K}$ gilt das Distributivgesetz:

$$a \cdot (b + c) \quad = \quad (a \cdot b) + (a \cdot c).$$

4.3.2 Stärker ausgebreitet

bedeutet dies, dass die folgenden Eigenschaften erfüllt sind:

$\boxed{\text{AG/A}}$ Das Assoziativgesetz der Addition.

Für alle $a, b, c \in \mathbb{K}$ gilt: $(a + b) + c \; = \; a + (b + c)$

$\boxed{\text{KG/A}}$ Kommutativgesetz der Addition.

Für alle $a, b \in \mathbb{K}$ gilt: $a + b = b + a$.

$\boxed{\text{NE/A}}$ Neutrales Element bzgl. Addition.

Es gibt genau ein Element $0 \in \mathbb{K}$, so dass für alle $a \in \mathbb{K}$ gilt: $a+0 = 0+a = a$.

$\boxed{\text{IE/A}}$ Inverses Element bzgl. Addition.

Zu jedem Element $a \in \mathbb{K}$ gibt es genau ein Element $-a$, so dass gilt: $a + (-a) = 0$.

$\boxed{\text{AG/M}}$ Assoziativgesetz der Multiplikation.

Für alle $a, b, c \in \mathbb{K} \setminus \{0\}$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$\boxed{\text{KG/M}}$ Kommutativgesetz der Multiplikation.

Für alle $a, b \in \mathbb{K} \setminus \{0\}$ gilt: $a \cdot b = b \cdot a$.

$\boxed{\text{NE/M}}$ Neutrales Element bzgl. Multiplikation.

Es gibt ein Element $1 \in \mathbb{K} \setminus \{0\}$, so dass für alle $a \in \mathbb{K}$ gilt: $a \cdot 1 = 1 \cdot a = a$.

$\boxed{\text{IE/M}}$ Inverses Element bzgl. Multiplikation.

Zu jedem Element $a \in \mathbb{K} \setminus \{0\}$ gibt es genau ein Element a^{-1}, so dass gilt: $a \cdot a^{-1} = 1$.

$\boxed{\text{DG}}$ Distributivgesetz.

Für alle $a, b, c \in \mathbb{K}$ gilt: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

4.3.3 Beispiele Ihnen bereits bekannte Beispiele von Körpern sind

- der Körper der rationalen Zahlen $\mathbb{Q}$
- der Körper der reellen Zahlen $\mathbb{R}$

mit der gewöhnlichen Addition und Multiplikation. Beachten Sie, dass die oben angegebenen Körpereigenschaften keine Aussage über die Ordnungsrelation $\leq$ machen.

4.3.4 Bemerkungen

- Das neutrale Element der Addition heißt *Null(–element)*.
- Die Addition eines inversen Elements wird als *Subtraktion* bezeichnet. Man schreibt kürzer $a - b \ := \ a + (-b)$.
- Das neutrale Element der Multiplikation heißt *Eins(–element)*.
- Die Multiplikation mit einem inversen Element wird als *Division* bezeichnet. Man schreibt kürzer $a : b \ := \ a \cdot b^{-1}$.
- Das Verknüpfungssymbol $\cdot$ wird oft weggelassen. Man schreibt kürzer:

$$a\,b \ = \ a \cdot b.$$

- Es wird die Konvention „Punkt vor Strich" benutzt. Das Distributivgesetz kann dann so geschrieben werden:

$$\begin{aligned} a \cdot (b + c) \ &= \ a \cdot b + a \cdot c \qquad \text{bzw.} \\ a\,(b + c) \ &= \ a\,b + a\,c \end{aligned}$$

4.3.5 Satz: Nullteilerfreiheit

Es seien a, b zwei beliebige Elemente in einem Körper $\mathbb{K} = (\mathbb{K}, +, \cdot)$. Dann gilt:

(i) $a = 0$ oder $b = 0 \qquad \Longleftrightarrow \qquad a \cdot b = 0.$

(ii) Die Implikation

$$a + a + \ldots + a \;=\; 0 \qquad \Longrightarrow \qquad a = 0$$

ist im allgemeinen nicht richtig.

4.3.6 Beweis

(i) „$\Rightarrow$": Wir setzen O.B.d.A. $b = 0$. Es gilt für ein beliebiges $a \in \mathbb{K}$:

$$a \cdot 0 \;=\; a \cdot (0 + 0) \;=\; a \cdot 0 + a \cdot 0.$$

Das heißt aber, dass $a \cdot 0$ das additiv neutrale Element ist. Also ist $a \cdot 0 = 0$.

(i) „$\Leftarrow$": Es seien $a, b \in \mathbb{K}$ gewählt mit

$$a \cdot b \;=\; 0 \quad \text{und} \quad a \;\neq\; 0.$$

Es gilt dann

$$b \;=\; 1 \cdot b \;=\; a^{-1} \cdot a \cdot b \;=\; a^{-1} \cdot 0 \;=\; 0.$$

Die Aussage (ii) verdeutlichen wir an einem (Gegen-)Beispiel:

In dem Körper $\{g, u\}$ (Abschnitt 4.5.2) gilt $u + u = 0$, u ist aber nicht das neutrale Element bzgl. der Addition.

4.3.7 Bemerkung

Die Aussage dieses Satzes führt dazu, dass in den Eigenschaften $\boxed{\text{AG/M}}$ und $\boxed{\text{KG/M}}$ die Menge der Elemente, für die die angegebenen Gleichungen gelten, von $\mathbb{K} \setminus \{0\}$ in das ganze $\mathbb{K}$ abgeändert werden kann.

4.4 Ringe

4.4.1 Definition: Ring

- Eine Menge R, auf der zwei Verknüpfungen $+$ und $\cdot$ definiert sind, heißt *Ring*, wenn sie bzgl. der Addition $+$ eine abelsche Gruppe ist und zusätzlich die Eigenschaften

  $\boxed{\text{AG/M}} \qquad \boxed{\text{DG}}$

  aufweist.

- Ein Ring R heißt *kommutativ*, wenn auch die Multiplikation kommutativ ist, also zusätzlich

  $\boxed{\text{KG/M}}$

  erfüllt ist.

- Ein Ring R heißt *unital (= mit Eins)*, wenn es genau ein neutrales Element bzgl. der Multiplikation gibt, also zusätzlich

  $\boxed{\text{NE/M}}$

  erfüllt ist.

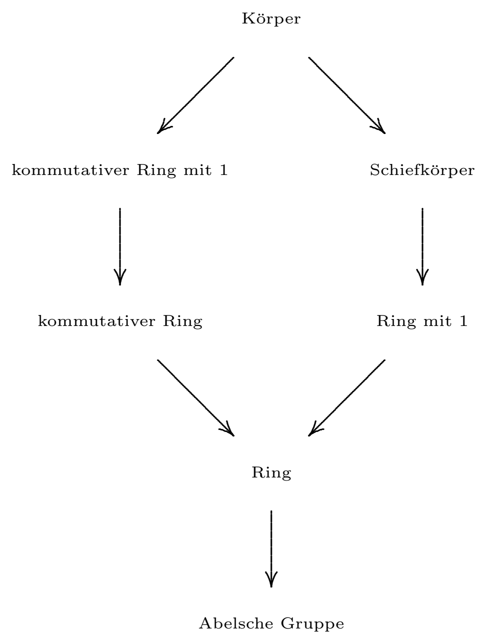
- Ein Ring R mit Eins heißt *Schiefkörper*, wenn jedes Element ungleich Null genau ein (eindeutiges) Inverses bzgl. der Multiplikation hat, also zusätzlich

  $\boxed{\text{IE/M}}$

  erfüllt ist. Ein Schiefkörper muss nicht multiplikativ-kommutativ sein.

4.4.2 Beispiele

- $\mathbb{Z}$ ist ein kommutativer Ring mit 1.
- Die Menge $\mathbb{R}[x]$ der Polynome in einer Variablen mit Koeffizienten aus $\mathbb{R}$ bildet einen kommutativen Ring mit 1.
- Die Menge $\mathbb{K}^{n\times n}$ der quadratischen Matrizen ist ein Ring mit 1. Für $n \geq 2$ ist er nicht kommutativ.
- Die Menge $2\,\mathbb{Z}$ der geraden ganzen Zahlen bildet einen kommutativen Ring (ohne 1).
- Der Quaternionen-Schiefkörper wird später noch vorgestellt.



4.5 Der Körper $\mathbb{F}_p$

4.5.1 Definition: Der Körper $\mathbb{F}_p$

- Es sei p eine Primzahl, die wir uns von jetzt ab fixiert denken.
- Definiere für jede ganze Zahl $k \in \mathbb{Z}$ die Teilmenge

$$\overline{k} \;:=\; \{\ldots, k-3p, k-2p, k-p, k, k+p, k+2p, k+3p, \ldots\} \subseteq \mathbb{Z}.$$

  Es ist die Menge aller ganzen Zahlen, die bei der Division durch p den Rest k ergeben. Man nennt sie deshalb *Restklassen modulo* p.

- Unterscheiden sich zwei Zahlen $k, \ell \in \mathbb{Z}$ um ein ganzzahliges Vielfaches von p, so gilt offenbar $\overline{k} = \overline{\ell}$.
- Es sei jetzt $\mathbb{F}_p$ die Menge aller Restklassen modulo p

$$\mathbb{F}_p \;=\; \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}.$$

- Definiere Addition und Multiplikation auf $\mathbb{F}_p$ durch

$$\begin{aligned} \overline{k} + \overline{\ell} \;&:=\; \overline{k+\ell} \\ \overline{k} \cdot \overline{\ell} \;&:=\; \overline{k \cdot \ell}. \end{aligned}$$

- Man kann dann beweisen, dass $\mathbb{F}_p$ ein Körper mit genau p Elementen ist.

4.5.2 Beispiele

- Wir nehmen $p = 2$ und sehen, dass auf der Menge $\{g, u\}$ mit

$$\begin{aligned} g \;&=\; \overline{0} \;=\; 2\mathbb{Z} \;=\; \{\text{gerade Zahlen}\} \\ u \;&=\; \overline{1} \;=\; 2\mathbb{Z}+1 \;=\; \{\text{ungerade Zahlen}\} \end{aligned}$$

  die Addition und Multiplikation gegeben sind durch

$+$	g	u
g	g	u
u	u	g

$\cdot$	g	u
g	g	g
u	g	u

  Der Beweis, dass dies ein Körper ist, besteht darin, alle Körpergesetze für alle Einsetzungen von g, u für die in diesen Gesetzen auftretenden Variablen zu testen. Das Null–Element ist $0 = g$. Das Eins–Element ist $1 = u$.

- Für $p = 3$ sind die Verknüpfungstabellen gegeben durch

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

- Für $p = 5$ sind die Verknüpfungstabellen gegeben durch

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

- In der Algebra wird dann weiter bewiesen, dass es zu jeder Primzahlpotenz $q = p^k$ genau einen Körper $\mathbb{F}_{p^k}$ mit dieser Mächtigkeit gibt. In diesem Fall können Addition und Multiplikation aber nicht nach der ,,Restklassenmethode" definiert werden. Man sollte nicht die Symbole

$$\overline{0}, \overline{1}, \ldots\ldots, \overline{p^k - 1}$$

  zur Beschreibung der Elemente benutzen.

- Endliche Körper mit Mächtigkeiten, die ungleich einer Primzahlpotenz sind — beispielsweise Mächtigkeit 6 — gibt es nicht.

- Beachte, dass in endlichen Körpern $\mathbb{F}_p$ oder $\mathbb{F}_{p^k}$ nicht in sinnvoller Weise eine ,,lineare Ordnung" $\leq$ definiert werden kann.

- Lässt man es zu, dass p keine Primzahl ist, so entsteht gemäß der obigen Definition von Addition und Multiplikation ein kommutativer Ring mit 1, der aber kein Körper ist. Er wird mit $\mathbb{Z}/p\mathbb{Z}$ bezeichnet.

  Ist nämlich $p = r \cdot s$ mit $1 < r, s < p$ eine Faktorzerlegung von p, so gilt

$$\overline{r} \cdot \overline{s} \;=\; \overline{p} \;=\; \overline{0}.$$

  In diesem Ring gibt es also Nullteiler, was nach Satz 4.3.5 in einem Körper unmöglich ist.

4.6 Der Körper der komplexen Zahlen

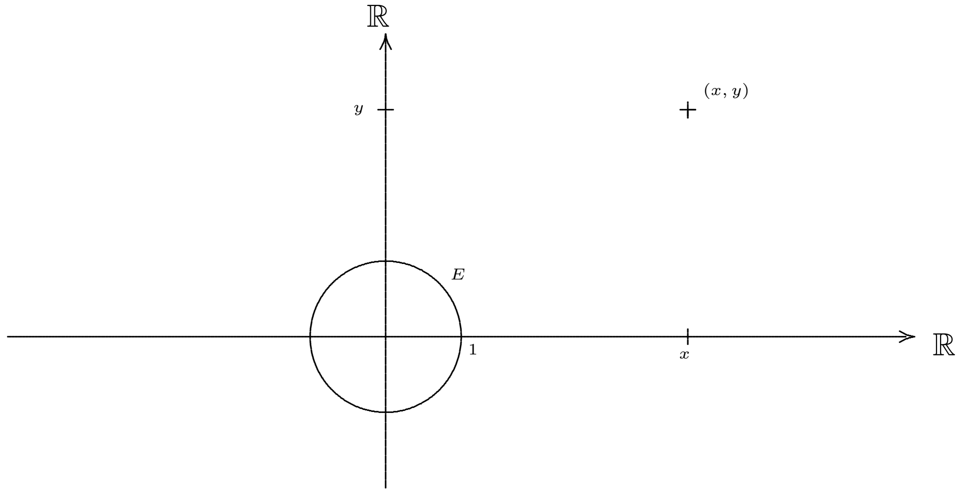
4.6.1 Gauß'sche Zahlenebene Wir betrachten die Menge der reellen Zahlenpaare

$$\mathbb{C} \ := \ \mathbb{R} \times \mathbb{R} \ := \ \Big\{ (x,y) \ \Big| \ x,y \in \mathbb{R} \Big\}.$$

In dem nun zu entwickelnden Kontext heißen die Zahlenpaare *komplexe Zahlen*. Im allgemeinen verwendet man die Buchstaben

$$z \ = \ (x,y) \qquad \text{oder} \qquad w = (u,v).$$

Wir stellen uns diese Menge als eine Ebene vor.



Bei Zugrundelegung dieser Auffassung heißt die Ebene auch *Gauß'sche Zahlenebene* oder *komplexe Zahlenebene*.

4.6.2 Versuch Wir stellen uns die Aufgabe, dieser Menge der Zahlenpaaren die ,,Grundrechenarten" so einführen, dass die Körperaxiome erfüllt sind. Ein erster Versuch könnte darin bestehen, die Verknüpfungen komponentenweise durchzuführen:

$$\begin{aligned} (x,y) + (u,v) \quad &:= \quad (x+u, y+v) \\ (x,y) \cdot (u,v) \quad &:= \quad (xu, yv) \end{aligned}$$

Tatsächlich ist dann $(\mathbb{R} \times \mathbb{R}, +)$ eine abelsche Gruppe mit dem neutralen Element $(0,0)$. Leider ist aber $(\mathbb{R} \times \mathbb{R} \setminus \{(0,0)\}, \cdot)$ keine Gruppe, da Elemente der Form $(a,0)$ oder $(0,b)$ keine Inversen besitzen. Anderes Argument: Es gilt auch

$$(a,0) \cdot (0,b) \ = \ (0,0).$$

Wir wissen aber aus Satz 4.3.5, dass Körper keine Nullteiler besitzen. SACKGASSE!

4.6.3 Komplexe Addition und Multiplikation

Es gibt aber eine Lösung unserer Aufgabe. Wir definieren auf der Menge $\mathbb{C}$ die Addition koordinatenweise und die Multiplikation ganz anders wie folgt:

$$\begin{aligned} (x,y) + (u,v) \quad &:= \quad (x+u, y+v) \\ (x,y) \cdot (u,v) \quad &:= \quad (xu - yv, xv + yu) \end{aligned}$$

Wir probieren diese Verknüpfungen an verschiedenen Beispielen aus.

4.6.4 Addition, skalare Multiplikation, reelle Zahlen als Teilmenge

- Die Addition ist einfach die aus der Schule bekannte Addition von Vektoren in der Zeichenebene. Das neutrale Element bzgl. der Addition ist $0 = (0, 0)$. Das additiv inverse zu einer Zahl (x, y) ist $(-x, -y)$.
- Wir betrachten die Verknüpfung für Zahlenpaare, deren zweite Koordinate 0 ist.

$$(x, 0) + (u, 0) \; = \; (x + u, 0), \qquad (x, 0) \cdot (u, 0) \; = \; (x \cdot u, 0).$$

  Das bedeutet, dass mit diesen Zahlen genauso gerechnet wird wie mit den reellen Zahlen. Auf diese Weise kann die Menge der reellen Zahlen als Teilmenge der komplexen Zahlen aufgefasst werden. Man sagt auch, dass die Zahlen $(a, 0)$ reell sind. Die Schreibweise als Inklusion

$$\mathbb{R} \; \subseteq \; \mathbb{C} \; = \; \mathbb{R} \times \mathbb{R}$$

  ist mengentheoretisch etwas skurril, aber algebraisch sinnvoll. Entsprechend schreibt man auch

$$x \; := \; (x, 0) \qquad \text{für alle } x \in \mathbb{R}.$$

- Aus der Schule ist bekannt, dass Vektoren auch vervielfacht werden können (Skalar–Multiplikation). Wir multiplizieren eine reelle Zahl mit einer beliebigen komplexen Zahl:

$$(x, 0) \cdot (u, v) \; = \; (xu, xv).$$

  Tatsächlich wird der ,,Vektor (u, v) mit x skalar vervielfacht.

4.6.5 Die imaginäre Einheit, Real- und Imaginärteil

- Das Quadrat von $(0, 1)$ ist

$$(0, 1)^2 \; = \; (0, 1) \cdot (0, 1) = (-1, 0).$$

  Wir haben also eine Wurzel der reellen Zahl -1 gefunden.
- Dies ist Anlass für die Definition der *Imaginären Einheit*:

$$i \; := \; (0, 1).$$

- Dann kann eine beliebige komplexe Zahl (x, y) ein-eindeutig geschrieben werden als

$$(x, y) \; = \; (x, 0) + (0, y) \; = \; (x, 0) + (0, 1) \cdot (y, 0) \; = \; x + iy.$$

- In Bezug auf eine gegebene komplexe Zahl $z = (x, y)$ heißt die reelle Zahl x der *Realteil* und y der *Imaginärteil.* Als Funktionen sind dies

$$\mathrm{Re} : \left\{ \begin{array}{rcl} \mathbb{C} & \to & \mathbb{R} \\ (x, y) & \mapsto & x \end{array} \right. \qquad \mathrm{Im} : \left\{ \begin{array}{rcl} \mathbb{C} & \to & \mathbb{R} \\ (x, y) & \mapsto & y \end{array} \right.$$

4.6.6 Distributive Interpretation der komplexen Multiplikation

Die Regel für die Multiplikation 4.6.3 zweier komplexer Zahlen kann in der i-Darstellung nun so aufgeschrieben werden:

$$(x + iy) \cdot (u + iv) \quad = \quad (xu - yv) + i(xv + yu).$$

Damit eröffnet sich im Nachhinein eine zugänglichere Sichtweise der komplexen Multiplikation. Bei Anwendung der Distributivität und der Regel $i^2 = -1$ auf die linke Seite kommt genau der Ausdruck rechts heraus.

Beachte, dass wir damit das Distributivgesetz weder bewiesen noch benutzt haben, wir haben lediglich die Definition der komplexen Multiplikation ,,distributiv interpretiert".

4.6.7 Multiplikativ Inverses

Das zu einem Element $z = x + iy \in \mathbb{C} \setminus \{0\}$ multiplikativ inverse ist gegeben durch

$$\frac{1}{z} \quad = \quad \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}.$$

Wie bei rationalen oder reellen Zahlen wird bei der Division zweier komplexer Zahlen die Bruchschreibweise verwendet.

In der Tat gilt:

$$(x + iy) \cdot \left(\tfrac{x}{x^2+y^2} - i\tfrac{y}{x^2+y^2}\right) \;=\; \left(\tfrac{x^2}{x^2+y^2} + \tfrac{y^2}{x^2+y^2}\right) + i\left(\tfrac{xy}{x^2+y^2} - \tfrac{yx}{x^2+y^2}\right) \;=\; 1.$$

4.6.8 Satz: $(\mathbb{C}, +, \cdot\,)$ ist ein Körper.

4.6.9 Beweis

(1) Dass bzgl. der Addition eine abelsche Gruppe vorliegt, ist offensichtlich.

(2) Dass für drei komplexe Zahlen p, q, z das Assoziativgesetz der Multiplikation gilt,

$$(p \cdot q) \cdot z \quad = \quad p \cdot (q \cdot z),$$

soll in einer Übungsaufgabe gezeigt werden.

(3) Neutrales Element und inverse Elemente bzgl. der Multiplikation haben wir schon angegeben. Die Eindeutigkeit ist mit Satz 4.2.4, angewandt auf die Gruppe $(\mathbb{C} \setminus \{0\}, \cdot\,)$, gezeigt.

(4) Unter Benutzung der distributiven Interpretation, vgl. Abschnitt 4.6.6, berechnen wir getrennt die linke und die rechte Seite im Distributivgesetz.

$$\begin{aligned}
& (x+iy) \cdot \big((u+iv) + (p+iq)\big) \\
= \; & (x+iy) \cdot \big(u+p+i(v+q)\big) \\
= \; & x(u+p) - y(v+q) + i\big(y(u+p) + x(v+q)\big) \\
= \; & xu + xp - yv - yq + i(yu + yp + xv + xq)
\end{aligned}$$

$$\begin{aligned}
& (x+iy) \cdot (u+iv) + (x+iy) \cdot (p+iq) \\
= \; & xu - yv + i(yu + xv) + xp - yq + i(yp + xq) \\
= \; & xu - yv + xp - yq + i(yu + xv + yp + xq).
\end{aligned}$$

Es stellt sich heraus, dass die beiden Ausdrücke übereinstimmen.

4.6.10 Definition: Konjugation in $\mathbb{C}$

Wir definieren für eine Zahl $z = x + iy$ in der komplexen Zahlenebene die *Konjugiert-Komplex-Bildung* durch:

$$\overline{} : \begin{cases} \mathbb{C} & \to \quad \mathbb{C} \\ z = x + iy & \mapsto \quad \overline{z} = x - iy \end{cases}$$

$\overline{z}$ heißt die zu z *konjugiert-komplexe* Zahl.

4.6.11 Satz: Eigenschaften der Konjugiert-Komplex-Bildung

Die Konjugiert-Komplex-Bildung hat folgende Eigenschaften.

(i) Sie ist ein „Automorphismus" des Körpers $\mathbb{C}$, d.h. es gilt für alle $z, w \in \mathbb{C}$

$$\begin{aligned} \overline{z+w} &= \overline{z} + \overline{w}, & \overline{z-w} &= \overline{z} - \overline{w}, \\ \overline{z \cdot w} &= \overline{z} \cdot \overline{w}, & \overline{\left(\tfrac{z}{w}\right)} &= \tfrac{\overline{z}}{\overline{w}}, \quad \text{falls } w \neq 0. \end{aligned}$$

(ii) Sie ist involutiv, d.h. es gilt für alle $z \in \mathbb{C}$

$$\overline{\overline{z}} = z$$

(iii) Für Real- und Imaginärteil einer komplexen Zahl z gelten die Identitäten

$$\begin{aligned} \operatorname{Re} z &= \frac{z + \overline{z}}{2} \\ \operatorname{Im} z &= \frac{z - \overline{z}}{2i} \end{aligned}$$

Eine komplexe Zahl stimmt mit ihrer konjugierten überein genau dann, wenn sie reell ist

$$z = \overline{z} \quad \Longleftrightarrow \quad z \in \mathbb{R}.$$

4.6.12 Definition: Absolutbetrag in $\mathbb{C}$

Wir definieren für eine Zahl $z = x + iy$ in der komplexen Zahlenebene die Konjugiert-Komplex-Bildung durch:

$$|\cdot| : \begin{cases} \mathbb{C} & \to \quad \mathbb{R}^{\geq 0} \\ z = x + iy & \mapsto \quad |z| = \sqrt{x^2 + y^2} \end{cases}$$

Die Zahl $|z|$ heißt der *Absolutbetrag* (kurz: *Betrag*) der komplexen Zahl z.

4.6.13 Satz: Eigenschaften des Absolutbetrags

Der Absolutbetrag hat folgende Eigenschaften

(i) Zusammenhang mit Konjugiert-Komplex-Bildung

$$\begin{aligned} |z|^2 &= z \cdot \overline{z} \in \mathbb{R}_0^+ \\ |z| &= 0 \quad \Longleftrightarrow \quad z = 0 \end{aligned}$$

(ii) Multiplikativität. Für zwei komplexe Zahlen z, w gilt

$$\begin{aligned} |w \cdot z| &= |w| \cdot |z| \\ \left|\tfrac{w}{z}\right| &= \tfrac{|w|}{|z|}, \quad \text{falls } z \neq 0 \\ |w + z| &\neq |w| + |z| \qquad \text{(im allgemeinen)} \\ |w - z| &\neq |w| - |z| \qquad \text{(im allgemeinen).} \end{aligned}$$

(iii) Mit Hilfe der Konjugiert-Komplexbildung und des Absolutbetrags lässt sich die Ermittlung des multiplikativ inversen Elements einer komplexen Zahl $z = x + iy$ so durchführen

$$\frac{1}{z} = \frac{\overline{z}}{\overline{z} \cdot z} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2}.$$

4.6.14 Einheitskreis Wir betrachten jetzt Zahlen, die auf dem Einheitskreis E der komplexen Zahlenebene liegen:

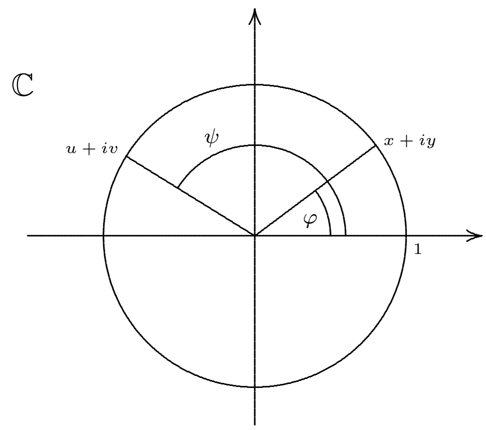
$$E \quad := \quad \left\{ z \in \mathbb{C} \,\middle|\, |z| = 1 \right\} \;\subseteq\; \mathbb{C}.$$

Ist $x + iy$ eine beliebige Zahl auf diesem Einheitskreis, so gibt es, wie in der Analysis gezeigt wird, eine Zahl $\varphi \in \mathbb{R}$ (das *Bogenmass*), so dass

$$x \quad = \quad \cos\varphi, \qquad y = \sin\varphi.$$

Beispielsweise kann man $\varphi = \arctan \frac{y}{x}$ nehmen.

Die Zahl φ heißt in diesem Zusammenhang das *Argument*, oder — im Kontext physikalischer Anwendungen — der *Phasenwinkel* von z.



4.6.15 Multiplikation auf dem Einheitskreis

Für zwei Zahlen aus E

$$\begin{aligned} x + iy &= \cos\varphi + i\sin\varphi \\ u + iv &= \cos\psi + i\sin\psi \end{aligned}$$

berechnen wir das Produkt:

$$\begin{aligned} (u+iv)\cdot(x+iy) &= (\cos\psi + i\sin\psi)\cdot(\cos\varphi + i\sin\varphi) \\ &= (\cos\psi\cdot\cos\varphi - \sin\psi\cdot\sin\varphi) + i(\cos\psi\cdot\sin\varphi + \cos\varphi\cdot\sin\psi) \\ \text{(Additionstheoreme)} \quad &= \cos(\psi+\varphi) + i\sin(\psi+\varphi). \end{aligned}$$

Das Produkt liegt wieder auf dem Einheitskreis. Der Multiplikation zweier komplexer Zahlen auf dem Einheitskreis entspricht die Addition der zugehörigen Bogenmasse.

4.6.16 Polarkoordinaten

Es sei $z = x + iy \in \mathbb{C} \setminus \{0\}$ eine komplexe Zahl ungleich Null. Dividiert man diese Zahl durch ihren Betrag $|z|$, so liegt der Quotient $\frac{z}{|z|}$ auf dem Einheitskreis:

$$\left|\frac{z}{|z|}\right| = \frac{1}{|z|} \cdot |z| = 1.$$

Setzt man jetzt $r := |z|$ und $\varphi := \arctan \frac{y}{x}$, so gilt weiter

$$z = |z| \cdot \frac{z}{|z|} = r \cdot (\cos\varphi + i \sin\varphi).$$

z lässt sich also als Produkt einer positiven reellen Zahl und einer Zahl auf dem Einheitskreis schreiben.

Man nennt die Darstellung von komplexen Zahlen mit Hilfe von *Betrag* r und *Argument (Phasenwinkel)* φ die *Darstellung in Polarkoordinaten (PKD)*. Es gilt

$$r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = r_1\, r_2\,(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).$$

Das heißt die Multiplikation zweier komplexer Zahlen manifestiert sich bei Benutzung von Polarkoordinaten als Multiplikation der Beträge und Addition der Phasenwinkel.

5 Vektorräume

5.1 Einführung

Sie werden vermutlich beim Begriff Vektor an Pfeile oder Klassen parallelgleicher Pfeile denken. Tatsächlich sind Pfeile als eine mögliche Veranschaulichung von Vektoren geeignet, man muss aber darauf achten, dass diese Veranschaulichung zu eng oder gar irreführend sein kann. Ganz knapp und nicht ganz exakt kann man sagen, dass Vektoren mathematische Objekte sind, die man addieren und vervielfachen, i.a. aber nicht miteinander multiplizieren kann. Wir wollen dies ganz exakt aufschreiben.

5.1.1 Definition $\mathbb{K}$–Vektorraum

Es sei ein Körper $\mathbb{K}$ vorgegeben. Eine Menge V heißt $\mathbb{K}$–*Vektorraum* oder *Vektorraum über* $\mathbb{K}$, wenn auf ihr eine Addition

$$\oplus : \begin{cases} V \times V & \to & V \\ (v,w) & \mapsto & v \oplus w \end{cases}$$

und eine *skalare Multiplikation*

$$\odot : \begin{cases} \mathbb{K} \times V & \to & V \\ (\alpha,w) & \mapsto & \alpha \odot w \end{cases}$$

festgelegt sind, so dass die folgenden Axiome gelten:

$\boxed{\text{Gr/A}}$ V ist bezüglich der Addition eine abelsche Gruppe.

$\boxed{\text{AG/sM}}$ Für $\alpha, \beta \in \mathbb{K}$ und $v \in V$ gilt:

$$(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v)$$

$\boxed{\text{NE/sM}}$ Für $v \in V$ gilt:

$$1 \odot v = v.$$

$\boxed{\text{DGa/sM}}$ Für $\alpha, \beta \in \mathbb{K}$ und $v \in V$ gilt:

$$(\alpha + \beta) \odot v = \alpha \odot v \oplus \beta \odot v.$$

$\boxed{\text{DGb/sM}}$ Für $\alpha \in \mathbb{K}$ und $v, w \in V$ gilt:

$$\alpha \odot (v \oplus w) = \alpha \odot v \ \oplus\ \alpha \odot w.$$

5.1.2 Bemerkungen

1. Die Elemente eines Vektorraums heißen *Vektoren*. Im Zusammenhang mit Vektorräumen heißen die Elemente des Körpers *Skalare*.

2. Sie werden vielleicht aus der Schule die Konvention kennen, dass Vektoren durch kleine Rechtspfeile oberhalb des Symbols gekennzeichnet werden, beispielsweise durch $\vec{v}$, $\vec{w}$ oder ähnlich. Dies ist auch in der wissenschaftlichen Mathematik möglich, aber eher unüblich.

3. Wir werden lediglich das neutrale Element der Addition, es heißt *Nullvektor*, als $\vec{0}$ schreiben, so dass eine Unterscheidung zur Zahl $0 \in \mathbb{K}$ sichtbar ist. Später, wenn keine Verwechslungen auftreten, werden wir auch nur wieder 0 schreiben.

4. Innerhalb der Axiome haben wir die Sonderzeichen $\oplus$ und $\odot$ benutzt, um die logisch-definitorischen Feinheiten herauszuarbeiten.

   Sie werden sich im Laufe des Kurses davon überzeugen können, dass es keine großen Probleme bedeutet, wenn wie für die beiden Vektorraumoperationen $\oplus$ und $\odot$ auch nur die einfachen Symbole $+$ bzw. $\cdot$ benutzen. Oft wird auch der Punkt weggelassen. Man sollte sich aber immer vergegenwärtigen, innerhalb welcher Menge diese Operationen gerade ausgeführt werden.

5. Der zu einem Vektor v bezüglich der Addition inverse Vektor heißt der zu v negative Vektor, er wird mit $-v$ bezeichnet.

6. Ein $\mathbb{R}$–Vektorraum wird auch einfach reeller Vektorraum genannt. Entsprechend gibt es komplexe oder rationale Vektorräume.

7. Die Vektorraum–Axiome enthalten keinerlei Aussagen über Basen, lineare Unabhängigkeit oder Dimension.

8. Beachte, dass noch nicht die Rede ist von Länge von Vektoren oder Winkeln zwischen Vektoren.

9. Wir haben durchgängig die Skalare links von den Vektoren geschrieben. Letztlich wegen der Kommutativität der Multiplikation in $\mathbb{K}$ stellt es kein Problem dar, Skalare auch rechts von Vektoren zu schreiben.

10. Wie oben bei der Formulierung der Distributivgesetze schon zu sehen war, gilt auch in Vektorräumen die Punkt–vor–Stich–Konvention.

5.1.3 Satz (Nullteilerfreiheit)

Für $\alpha \in \mathbb{K}$ und $v \in V$ gilt die folgende Äquivalenz

$$\alpha \cdot v \;=\; \vec{0} \qquad \Longleftrightarrow \qquad \alpha = 0 \text{ oder } v = \vec{0}.$$

5.1.4 Beweis Der Beweis besteht aus drei Schritten:

(1) Wir beweisen zuerst die Implikation $\alpha = 0 \Rightarrow \alpha \cdot v = \vec{0}$.

Für $v \in V$ gilt

$$0 \cdot v \;=\; (0+0) \cdot v \;=\; 0 \cdot v + 0 \cdot v.$$

Deshalb ist $0 \cdot v$ das neutrale Element der Addition, also $0 \cdot v = \vec{0}$.

(2) Wir beweisen dann die Implikation $v = \vec{0} \Rightarrow \alpha \cdot v = \vec{0}$. Für $\alpha \in \mathbb{K}$ ist hier

$$\alpha \cdot \vec{0} \;=\; \alpha \cdot (\vec{0} + \vec{0}) \;=\; \alpha \cdot \vec{0} + \alpha \cdot \vec{0}.$$

Wieder ist $\alpha \cdot \vec{0}$ neutrales Element der Addition, somit $\alpha \cdot \vec{0} = \vec{0}$.

(3) Es bleibt noch der $\Rightarrow$ Anteil der Behauptung zu zeigen. Ist $\alpha \neq 0$ und $v \in V$ mit $\alpha \cdot v = \vec{0}$, so gilt

$$v \;=\; 1 \cdot v \;=\; \tfrac{1}{\alpha} \cdot \alpha \cdot v \;=\; \tfrac{1}{\alpha} \cdot \vec{0} \;=\; \vec{0}.$$

Das war's.

5.2 Beispiele

5.2.1 Matrizen-Vektorräume

Die Menge $\mathbb{K}^{m\times n}$ der $m \times n$-Matrizen bildet unter Addition und skalarer Multiplikation einen $\mathbb{K}$-Vektorraum. Man überzeuge sich davon, dass die Vektorraumaxiome erfüllt sind.

5.2.2 Zahlentupel-Vektorräume

Wir nennen den $\mathbb{K}$-Vektorraum $\mathbb{K}^n$ den Vektorraum der n-Tupel oder den der n-Spaltenvektoren.

5.2.3 Der Körper selbst

Ein Körper $\mathbb{K}$ kann immer als Vektorraum $\mathbb{K}^1$ über sich selbst angesehen werden. Die Vektoraddition in $\mathbb{K}^1$ entspricht der Addition in $\mathbb{K}$, die skalare Multiplikation entspricht der Multiplikation in $\mathbb{K}$.

5.2.4 Der Null-Vektorraum Eine Menge mit genau einem Element kann für jeden Körper $\mathbb{K}$ als $\mathbb{K}$–Vektorraum aufgefasst werden, indem man das einzige Element als Null–Vektor $\vec{0}$ ansieht:

$$\mathbb{K}^0 \quad := \quad \{\vec{0}\}.$$

Die Vektoraddition und die skalare Multiplikation sind durch

$$\vec{0}+\vec{0} \;=\; \vec{0} \qquad \text{bzw.} \qquad \alpha\cdot\vec{0} \;=\; \vec{0} \quad \text{für alle } \alpha\in\mathbb{K}$$

festgelegt.

5.2.5 Vektorräume $\mathbb{K}$-wertiger Funktionen

Es sei X eine beliebige Menge. Auf der Menge $\mathbb{K}^X$ der Funktionen $X \to \mathbb{K}$ ist eine $\mathbb{K}$-Vektorraumstruktur gegegeben. Addition und skalare Multiplikation von Funktionen erfolgen „stellenweise". Für $f, \widetilde{f} \in \mathbb{K}^X$ und $\alpha \in \mathbb{K}$ sind $f+\widetilde{f}$ und αf die Funktionen

$$(f+\widetilde{f}) : \begin{cases} X & \to & \mathbb{K} \\ x & \mapsto & f(x)+\widetilde{f}(x) \end{cases} \qquad\qquad (\alpha f) : \begin{cases} X & \to & \mathbb{K} \\ x & \mapsto & \alpha f(x). \end{cases}$$

5.2.6 Frei erzeugte $\mathbb{K}$-Vektorräume

Wir nennen eine Abbildung $f : X \to \mathbb{K}$ *finit*, wenn sie höchstens an endlich vielen Stellen $x \in X$ Werte ungleich Null annimmt. Es ist klar, dass die Summe zweier finiter Abbildungen bzw. das skalare Vielfache einer finiten Abbildung wieder finit ist.

Der Vektorraum aller finiten Funktionen

$$\mathcal{F}_{\mathbb{K}}(X) \quad := \quad \Big\{ f : X \to \mathbb{K} \Big| f \text{ finit} \Big\}$$

heißt der von X über $\mathbb{K}$ *frei erzeugte Vektorraum.*

5.2.7 Körpererweiterungen Wegen der Teilmengenbeziehung

$$\mathbb{Q} \;\subseteq\; \mathbb{R} \;\subseteq\; \mathbb{C}$$

ist ein jeweils weiter rechts stehender Körper ein Vektorraum über einem weiter links stehenden Körper. Man prüfe selbst die Vektorraum-Axiome nach.

5.3 Linearkombinationen

5.3.1 Definition: Linearkombination

Es seien ein $\mathbb{K}$–Vektorraum V und eine Teilmenge $W \subseteq V$ gegeben.

Wir nennen eine finite Abbildung $\ell : W \to \mathbb{K}$ eine *Linearkombination (aus W)*.

Es gibt also endlich viele Vektoren $v_1, \ldots, v_n \in W$ und endlich viele Zahlen $\alpha_1, \ldots, \alpha_n$, so dass

$$\ell(v) = \begin{cases} \alpha_k, & \text{falls } v = v_k \text{ für ein } k \in \{1, \ldots, n\} \\ 0, & \text{sonst.} \end{cases}$$

5.3.2 Sichtweise als formale Summe

Es ist allgemein üblich, eine Linearkombination aus W als formale Summe

$$\alpha_1 \cdot v_1 + \alpha_2 \cdot v_2 + \ldots\ldots + \alpha_n \cdot v_n$$

aufzuschreiben. Für $\alpha_k = 0$ kann der k-te Summand auch weggelassen werden.

5.3.3 Wert einer Linearkombination

Ist eine solche Linearkombination (als finite Abbildung oder als formale Summe) gegeben, so kann man ihr einen Vektor $v \in V$ zuordnen, nämlich die Summe:

$$v = \alpha_1 \cdot v_1 + \alpha_2 \cdot v_2 + \ldots\ldots + \alpha_n \cdot v_n.$$

Umgekehrt sagt man, dass v als diese Linearkombination dargestellt wird.

5.3.4 Unterschied

Die feine Unterscheidung zwischen einer ,,Linearkombination" und ihrem ,,Wert" ist in der Literatur wenig ausgearbeitet. Es ist gängige Praxis, sowohl den Rechenausdruck in 5.3.2 als auch ihren Wert als Linearkombination zu bezeichnen.

Die mangelnde Präzision kann manche Unklarheiten verursachen, wie das folgende Beispiel zeigt:

5.3.5 Beispiel

Für $W = \{v_1, v_2, v_3\}$ betrachten wir die (vermeintlichen) Linearkombinationen

$$\begin{array}{rrcccc} \text{(I)} & 5 \cdot v_1 & - & 3 \cdot v_2 & & \\ \text{(II)} & 4 \cdot v_1 + v_1 & - & 3 \cdot v_2 & & \\ \text{(III)} & -3 \cdot v_2 & + & 5 \cdot v_1 & & \\ \text{(IV)} & 5 \cdot v_1 & - & 3 \cdot v_2 & + & 0 \cdot v_3 \\ \text{(V)} & 5 \cdot v_1 & - & 3 \cdot v_2 & + & 2 \cdot \vec{0} \end{array}$$

Die Werte stimmen offensichtlich alle überein. Bzgl. des Begriffs Linearkombination treten aber einige Spezialitäten in Erscheinung.

- (II) ist gar keine Linearkombination, da zum Vektor v_1 zwei Skalare gehören.

- (I), (III) und (IV) stimmen als Linearkombination überein, da zu ihnen allen die Abbildung

$$\ell : \begin{cases} W & \to & \mathbb{K} \\ v_1 & \mapsto & 5 \\ v_2 & \mapsto & -3 \\ v_3 & \mapsto & 0 \end{cases}$$

  gehört.

- (V) ist eine andere Linearkombination, da ihr die Abbildung

$$\widetilde{\ell} : \begin{cases} \{v_1, v_2, v_3, \vec{0}\} & \to & \mathbb{K} \\ v_1 & \mapsto & 5 \\ v_2 & \mapsto & -3 \\ v_3 & \mapsto & 0 \\ \vec{0} & \mapsto & 2 \end{cases}$$

  zugrundeliegt.

5.3.6 Fazit

Die in den Beispielen beschriebenen Unklarheiten sind nicht so gravierend, als dass die weitere Erschließung der Vektorraum-Theorie nur mit dauernder Berücksichtigung der abstrakten Definition 5.3.1 funktionieren würde.

Im wesentlichen genügt es, die Sichtweise ,,Linearkombinationen als formale Summe oder als Wert" im Auge zu behalten.

5.4 Linear unabhängige Mengen

5.4.1 Satz: Charakterisierung linear unabhängiger Mengen

Es sei V ein $\mathbb{K}$ -Vektorraum. Die folgenden Aussagen über eine nicht-leere Teilmenge $W \subseteq V$ sind äquivalent:

(A) (Per definitionem) W ist *linear unabhängig* (ℓ.u.).

(B) Jeder Vektor $v \in V$ kann auf **höchstens** eine Weise als Wert einer Linearkombination aus W dargestellt werden. Das heißt genauer:

Gelten mit $n \in \mathbb{N}$, paarweise verschiedenen $v_k \in W$, $\alpha_k, \beta_k \in \mathbb{K}$ die Gleichungen

$$\begin{aligned} v &= \alpha_1 v_1 + \cdots + \alpha_n v_n \\ v &= \beta_1 v_1 + \cdots + \beta_n v_n, \end{aligned}$$

so folgt:

$$\alpha_k = \beta_k \quad \text{für alle } k \in \{1, \ldots, n\}.$$

(C) Der Nullvektor kann **nur** als Wert der trivialen Linearkombination aus W geschrieben werden. Das heißt genauer:

Gilt mit $n \in \mathbb{N}$, paarweise verschiedenen $v_k \in W$ und $\alpha_k \in \mathbb{K}$ die Gleichung

$$\vec{0} = \alpha_1 v_1 + \cdots + \alpha_n v_n,$$

so folgt

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0.$$

(D) Es ist unmöglich, dass ein Vektor $w \in W$ als Linearkombination aus $W \setminus \{w\}$ dargestellt werden kann.

5.4.2 Beweis

(0) Wir zeigen die Äquivalenz der drei Aussagen (B), (C), (D) durch einen Ringschluss zwischen den negierten Aussagen: $\neg$(B) $\Rightarrow$ $\neg$(C) $\Rightarrow$ $\neg$(D) $\Rightarrow$ $\neg$(B).

(1) Gäbe es gemäß $\neg$(B) zwei verschiedene Linearkombinationen für einen Vektor v, so führt deren Subtraktion auf eine nichttriviale Linearkombination für $\vec{0}$. Das ist die Aussage $\neg$(C).

(2) Gäbe es gemäß $\neg$(C) eine nichttriviale Linearkombination für $\vec{0}$,

$$\vec{0} = \alpha_1 v_1 + \cdots + \alpha_n v_n,$$

so ist mindestens eines der α_k ungleich Null und dann kann nach v_k aufgelöst werden:

$$v_k = -\sum_{j=1, j \neq k}^{n} \frac{\alpha_j}{\alpha_k} v_j.$$

Das ist die Aussage $\neg$(D).

(3) Gäbe es gemäß $\neg$(D) einen Vektor $w \in W$, der als Linearkombination aus $W \setminus \{w\}$ geschrieben werden kann

$$w = \alpha_1 v_1 + \cdots + \alpha_n v_n,$$

so wäre der Nullvektor Wert zweier verschiedener Linearkombination aus W:

$$\begin{aligned}\vec{0} &= \alpha_1 v_1 + \cdots + \alpha_n v_n - w \\ \vec{0} &= 0\, v_1 + \cdots + 0\, v_n + 0\, w.\end{aligned}$$

Das ist aber dann $\neg$(B).

5.4.3 Test auf lineare Unabhängigkeit

Eine endliche Teilmenge $\{v_1, \ldots, v_n\} \subseteq \mathbb{K}^m$ ist linear unabhängig genau dann, wenn das $m \times n$-LGS

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

nur die Lösung $\alpha_1 = \cdots = \alpha_n = 0$ hat.

5.4.4 Begründung

Das liegt daran, dass dann der Nullvektor $\vec{0} \in \mathbb{K}^m$

$$\vec{0} = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

nur als triviale Linearkombination aus W dargestellt werden kann.

5.4.5 Beispiele Es seien die Vektoren

$$v_1 = \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

im $\mathbb{R}^3$ gegeben.

- $\{v_1, v_2, v_3\}$ ist linear unabhängig, da das LGS

  $$\begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 3 \\ -1 & 3 & 0 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

  nur $\alpha_1 = \alpha_2 = \alpha_3$ als Lösung hat.

- $\{v_1, v_3, v_4\}$ ist nicht linear unabhängig, da das LGS

  $$\begin{pmatrix} 0 & 0 & 0 \\ 2 & 3 & 0 \\ -1 & 0 & 2 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

  auch die Lösung $\alpha_1 = 6$, $\alpha_3 = -4$, $\alpha_4 = 3$ hat.

5.4.6 Satz: Eigenschaften linear unabhängiger Mengen

Es sei V ein $\mathbb{K}$-Vektorraum. Für eine Teilmenge $W \subseteq V$ gelten die folgenden Aussagen:

(i) Ist W linear unabhängig, so enthält W nicht den Nullvektor.

(ii) Für jeden Vektor $v \neq \vec{0}$ ist $\{v\}$ linear unabhängig.

(iii) Ist $\widetilde{W}$ Teilmenge einer linear unabhängigen Menge W, so ist auch $\widetilde{W}$ linear unabhängig.

(iv) Die leere Menge zählt als linear unabhängig.

5.4.7 Beweis

(i) Der Nullvektor ist immer Wert der nichttrivialen Linearkombination $\vec{0} = 1 \cdot \vec{0}$.

(ii) Der Nullvektor kann dann nur als Linearkombination $\vec{0} = 0 \cdot v$ dargestellt werden.

(iii) Wäre der Nullvektor als nichttriviale Linearkombination aus $\widetilde{W}$ darstellbar, so wäre dies auch eine nichttriviale Linearkombination aus W.

(iv) Man kann diese Aussage einer genauen Analyse der Definition entnehmen. Notfalls kann man das einfach der Definition hinzufügen.

5.5 Linear abhängige Mengen

5.5.1 Satz: Charakterisierung linear abhängiger Mengen

Es sei V ein $\mathbb{K}$ -Vektorraum.
Die folgenden Aussagen über eine nichtleere Teilmenge $W \subseteq V$ sind äquivalent:

(A) (Per definitionem) W ist *linear abhängig* (ℓ.a.).

(B) Es gibt einen Vektor $v \in V$, der als Wert von **mindestens** zwei verschiedenen Linearkombinationen aus W dargestellt werden kann.

(C) Der Nullvektor kann als Wert einer nicht-trivialen Linearkombination aus W dargestellt werden.

(D) Es gibt einen Vektor $w \in W$, der als Linearkombination aus $W \setminus \{w\}$ dargestellt werden kann.

5.5.2 Beweis Es handelt sich jeweils um die Negation der entsprechenden Aussage aus Satz 5.4.1.

5.5.3 Weitere Eigenschaften linear abhängiger Mengen

Für eine Teilmenge $W \subseteq V$ gelten die folgenden Aussagen:

(i) Enthält W den Nullvektor, so ist W linear abhängig.

(ii) Ist $\widetilde{W}$ Obermenge einer linear abhängigen Menge W, so ist auch $\widetilde{W}$ linear abhängig.

5.6 Erzeugendensysteme

5.6.1 Definition: Erzeugendensystem

Es sei V ein $\mathbb{K}$-Vektorraum. Eine Teilmenge W von V heißt *Erzeugendensystem* von V, wenn jeder Vektor $v \in V$ auf **mindestens** eine Weise als Linearkombination aus W dargestellt werden kann.

5.7 Basen

5.7.1 Definition: Basis

Die folgenden Aussagen über eine nicht-leere Teilmenge W eines $\mathbb{K}$-Vektorraums V sind äquivalent:

(A) (Per definitionem) W ist Basis von V.

(B) Jeder Vektor $v \in V$ kann auf **genau** eine Weise als Wert einer Linearkombination aus W dargestellt werden. Das heißt genauer:

Zu jedem $v \in V$ gibt es eine Zahl $n \in \mathbb{N}$ und dann paarweise verschiedene $v_k \in W$, $\alpha_k \in \mathbb{K}$, $k = 1, \ldots, n$, so dass

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n.$$

Es gibt keine zweite solche Linearkombination.

(C) W ist linear unabhängig und ein Erzeugendensystem.

Zusatz: Die leere Menge wird als Basis des Nullvektorraums $\{\vec{0}\}$ angesehen.

5.7.2 Beispiel: Kanonische Basis im $\mathbb{K}^n$

Im $\mathbb{K}^n$ definieren wir die Vektoren

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{mit der 1 in der } j\text{–ten Zeile.}$$

Die Menge

$$E = \{e_j | j = 1, \ldots, n\}$$

ist eine Basis des $\mathbb{K}^n$. Sie heißt die *kanonische Basis* oder *Standardbasis* von $\mathbb{K}^n$.

Begründung: Jeder Vektor $v \in \mathbb{K}^n$ lässt sich in dieser Basis darstellen:

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = v_1 e_1 + \cdots + v_n e_n.$$

Es ist offensichtlich, dass diese Darstellung eindeutig ist.

5.7.3 Beispiel: $\mathbb{K}$-wertige Funktionen

Im Vektorraum $\mathbb{K}^X$ aller $\mathbb{K}$-wertigen Funktionen auf X definieren wir für jedes $a \in X$ die Funktion e_a durch

$$e_a : \begin{cases} X & \to & \mathbb{K} \\ x & \mapsto & \begin{cases} 1, & \text{falls } x = a, \\ 0, & \text{sonst.} \end{cases} \end{cases}$$

Die Menge

$$E = \{e_a | a \in X\}$$

ist linear unabhängig.

Begründung: Gilt für endlich viele $e_{a_1}, \ldots, e_{a_n} \in V$ und $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$

$$\vec{0} = \alpha_1 e_{a_1} + \cdots + \alpha_n e_{a_n},$$

so folgt $\alpha_j = 0$ für alle $j \in \{1, \ldots, n\}$.

Im Fall eines unendlichen X ist die Menge E aber kein Erzeugendensystem — und damit keine Basis — von $\mathbb{K}^X$, da sich beispielsweise die Konstant-1-Funktion $(1, 1, 1, \ldots)$ nicht als Linearkombination (endlich viele Summanden!) aus E darstellen lässt.

Hat der Vektorraum der Funktionen in diesem Fall überhaupt eine Basis?

5.7.4 Beispiel: $\mathbb{K}$-wertige finite Funktionen

Die Menge E ist aber eine Basis des Vektorraums $\mathcal{F}_{\mathbb{K}}(X)$ der finiten Funktionen. Für jede finite Funktion $f : \mathbb{K} \to X$ gibt es nämlich eine Darstellung

$$f = \alpha_1 e_{a_1} + \cdots + \alpha_n e_{a_n},$$

wobei die Stellen $a_1, \ldots, a_n$ die Stellen sind, an denen f die Werte $\alpha_1, \ldots, \alpha_n \neq 0$ annimmt.

5.7.5 Beispiel: Der $\mathbb{R}$-Vektorraum $\mathbb{C}$

Der $\mathbb{R}$–Vektorraum $\mathbb{C}$ besitzt die Menge $\{1, i\}$ als Basis. Jede komplexe Zahl z läßt sich nämlich schreiben als $z = x + iy$. Außerdem sind die reellen Zahlen x, y durch z eindeutig bestimmt.

5.7.6 Satz: Ergänzung, Herausnahme und Austausch von Vektoren

Es sei W eine Teilmenge des $\mathbb{K}$–Vektorraums V. Dann gilt:

(i) Ist W linear unabhängig, aber kein Erzeugendensystem, so gibt es einen Vektor $w \in V \setminus W$, so dass $W \cup \{w\}$ immer noch linear unabhängig ist.

(ii) Ist W ein Erzeugendensystem, aber nicht linear unabhängig, so gibt es einen Vektor $w \in W$, so dass $W \setminus \{w\}$ immer noch ein Erzeugendensystem ist.

(iii) (Austauschlemma[2]) Ist W eine Basis, so gibt es zu jedem Vektor $v \in V \setminus \{\vec{0}\}$ einen Vektor $w \in W$, so dass

$$\widetilde{W} := (W \setminus \{w\}) \cup \{v\}$$

ebenfalls eine Basis ist.

Genauer: Hat der Vektor v die Darstellung

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

als Linearkombination aus W, so kann er gegen jeden Vektor $v_k \in W$, für den $\alpha_k \neq 0$ in dieser Darstellung ist, ausgetauscht werden.

5.7.7 Beweis

Zu (i) Da W kein Erzeugendensystem ist, gibt es einen Vektor $w \in V$, der nicht als Linearkombination aus W darstellbar ist.

Wir zeigen jetzt, dass $W \cup \{w\}$ linear unabhängig ist. Dazu betrachten wir eine beliebige Linearkombination aus $W \cup \{w\}$, die den Nullvektor darstellt:

$$\vec{0} = \alpha \cdot w + \sum_{j=1}^{n} \alpha_j v_j.$$

1. Fall: $\alpha = 0$. Dann sind wegen der linearen Unabhängigkeit von W auch die Zahlen $\alpha_j = 0$.

Es sind also alle Skalare in der Linearkombination Null, nach Satz 5.4.1 ist $W \cup \{w\}$ linear unabhängig.

2. Fall: $\alpha \neq 0$. Daraus folgt, dass w als Linearkombination aus W darstellbar ist:

$$w = \sum_{j=1}^{n} \frac{-\alpha_j}{\alpha} v_j$$

Dies widerspricht aber der am Anfang des Beweises konstatierten Eigenschaft von w.

Zu (ii): W ist nicht linear unabhängig, also gibt es nach Satz 5.4.1 einen Vektor $w \in W$, der als Linearkombination von n anderen Vektoren $v_j \in W \setminus \{w\}$ dargestellt werden kann:

$$w = \sum_{j=1}^{n} \alpha_j v_j.$$

[2] Ein Lemma ist ein Hilfssatz, der zum Beweis eines anderen Satzes gebraucht wird.

Ein beliebiger Vektor $v \in V$ ist nach Voraussetzung als Linearkombination von w und m anderen Vektoren $p_j \in W \setminus \{w\}$ darstellbar:

$$v = \beta w + \sum_{j=1}^{m} \beta_j p_j.$$

Daraus folgt aber:

$$v = \beta \cdot \big(\sum_{j=1}^{n} \alpha_j v_j\big) + \sum_{j=1}^{m} \beta_j p_j = \sum_{j=1}^{n} \beta \alpha_j v_j + \sum_{j=1}^{m} \beta_j p_j.$$

Also ist v auch als Linearkombination von $W \setminus \{w\}$ darstellbar.

Zu (iii) v ist als Linearkombination aus W darstellbar:

$$v = \sum_{j=1}^{n} \alpha_j v_j. \qquad (*)$$

Wegen $v \neq \vec{0}$ gibt es ein $k \in \{1, \ldots, n\}$, so dass

$$\alpha_k \neq 0.$$

Wir beweisen, dass die Menge $\widetilde{W} := (W \setminus \{v_k\}) \cup \{v\}$ linear unabhängig und ein Erzeugendensystem ist.

1. $\widetilde{W}$ ist ein Erzeugendensystem. Ist $p \in V$ ein beliebiger Vektor, so ist er als Linearkombination aus W, das heißt evtl. von v_k und m anderen Vektoren v'_j aus W, darstellbar:

   $$p = \beta v_k + \sum_{j=1}^{m} \beta_j v'_j.$$

   Wegen $(*)$ ist

   $$v_k = \frac{1}{\alpha_k} \cdot \Big(v - \sum_{j=1, j\neq k}^{n} \alpha_j v_j\Big).$$

   Daraus folgt aber:

   $$\begin{aligned} p &= \beta \cdot \Big[\frac{1}{\alpha_k} \cdot \Big(v - \sum_{j=1, j\neq k}^{n} \alpha_j v_j\Big)\Big] + \sum_{j=1}^{m} \beta_j v'_j = \\ &= \frac{\beta}{\alpha_k} v - \sum_{j=1, j\neq k}^{n} \frac{\beta\, \alpha_j}{\alpha_k} v_j + \sum_{j=1, j\neq k}^{m} \beta_j v'_j. \end{aligned}$$

   Also ist p als Linearkombination von $\widetilde{W}$ darstellbar.

2. $\widetilde{W}$ ist linear unabhängig. Es sei

$$\vec{0} \;=\; \gamma v + \sum_{j=1}^{\ell} \gamma_j v'_j \qquad \text{mit} \qquad v'_j \in \widetilde{W}$$

eine Darstellung des Nullvektors als Linearkombination von $\widetilde{W}$.

1. Fall: Ist $\gamma = 0$, so ist

$$\vec{0} \;=\; \sum_{j=1}^{\ell} \gamma_j v'_j.$$

eine Linearkombination aus W. Da W linear unabhängig ist, folgt $\gamma_j = 0$ für alle $j = 1, \ldots, \ell$. Es folgt, dass $\widetilde{W}$ linear unabhängig ist.

2. Fall: Ist $\gamma \neq 0$, so gilt

$$\vec{0} \stackrel{(*)}{=} \gamma\Big(\sum_{j=1}^{n} \alpha_j v_j\Big) + \sum_{j=1}^{\ell} \gamma_j v'_j = \gamma\alpha_k\, v_k + \sum_{j=1, j\neq k}^{n} \gamma\alpha_j v_j + \sum_{j=1}^{\ell} \gamma_j v'_j.$$

Aufgrund von $\gamma\alpha_k \neq 0$ kann aber dann v_k als Linearkombination von anderen Vektoren aus W dargestellt werden im Widerspruch dazu, dass W linear unabhängig ist, vgl. Satz 5.4.1. Dieser Fall kann also nicht eintreten.

5.7.8 Steinitz'scher Austauschsatz Es sei V ein $\mathbb{K}$-Vektorraum. Weiter seien

- B eine Basis von V und
- W eine linear unabhängige endliche Teilmenge von V.

Dann gibt es eine Teilmenge A von B, so dass die Menge

$$B^{\text{neu}} \;:=\; (B \setminus A) \,\cup\, W$$

(A wird aus B entfernt und W eingefügt) wieder eine Basis von V mit gleicher Mächtigkeit wie B ist.

5.7.9 Beweis

Man könnte auf die Idee kommen, den Beweis durch Hinweis auf die mehrfache Anwendung des Austauschlemmas 5.7.6 (iii) als erbracht anzusehen. Tatsächlich könnte es aber passieren, dass ein in B eingefügter Vektor $v \in W$ bei einem nachfolgenden Schritt wieder entfernt wird. Wir müssen also genauer hinsehen.

(1) Wir können annehmen, dass W und B disjunkt sind.

(2) Wir beweisen die Aussage durch Induktion über die Anzahl $n \in \mathbb{N}$ der Elemente von W. Der Fall $n = 1$ ist bereits durch das Austauschlemma abgedeckt.

(3) Für den Induktionsschluss sei also $|W| = n+1$. Es sei W' eine Teilmenge von W mit $|W'| = n$. Aufgrund der Induktionsvoraussetzung existiert eine Teilmenge A' von B, so dass

$$B^{\text{neu}'} \quad := \quad (B \setminus A') \,\dot{\cup}\, W'$$

eine Basis ist mit $|B^{\text{neu}'}| = |B|$. ($\dot{\cup}$ heißt ,,disjunkt")

(4) Der (einzige) Vektor $w \in W \setminus W'$ besitzt eine Darstellung

$$w \quad = \quad \sum_{j=1}^{m} \beta_j p_j + \sum_{j=1}^{n} \alpha_j v_j$$

mit Vektoren $p_j \in B \setminus A'$ und Vektoren $v_j \in W'$. Angenommen, alle β_j wären Null. Dann wäre aber

$$w \quad = \quad \sum_{j=1}^{n} \alpha_j v_j$$

im Widerspruch zur linearen Unabhängigkeit von W. Es existiert also ein $\beta_j \neq 0$, sagen wir, es ist β_k.

(5) Dann kann aber nach dem Austauschlemma der Vektor p_k aus $B^{\text{neu}'}$ entfernt und der Vektor w zu $B^{\text{neu}'}$ hinzugefügt werden. Es entsteht einen neue Basis, die wir B^{neu} nennen. Für sie gilt dann

$$\begin{aligned} B^{\text{neu}} \quad &= \quad (B^{\text{neu}'} \setminus \{p_k\}) \,\dot{\cup}\, \{w\} \\ &= \quad ((B \setminus A') \,\dot{\cup}\, W') \setminus \{p_k\}) \,\dot{\cup}\, \{w\} \\ &\overset{(*)}{=} \quad ((B \setminus (\underbrace{A' \,\dot{\cup}\, \{p_k\}}_{=:\,A}) \,\dot{\cup}\, (\underbrace{W' \dot{\cup} \{w\}}_{=W}) \\ &= \quad (B \setminus A) \,\dot{\cup}\, W \end{aligned}$$

Im Schritt $(*)$ haben wir benutzt, dass $p_k \in B \setminus A'$, was wegen (1) auch $p_k \notin W$ bedeutet.

(6) Wegen $p_k \notin W$ ist auch $p_k \neq w$ und deshalb $|\widetilde{B}| = |\widetilde{B}'| = |B|$.

5.8 Existenz von Basen

5.8.1 Satz Es sei V ein $\mathbb{K}$-Vektorraum. Betrachte für eine Teilmenge W die beiden Aussagen

(A) Ist W ein Erzeugendensystem, so gibt es eine Basis B mit $B \subseteq W$. (Basisauswahlsatz)

(B) Ist W linear unabhängig, so gibt es eine Basis B mit $W \subseteq B$. (Basisergänzungssatz)

Dann

(i) (A) ist gültig unter der Voraussetzung, dass W endlich ist.

(ii) (B) ist gültig unter der Voraussetzung, dass W endlich ist und eine Basis existiert.

(iii) (B) ist generell gültig.

5.8.2 Beweis

(i) Unter der Voraussetzung, dass W endlich ist, kann der Beweis mittels des Herausnahmeverfahrens geführt werden:

Wir nehmen gemäß Satz 5.7.6 (ii) sukzessive Vektoren aus W heraus, bis wir nach endlich vielen Schritten bei einer linear unabhängigen Menge angekommen sind. Das Verfahren führt zum Ziel, da ja (spätestens) eine 1-Teilmenge von W erreicht wird, die ja linear unabhängig ist.

(ii) Dies ist einfach eine Umformulierung des Steinitz'schen Austauschsatzes.

(iii) Durch ein Axiom der Mengenlehre, das sogenannte *Auswahlaxiom* oder das dazu äquivalente *Zorn'sche Lemma* wird sichergestellt, dass auch in diesem Fall eine Basis B mit $W \subseteq B$ existiert.

5.8.3 Folgerung Jeder $\mathbb{K}$-Vektorraum besitzt eine Basis.

5.8.4 Beweis Man beachte, dass die Menge $\{w\}$ mit $w \neq 0$ immer linear unabhängig ist. Wende dann Teil (iii) des letzten Satzes 5.8.1 an!

5.9 Dimension eines Vektorraums

5.9.1 Satz Der $\mathbb{K}$–Vektorraums V habe eine endliche Basis B.

Ist W eine beliebige linear unabhängige Teilmenge von V, so gilt:

(i) $|W| \leq |B|$.

(ii) $|W| = |B| \quad \Longleftrightarrow \quad W$ ist ebenfalls eine Basis von V.

Ist W ein beliebiges Erzeugendensystem von V, so gilt:

(iii) $|W| \geq |B|$.

(iv) $|W| = |B| \quad \Longleftrightarrow \quad W$ ist ebenfalls eine Basis von V.

5.9.2 Beweis

Zu (i): Angenommen, W hat eine größere Mächtigkeit als B. Wähle dann eine (immer noch linear unabhängige) Teilmenge $\widetilde{W}$ von W mit $|\widetilde{W}| = |B|$.

Gemäß Steinitz'schem Austauschsatz 5.7.8 ersetzen wir alle Vektoren aus B durch Vektoren aus $\widetilde{W}$ und schließen daraus, dass $\widetilde{W}$ eine Basis ist.

Dann gibt es einen Vektor $v \in W \setminus \widetilde{W}$, der als Linearkombination von $\widetilde{W} \subseteq W \setminus \{v\}$ dargestellt werden kann. Das ist ein Widerspruch zur linearen Unabhängigkeit von W.

Zu (ii)$^{\Rightarrow}$: Gemäß Steinitz'schem Austauschsatz 5.7.8 ersetzen wir alle Vektoren aus B durch Vektoren aus W und schließen daraus, dass W eine Basis ist.

Zu (ii)$^{\Leftarrow}$: Gemäß (i) ist $|W| \leq |B|$. Also ist auch W eine endliche Basis und wir können die Rollen von W und B in (i) vertauschen. Es folgt $|B| \leq |W|$.

Zu (iii): Wir formulieren die gegenteilige Behauptung:

> Es existiert ein Erzeugendensystem W für V mit $|W| < |B|$.

Diese Menge W ist nicht linear unabhängig. Anderenfalls wäre sie eine Basis und hätte dann aufgrund (ii)$^{\Leftarrow}$ die Mächtigkeit $|W| = |B|$.

Deshalb können nach Satz 5.7.6(ii) sukzessive aus W Vektoren entfernt werden, bis ein linear unabhängiges Erzeugendensystem, d.h. eine Basis, entsteht. Diese hätte aber weniger Elemente als B — im Widerspruch zu (ii)$^{\Leftarrow}$.

Zu (iv)$^{\Rightarrow}$: Wäre ein Erzeugendensystem mit $|W| = |B|$ Elementen keine Basis, so könnte man diese Menge nach Satz 5.7.6(ii) zu einer Basis verkleinern. Dann gäbe es aber zwei endliche Basen mit unterschiedlicher Mächtigkeit — im Widerspruch zu (ii)$^{\Leftarrow}$.

Zu (iv)$^{\Leftarrow}$: W ist als Basis auch linear unabhängig. Deshalb ist die Aussage (ii)$^{\Leftarrow}$ anwendbar.

5.9.3 Folgerung: Gleichmächtigkeit von Basen

Hat ein $\mathbb{K}$-Vektorraum eine endliche Basis B so hat jede andere Basis $\widetilde{B}$ gleiche Mächtigkeit.

5.9.4 Definition: Dimension

Aufgrund der Folgerung 5.9.3 ist die folgende Definition sinnvoll:

Die Mächtigkeit einer Basis B eines $\mathbb{K}$–Vektorraums V (mit endlicher Basis) heißt die *Dimension* des Vektorraums V. Man schreibt dafür

$$\dim V \quad := \quad |B|.$$

Hat ein Vektorraum keine endliche Basis, so heißt er *endlich–dimensional* und man schreibt $\dim V = \infty$. Es lässt sich auch in diesem Fall beweisen, dass alle Basen gleiche Mächtigkeit haben.

5.9.5 Beachte

Bei der Festlegung der Dimension eines Vektorraums kommt es darauf an, über welchem Körper er betrachtet wird. Um dies genauer zu betonen, müsste man eigentlich von der $\mathbb{K}$–*Dimension* sprechen und die Schreibweise $\dim_{\mathbb{K}} V$ benutzen.

5.9.6 Beispiele

- Der Vektorraum $\mathbb{K}^n$ hat die Dimension n, da die kanonische Basis 5.7.2 n Elemente enthält.
- Jeder Körper $\mathbb{K}$ hat als Vektorraum über sich selbst die Dimension 1, da $\{1\}$ eine Basis ist.
- Der $\mathbb{R}$–Vektorraum $\mathbb{C}$ hat die Dimension $\dim_{\mathbb{R}} \mathbb{C} = 2$.
- Der Null-Vektorraum $\{\vec{0}\}$ hat die Dimension Null, da die leere Menge eine Basis ist.
- Der $\mathbb{Q}$-Vektorraum $\mathbb{R}$ hat Dimension ∞. Eine Begründung wird hier nicht gegeben.

6 Operationen mit Vektorräumen

6.1 Unterräume

6.1.1 Erzeugnis einer Teilmenge

Es sei W wieder Teilmenge eines $\mathbb{K}$-Vektorraums V. Die Menge (der Werte) der Linearkombinationen aus W heißt das *Erzeugnis* oder der *Span* von W:

$$\operatorname{span} W = \langle W \rangle \ := \Big\{ \alpha_1 w_1 + \cdots + \alpha_n w_n \ \Big| \ n \in \mathbb{N}, \alpha_k \in \mathbb{K}, w_k \in W \text{ für alle } k = 1, \ldots, n \Big\}$$

Ist die Menge $W = \{w_1, \ldots, w_n\}$ endlich, so schreibt man auch

$$\langle W \rangle = \langle w_1, \ldots, w_n \rangle.$$

Man definiert zusätzlich: $\operatorname{span} \varnothing = \{\vec{0}\}$.

6.1.2 Beispiele

- Ist W ein Erzeugendensystem, so gilt $\langle W \rangle = V$.
- Für eine beliebige Teilmenge $W \subseteq V$ gilt: $\vec{0} \in \langle W \rangle$.

  Begründung: Mit $w \in W$ beliebig gilt $\vec{0} = 0 \cdot w$, also ist $\vec{0}$ als Linearkombination aus W darstellbar.
- Es sei $W = \langle w \rangle$ mit einem Vektor $w \neq \vec{0}$. Dann gilt:

  $$\langle w \rangle = \{\alpha \cdot w \,|\, \alpha \in \mathbb{K}\}.$$

  Man nennt dies auch die durch $w \in V$ definierte *Gerade* (durch den Ursprung) im Vektorraum.
- Es sei $W = \langle w, \widetilde{w} \rangle$ linear unabhängig. Dann gilt:

  $$\langle w, \widetilde{w} \rangle = \{\alpha \cdot w + \widetilde{\alpha} \cdot \widetilde{w} \,|\, \alpha, \widetilde{\alpha} \in \mathbb{K}\}.$$

  Man nennt diese Menge auch die durch w und $\widetilde{w}$ aufgespannte *Ebene* (durch den Ursprung) im Vektorraum.

6.1.3 Definition und Satz: Unterraum

Die folgenden Aussagen über eine Teilmenge U des $\mathbb{K}$-Vektorraums V sind äquivalent:

(A) (Per definitionem) U heißt *Unterraum von* V.

(B) U ist bzgl. der von V her gegebenen Verknüpfungen selbst ein Vektorraum.

(C) Für alle $u_1, u_2 \in U$ gilt $u_1 + u_2 \in U$ und für alle $\alpha \in \mathbb{K}$, $u \in U$ gilt $\alpha\, u \in U$.

(D) Für alle $\alpha_1, \alpha_2 \in \mathbb{K}, u_1, u_2 \in U$ gilt

$$\alpha_1\, u_1 + \alpha_2\, u_2 \in U.$$

6.1.4 Beweis

(C) ist eine Präzisierung der Aussage (B).

(D) ist eine Zusammenfassung der beiden Aussagen von (C).

6.1.5 Satz: Span ist Unterraum

Es sei W eine Teilmenge von V. Dann ist das Erzeugnis $\operatorname{span} W$ ein Unterraum von V.

6.1.6 Beweis

Es seien $u_1, u_2 \in \operatorname{span} W$, $\alpha_1, \alpha_2 \in \mathbb{K}$. Die beiden Vektoren sind Linearkombinationen aus W:

$$u_1 = \sum_{j=1}^{n} \beta_j w_j \quad \text{und} \quad u_2 = \sum_{j=1}^{m} \gamma_j w'_j$$

Für beliebige $\alpha_1, \alpha_2 \in \mathbb{K}$ gilt dann

$$\alpha_1 u_1 + \alpha_2 u_2 = \sum_{j=1}^{n} \alpha_1 \beta_j w_j + \sum_{j=1}^{m} \alpha_2 \gamma_j w'_j.$$

Dieser Vektor ist also ebenfalls der Wert einer Linearkombination aus W, also enthalten in $\operatorname{span} W$.

6.1.7 Beispiele

- Jeder Vektorraum V besitzt die sogenannten *trivialen* Unterräume V und $\{\vec{0}\}$.
- Geraden oder Ebenen durch den Ursprung sind Unterräume.
- Es sei $A \in \mathbb{K}^{m \times n}$. Man überlege, dass die Lösungsmenge $\mathcal{L}(A|\vec{0})$ des LGS $Ax = \vec{0}$ ein Unterraum von $\mathbb{K}^n$ ist.

6.1.8 Satz: Dimension und Unterraum Es sei U ein Unterraum von V.

(i) Es ist: $\dim U \leq \dim V$.

(ii) Ist V endlich-dimensional, so gilt die Implikation: $\dim U = \dim V \Rightarrow U = V$.

6.1.9 Beweis

(i) Es sei B_U eine Basis von U.

Ist v ein beliebiger Vektor aus V, so lässt er sich

- im Fall $v \in U$ auf genau eine Weise,
- im Fall $v \notin U$ auf keine Weise,
- im allgemeinen also auf höchstens eine Weise

als Linearkombination von B_U darstellen. Das aber bedeutet, dass B_U eine linear unabhängige Teilmenge von V ist, die zu einer Basis B_V von V ergänzt werden kann.

Daraus folgt aber $|B_U| \leq |B_V|$ und das ist genau die Aussage von (i).

(ii) Nach Satz 5.7.8 können wir eine Basis B_U von U zu einer Basis B_V von V ergänzen. Wegen $\dim U = \dim V$ muss dann aber $B_V = B_U$ gelten. Da jeder Vektor $v \in V$ als Linearkombination von B_V dargestellt werden kann, kann er auch als Linearkombination von B_U dargestellt werden. Damit gilt $v \in U$ für jeden beliebigen Vektor $v \in V$, also $V = U$.

6.1.10 Satz: Schnitt und innere Summe

Es seine U_1, U_2 Unterräume eines $\mathbb{K}$-Vektorraums V.

(i) Die Menge $U_1 \cap U_2$ ist ein Unterraum von V, der sogenannte *Schnittraum*.

(ii) Die *innere Summe* von U_1 und U_2, das ist der von U_1 und U_2 erzeugte Raum

$$U_1 + U_2 \quad := \quad \operatorname{span}(U_1 \cup U_2) \;=\; \{u_1 + u_2 | u_1 \in U_1, u_2 \in U_2\},$$

ist ein Unterraum von V.

(iii) Es gilt die Teilmengenrelation

$$U_1 \cup U_2 \quad \subseteq \quad U_1 + U_2.$$

Beachte aber, dass $U_1 \cup U_2$ im allgemeinen kein Unterraum ist.

6.1.11 Beweis Fehlt hier!

6.1.12 Satz Sind U_1, U_2 endlich-dimensionale Unterräume des $\mathbb{K}$-Vektorraums V, so gilt

$$\dim U_1 + \dim U_2 \quad = \quad \dim(U_1 \cap U_2) + \dim(U_1 + U_2).$$

Machen Sie sich diese Gleichung anhand verschiedener Beispiele (Geraden, Ebenen im 3–dimensionalen Anschauungsraum) klar.

6.1.13 Beweis

(0) Der Beweis lässt sich durchsichtiger ausführen, wenn wir die Bezeichnungen ändern. Wir setzen

$$U \;:=\; U_1 \cap U_2, \quad W \;:=\; U_1 + U_2, \quad P \;:=\; U_1, \quad Q \;:=\; U_2$$

und wollen zeigen, dass

$$\dim P + \dim Q \;=\; \dim U + \dim W.$$

(1) Eine Basis $B_U = \{u_1, \dots, u_n\}$ von U kann sowohl zu einer Basis $B_P = \{u_1, \dots, u_n, p_1, \dots, p_m\}$ von P als auch zu einer Basis $B_Q = \{u_1, \dots, u_n, q_1, \dots, q_\ell\}$ von Q ergänzt werden. Wir zeigen jetzt, dass

$$B_W \;:=\; \{u_1, \dots, u_n, p_1, \dots, p_m, q_1, \dots, q_\ell\}$$

eine Basis von W ist.

(2) Zunächst ist klar, dass B_W ein Erzeugendensystem für W ist, denn es kann jeder Vektor aus $\langle P \cup Q \rangle$ als Linearkombination von Vektoren aus P und Vektoren aus Q, damit als Linearkombination der Basen B_P und B_Q, damit als Linearkombination von B_W geschrieben werden.

(3) Um die lineare Unabhängigkeit von B_W zu zeigen, setzen wir den Nullvektor als Linearkombination an:

$$\vec{0} \;=\; \underbrace{\sum_{j=1}^{n} \alpha_j u_j}_{=:\,u} + \underbrace{\sum_{j=1}^{m} \beta_j p_j}_{=:\,p} + \underbrace{\sum_{j=1}^{\ell} \gamma_j q_j}_{=:\,q}. \qquad (*)$$

Daraus folgt aber, dass der Vektor $q \in Q$ wegen

$$q \;=\; -u - p \in P$$

in $U = P \cap Q$ enthalten ist, deshalb als Linearkombination von B_U geschrieben werden kann:

$$\sum_{j=1}^{\ell} \gamma_j q_j \;=\; q \;=\; \sum_{j=1}^{k} \delta_j u_j.$$

Diese Gleichung stellt q als Linearkombinationen von zwei disjunkten Teilmengen von B_Q dar, was nur im Fall $q = 0$ möglich ist.

Völlig analog zeigt man, dass $p = 0$ ist, es folgt mit $(*)$, dass $u = \vec{0}$.

Die lineare Unabhängigkeit B_U, B_P, B_Q impliziert nun, dass alle Koeffizienten in $(*)$ Null sein müssen.

(4) Jetzt kann man leicht nachrechnen:

$$\begin{aligned} \dim P + \dim Q &= (n+m) + (n+\ell) = n + (n+m+\ell) \\ &= \dim(P \cap Q) + \dim(P+Q). \end{aligned}$$

6.2 Äußere Summe

6.2.1 Definition Es seien V_1, V_2 zwei Vektorräume über dem Körper $\mathbb{K}$. Wir bilden das kartesische Produkt

$$V_1 \times V_2 \quad = \quad \{(v_1, v_2) | v_1 \in V_1, v_2 \in V_2\}$$

dieser zwei Mengen und definieren die Addition und skalare Multiplikation für solche Paare komponentenweise:

$$\begin{aligned} (v_1, v_2) + (\widetilde{v}_1 + \widetilde{v}_2) \quad &:= \quad (v_1 + \widetilde{v}_1, v_2 + \widetilde{v}_2) \\ \alpha \cdot (v_1, v_2) \quad &:= \quad (\alpha \cdot v_1, \alpha \cdot v_2) \end{aligned}$$

Es ist leicht nachzuprüfen, dass so ein neuer $\mathbb{K}$-Vektorraum entsteht. Er heißt die *(äußere) direkte Summe* (evtl. auch Produkt) der beiden Vektorräume V_1 und V_2 und wird als $V_1 \oplus V_2$ geschrieben.

6.2.2 Satz Situation wie oben.

- Ist B_1 eine Basis für V_1 und B_2 eine Basis für V_2, so ist die Teilmenge

  $$\{(w_1, \vec{0}) | w_1 \in B_1\} \ \cup \ \{(\vec{0}, w_2) | w_2 \in B_2\} \ \subseteq V_1 \oplus V_2$$

  eine Basis von $V_1 \oplus V_2$.

- Sind die Dimensionen von V_1 und V_2 endlich, so gilt

  $$\dim(V_1 \oplus V_2) \quad = \quad \dim V_1 + \dim V_2.$$

(ii) ist eine direkte Konsequenz von (i). Der Beweis für (i) besteht wieder darin, dass man die genannte Menge als linear unabhängig und Erzeugendensystem erweist.

6.2.3 Bemerkungen

- Die Definition und der Satz können für endlich viele Vektorräume verallgemeinert werden.

- Es gibt auch die Möglichkeit, Summen für unendlich viele Vektorräume zu bilden.

- Die Menge der Zeilenvektoren ist $\mathbb{K}^{1\times n} = \mathbb{K} \oplus \mathbb{K} \oplus \cdots \oplus \mathbb{K}$.

- Sind U_1 und U_2 zwei Unterräume eines Vektorraums V, so kennen wir inzwischen

  – die innere Summe

  $$U_1 + U_2 \;=\; \{u_1 + u_2 \,|\, u_1 \in U_1, u_2 \in U_2\} \subseteq V$$

  mit Dimension $\dim(U_1 + U_2) \;=\; \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$.

  – die äußere Summe

  $$U_1 \oplus U_2 \;=\; \{(u_1, u_2) \,|\, u_1 \in U_1, u_2 \in U_2\} \subseteq V \times V$$

  mit Dimension $\dim(U_1 + U_2) \;=\; \dim U_1 + \dim U_2$.

  Im Fall $U_1 \cap U_2 = \{\vec{0}\}$ sind die beiden Summanden als Mengen verschieden, es besteht aber eine ,,kanonische" bijektive Abbildung

  $$\begin{cases} U_1 \oplus U_2 & \to & U_1 + U_2 \\ (u_1, u_2) & \mapsto & u_1 + u_2, \end{cases}$$

  aufgrund derer die beiden Vektorräume ,,isomorph" (= gleichstrukturiert) sind.

- Die beiden Unterräume $U_1 \times \{\vec{0}\}$ und $\{\vec{0}\} \times U_2$ von $U_1 \oplus U_2$ können auch kanonisch mit U_1 bzw. U_2 identifiziert werden.

  Deshalb trifft man häufig auf die — mengentheoretisch nicht haltbare — Formulierung, dass U_1 und U_2 Unterräume, das heißt Teilmengen, von $U_1 \oplus U_2$ wären.

6.3 Äquivalenzrelationen und Äquivalenzklassen

6.3.1 Zerlegung einer Menge Es seien X und I zwei Mengen.

Zu jedem $i \in I$ sei X_i eine nicht-leere Teilmenge von X. Wir bilden die Menge aller dieser Teilmengen $\mathcal{X} = \{X_i | i \in I\}$.

$\mathcal{X}$ heißt eine *Zerlegung (= Partition)* von X, wenn die beiden Bedingungen

$$\begin{aligned} X &= \bigcup_{i \in I} X_i \qquad \text{(Überdeckung)} \\ X_i \cap X_j &= \varnothing, \quad \text{falls} \quad i \neq j \qquad \text{(Keine Überlappung)} \end{aligned}$$

erfüllt sind.

Mit

$$\mathcal{Z}(X) = \{\mathcal{X} | \mathcal{X} \text{ ist Zerlegung von } X\}$$

bezeichnen wird die Menge aller Zerlegungen von X.

6.3.2 Beispiel

Für $X = \{x, y, z\}$ ist

$$\mathcal{Z}(X) = \Big\{ \{\{x\}, \{y\}, \{z\}\}, \ \{\{x\}, \{y, z\}\}, \ \{\{y\}, \{x, z\}\}, \ \{\{z\}, \{x, y\}\}, \ \{\{x, y, z\}\}, \Big\}$$

6.3.3 Bemerkungen

- I heißt in diesem Zusammenhang auch Indexmenge.
- Vielleicht wollen Sie überlegen, dass $\mathcal{Z}(X)$ ein Element von $\mathcal{P}(\mathcal{P}(\mathcal{P}(X)))$ — und damit ein wohldefiniertes mathematisches Objekt — ist.
- Für jede Menge X sind $\{X\}$ und $\{\{x\} | x \in X\}$ Zerlegungen für X.
- Es sei $|X| = n$. Bestimme $|\mathcal{Z}(X)|$ für $n = 1, 2, 3, 4, \ldots$

6.3.4 Verknüpfung und Zerlegung

Es sei X eine Menge und $\mathcal{X}$ eine Zerlegung. Ist nun auf X zusätzlich eine Verknüpfung

$$\star : \begin{cases} X \times X & \to \quad X \\ (x, y) & \mapsto \quad x \star y \end{cases} \qquad \text{(elementweise)}$$

gegeben, so ergibt sich die Idee, diese zu einer Verknüpfung auf $\mathcal{X}$

$$\star : \begin{cases} \mathcal{X} \times \mathcal{X} & \to \quad \mathcal{X} \\ (X_i, X_j) & \mapsto \quad X_i \star X_j \ := \ \{x \star y | x \in X_i, y \in X_j\} \end{cases} \qquad \text{(teilmengenweise)}$$

,,abzusenken".

Diese Definition einer ,,teilmengenweisen" Verknüpfung ist leicht hingeschrieben, es stellen sich aber zwei Fragen:

- Ist denn die Menge $X_i \star X_j$ überhaupt wieder ein Element der Zerlegung $\mathcal{X}$?
- Vererben sich Eigenschaften der elementweisen Verknüpfung wie beispielsweise das Assoziativgesetz sinnvoll auf die teilmengenweise Verknüpfung?

6.3.5 Beispiel

Wir haben für $n \in \mathbb{N}$, $n \geq 2$, bereits die Zerlegung

$$\mathbb{Z}_n \quad = \quad \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

von $\mathbb{Z}$ in Restklassen kennengelernt. Es hat sich dann herausgestellt, dass die beiden elementweisen Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}$ zu Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}_n$ abgesenkt werden können. Summe und Produkt von zwei Restklassen sind wieder Restklassen.
Die Ringstruktur wird von $\mathbb{Z}$ auf $\mathbb{Z}_n$ vererbt, wobei

- $\mathbb{Z}_n$ sogar zu einem Körper wird, falls n eine Primzahl ist
- $\mathbb{Z}_n$ die Nullteilerfreiheit einbüßt, falls n keine Primzahl ist.

Wir wollen uns im nächsten Abschnitt 6.4 dem Zusammenspiel von Verknüpfungen und Zerlegungen zuwenden, wenn X ein Vektorraum ist. Dazu noch weitere Vorbereitungen.

6.3.6 Äquivalenzrelation auf einer Menge

Erinnerung: Eine Relation R auf einer Menge X ist eine Teilmenge von $X \times X$.

Für zwei Elemente $x, y \in X$ schreiben und sagen wir

$$(x, y) \in R \quad \overset{\text{def}}{\Longleftrightarrow} \quad x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad x \text{ und } y \text{ sind äquivalent.}$$

Eine Relation $\sim$ heißt *Äquivalenzrelation*, wenn die folgenden drei Bedingungen erfüllt sind:

Reflexivität: Für jedes $x \in X$ ist $x \sim x$.

Symmetrie: Für zwei Elemente $x, y \in X$ gilt die Äquivalenz

$$x \sim y \quad \Longleftrightarrow \quad y \sim x.$$

Transitivität: Für drei beliebige Elemente $x, y, z \in X$ gilt die Implikation

$$x \sim y \quad \text{und} \quad y \sim z \quad \Longrightarrow \quad x \sim z.$$

Es sei $\mathcal{E}(X)$ die Menge aller Äquivalenzrelationen auf X.

6.3.7 Beispiele für Äquivalenzrelationen

- Auf einer beliebigen Menge X gibt es die Äquivalenzrelationen (die *Diagonale*)

$$x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad x = y.$$

- Auf einer beliebigen Menge X gibt es die Äquivalenzrelationen (die *All-Relation*)

$$x \sim y \qquad \text{für alle } x, y.$$

- Es sei $n \in \mathbb{N}, n \geq 2$. Auf $\mathbb{Z}$ ist durch

  $$x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad x, y \ \text{ haben bei Division durch } n \text{ den gleichen Rest}$$

  eine Äquivalenzrelation gegeben.

- Es sei $\mathbb{N}_0 \times \mathbb{N}$ die Menge aller Zahlenpaare mit zweiter Koordinate ungleich Null. Definiere

  $$(x, y) \sim (u, v) \quad \overset{\text{def}}{\Longleftrightarrow} \quad x \cdot v \ = \ y \cdot u$$

- Es sei X die Menge aller Geraden in einem Raum. Eine Ä-Relation ist dann

  $$x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad x \ \text{ ist parallel zu } \ y$$

- Es sei X die Menge aller Dreiecke in der Zeichenebene. Durch

  $$\begin{array}{lcll} x \sim y & \overset{\text{def}}{\Longleftrightarrow} & x, y & \text{sind kongruent zueinander} \qquad \text{oder} \\ x \sim y & \overset{\text{def}}{\Longleftrightarrow} & x, y & \text{sind ähnlich zueinander} \end{array}$$

  sind Äquivalenzrelationen auf X gegeben.

- Es sei X eine Menge und $f : X \to Y$ eine Abbildung. Dann wird durch

  $$x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad f(x) = f(y)$$

  eine Äquivalenzrelation erklärt. Konkret könnte man hier bei X an eine Menge von Befragten bei einer Frage mit Menge der möglichen Antworten Y denken.

6.3.8 Definition: Äquivalenzklassen

Ist eine Äquivalenzrelation $\sim$ auf X gegeben, so definieren wir für ein festes $a \in X$ durch

$$[a] \quad := \quad \{x \in X \,|\, x \sim a\}$$

die zu a gehörige *Äquivalenzklasse* als eine nicht-leere Teilmenge von X.

6.3.9 Satz über Äquivalenzklassen

Für zwei Elemente $a, b \in X$ sind die folgenden Aussagen äquivalent

(A) $[a] = [b]$

(B) $[a] \cap [b] \neq \varnothing$.

(C) $a \sim b$

(D) Für alle $x \in [a]$ und alle $y \in [b]$ gilt $x \sim y$.

6.3.10 Beweis

(A) $\Rightarrow$ (B) ist trivial.

(B) $\Rightarrow$ (C): Enthält $[a]\cap[b]$ ein Element c, so gilt $c \sim a$ und $c \sim b$, dann wegen Symmetrie und Transitivität auch $a \sim b$.

(C) $\Rightarrow$ (D): Ist $x \in [a]$ und $y \in [b]$, so gilt $x \sim a$ und $y \sim b$, wegen Symmetrie auch $b \sim y$. Aufgrund der Transitivität gilt dann die Implikation

$$x \sim a, \quad a \sim b, \quad b \sim y \quad \Longrightarrow \quad x \sim y.$$

(D) $\Rightarrow$ (A). Sei $x \in [a]$. Wegen $b \in [b]$ folgt aus (D) dann $x \sim b$, also $x \in [b]$.

So haben wir also $[a] \subseteq [b]$ gezeigt. Ganz genauso zeigt man $[b] \subseteq [a]$.

6.3.11 Korrespondenz von Äquivalenzrelationen und Zerlegungen

Aufgrund des Satzes 6.3.9 bilden die Äquivalenzklassen bzgl. einer Äquivalenzrelation eine Zerlegung von X. Wir haben auf diese Weise eine Abbildung (einen Operator)

$$\Phi : \mathcal{E}(X) \to \mathcal{Z}(X)$$

von der Menge der Äquivalenzrelationen in die Menge der Zerlegungen definiert. Man sagt auch, dass die Äquivalenzrelation eine Zerlegung in Äquivalenzklassen induziert.

Ist umgekehrt eine Zerlegung $\mathcal{X} = \{X_i | i \in I\}$ vorgegeben, so können wir ihr eine Relation ,,gemeinsame Zugehörigkeit"

$$x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad x, y \text{ gehören zur gleichen Menge } X_i.$$

zuordnen. Man kann ganz leicht einsehen, dass dies eine Äquivalenzrelation auf X ist.

Insgesamt ist dies ein Operator

$$\Psi : \mathcal{Z}(X) \to \mathcal{E}(X).$$

Dem Satz 6.3.9 kann man entnehmen, dass die beiden Operatoren Φ und Ψ invers zueinander sind, ausführlicher:

- Ist auf einer Menge X eine Äquivalenzrelation gegeben, so induziert diese eine Zerlegung in Äquivalenzklassen. Definiert man mit Hilfe der Äquivalenzklassen dann die Relation der ,,gemeinsamen Zugehörigkeit", so landet man wieder bei der ursprünglichen Äquivalenzrelation.

- Ist auf einer Menge X eine Zerlegung gegeben, so induziert diese die Äquivalenzrelation der ,,gemeinsamen Zugehörigkeit". Die zu dieser Äquivalenzrelation gehörigen Äquivalenzklassen sind die Teilmengen der ursprünglichen Zerlegung.

- Die beiden Abbildungen und ihre Symbole Φ, Ψ sind in Zukunft nicht so wichtig. Es geht nur darum, die Korrespondenz zwischen Äquivalenzrelationen und Zerlegungen verstanden zu haben.

6.4 Faktorräume

6.4.1 Unterraum induziert Äquivalenzrelation Es sei nun V ein $\mathbb{K}$-Vektorraum und U ein Unterraum. Wir definieren auf V die von U abhängige Relation

$$v \sim w \qquad \stackrel{\text{def}}{\Longleftrightarrow} \qquad v - w \in U.$$

und überlegen, dass es sich um eine Äquivalenzrelation handelt:

Reflexivität: Wegen $v - v = \vec{0} \in U$ ist $\sim$ reflexiv.

Symmetrie: Ist $v \sim w$, so gilt $v - w \in U$ und dann $w - v = -(v - w) \in U$, also $w \sim v$.

Transitivität Sind v, w, p drei Vektoren aus V mit $v \sim w$ und $w \sim u$, so heißt dies $v - w \in U$ und $w - p \in U$. Daraus folgt aber $v - p = (v - w) + (w - p) \in U$, also $v \sim p$.

6.4.2 Unterraum induziert Zerlegung

Jede Äquivalenzrelation induziert eine Zerlegung in Äquivalenzklassen, so auch hier. Wir schauen uns die durch einen Vektor $w \in V$ gegebene Äquivalenzklasse genau an:

$$\begin{aligned}
[w] &= \{v \in V \mid v \sim w\} \\
&= \{v \in V \mid v - w \in U\} \\
&= \{v \in V \mid \text{Es ex. } u \in U \text{ mit } u = v - w\} \\
&= \{v \in V \mid \text{Es ex. } u \in U \text{ mit } v = w + u\} \\
&= w + U.
\end{aligned}$$

In diesem Zusammenhang heißen die Äquivalenzklassen auch *Nebenklassen*.

6.4.3 Eigenschaften der Äquivalenzklassen

- Es ist $w + U \; = \; \widetilde{w} + U$ genau dann, wenn $w - \widetilde{w} \in U$.
- Beachte, dass der Vektor w durch die Menge $w + U$ nicht eindeutig festgelegt ist; dies wird nur durch die spezielle Schreibweise suggeriert.

Wir bezeichnen die Menge aller Äquivalenzklassen mit

$$V/U \quad := \quad \{w + U \mid w \in V\}$$

und nennen sie den *Faktorraum* von V nach U. Es sind auch die Bezeichnungen Faktorvektorraum, Quotientenvektorraum, Quotientenraum üblich.

6.4.4 Satz: Faktorraum ist Vektorraum

Es sei V ein $\mathbb{K}$-Vektorraum und U ein Unterraum.

(i) Die Verknüpfungen

$$+ : \begin{cases} V/U \times V/U & \to & V/U \\ (w+U, \widetilde{w}+U) & \mapsto & (w+\widetilde{w})+U \end{cases}$$

und

$$\cdot : \begin{cases} \mathbb{K} \times V/U & \to & V/U \\ (\alpha, w+U) & \mapsto & (\alpha \cdot w)+U \end{cases}$$

sind wohldefiniert, das heißt unabhängig von der Auswahl des Vektors $x \in w+U$.

(ii) Mit diesen Verknüpfungen wird die Menge V/U zu einem $\mathbb{K}$-Vektorraum.

(iii) Der Nullvektor ist die Menge $\vec{0}+U = U$.

(iv) Der zu einem Vektor $w+U \in V/U$ additiv inverse Vektor ist $-w+U$.

6.4.5 Beweis

(i) Sind die Vektoren $x \in w+U$ und $y \in \widetilde{w}+U$ beliebig ausgewählt, so gilt

$$\begin{aligned} x+y-(w+\widetilde{w}) &= (x-w)+(y-\widetilde{w}) \in U, \quad \text{also} \quad x+y \in (w+\widetilde{w})+U \\ (\alpha \cdot x - \alpha w) &= \alpha \cdot (x-w) \in U, \quad \text{also} \quad \alpha \cdot x \in \alpha \cdot w + U. \end{aligned}$$

(ii) Wir rechnen nur als Beispiel vor, dass das Assoziativgesetz der Addition stimmt. Für drei Elemente $w+U, p+U, q+U \in V/U$ gilt

$$\begin{aligned} (w+U+p+U)+q+U &= (w+p)+U+q+U = (w+p)+q+U \\ w+U+(p+U+q+U) &= w+U+(p+q)+U = w+(p+q)+U \end{aligned}$$

Aufgrund des elementweisen Assoziativgesetzes stimmen die beiden Vektoren rechts überein. Damit stimmen auch die Äquivalenzklassen links überein.

(iii) Für ein beliebiges Element $w+U \in V/U$ gilt

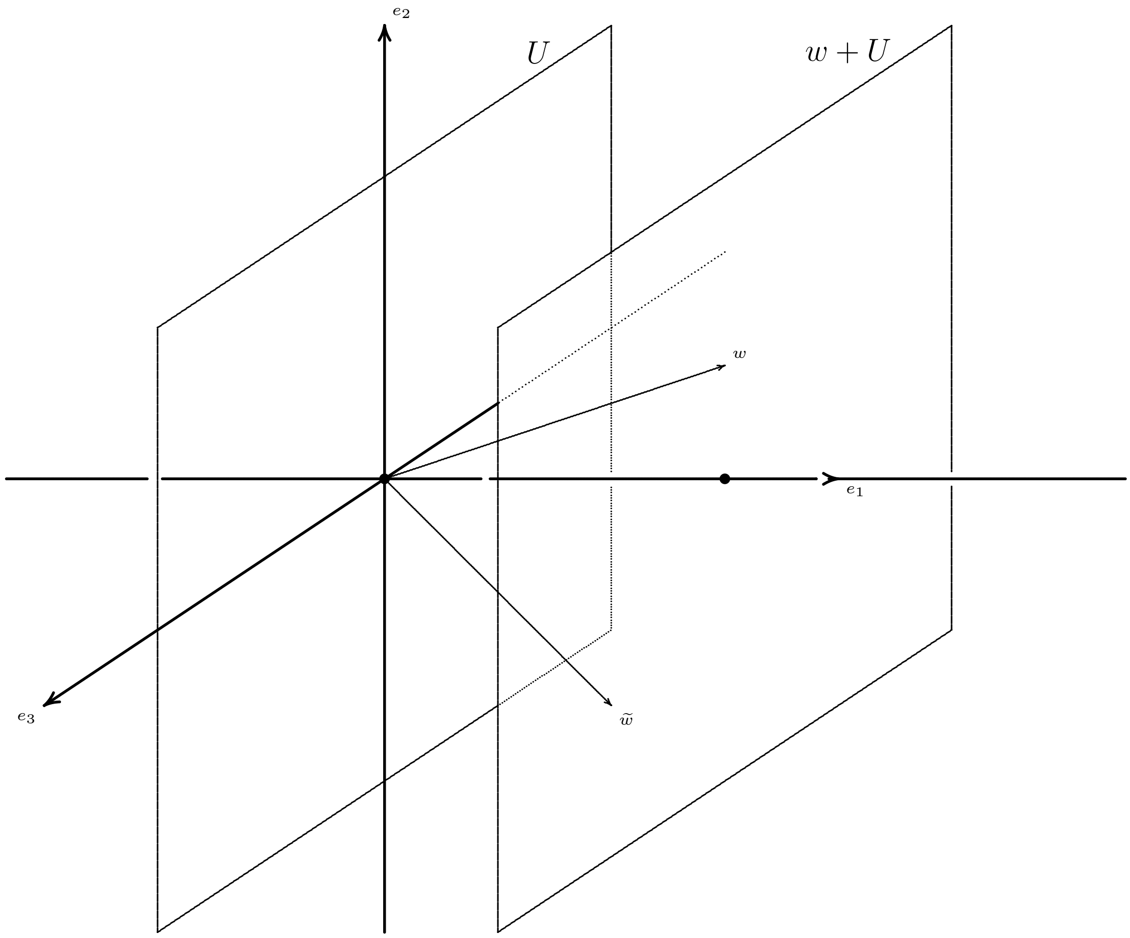
$$w+U+\vec{0}+U = w+\vec{0}+U = w+U.$$

(iv) Für ein beliebiges Element $w+U \in V/U$ ist

$$w+U+(-w+U) = w+(-w)+U = \vec{0}+U.$$

6.4.6 Beispiel

Es sei $V = \mathbb{R}^3$ und $U = \text{span}\{e_2, e_3\}$ die durch e_2 und e_3 aufgespannte Ebene. Dann sind die Mengen $w + U$ die Ebenen parallel zu U.



- Es ist dann

$$V/U \quad = \quad \{w + U \mid w \in V\}$$

  die Menge der Ebenen. Die Ebenen werden zu Elementen des Faktorraums V/U.

- Ist die Differenz zweier Vektoren w und $\widetilde{w}$ in U enthalten, so stimmen die beiden Ebenen $w + U$ und $\widetilde{w} + U$ überein.

- Die Addition zweier Ebenen geschieht dadurch, dass man sich aus beiden Ebenen je einen Vektor heraussucht, diese beiden — herkömmlich — addiert und dann die Ebene als Summe heranzieht, die die Summe der Vektoren enthält.

- Die skalare Multiplikation einer Ebene mit einem Skalar α geschieht dadurch, dass man sich aus der Ebene einen Vektor heraussucht, diesen — herkömmlich — skalar mit α multipliziert und dann die Ebene als α-Vielfaches heranzieht, die den α-vervielfachten Vektor enthält.

- Die Ebene U verläuft durch den Ursprung, sie dient als Nullvektor.

- Zur Ebene $w + U$ gehört die Ebene $-w + U$ als negatives Element.

6.4.7 Satz: Dimension des Faktorraums

Es sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum und U ein Unterraum. Dann gilt:

$$\dim V \quad = \quad \dim U + \dim(V/U).$$

6.4.8 Beweis

Es sei $B_U = \{u_1, \ldots, u_n\}$ eine Basis von U, die zu einer Basis

$$B_V \quad = \quad \{u_1, \ldots, u_n, w_1, \ldots, w_m\}$$

von V ergänzt werden kann.

Wir zeigen, dass

$$B \quad := \quad \{w_1 + U, \ldots, w_m + U\}$$

eine Basis vonV/U ist.

Erzeugendensystem: Dazu sei $v + U \in V/U$ ein beliebiger Vektor. $v \in V$ besitzt eine Darstellung bzgl. B_V als

$$v \quad = \quad \alpha_1 u_1 + \cdots + \alpha_n u_n + \beta_1 w_1 + \cdots + \beta_m w_m.$$

Dann ist

$$\begin{aligned} v + U &= (\alpha_1 u_1 + \cdots + \alpha_n u_n + \beta_1 w_1 + \cdots + \beta_m w_m) + U \\ &= (\beta_1 w_1 + \cdots + \beta_m w_m) + U \\ &= \beta_1(w_1 + U) + \cdots + \beta_m(w_m + U) \end{aligned}$$

Also ist B Erzeugendensystem.

Linear unabhängig: Wir setzten den Nullvektor als Linearkombination an:

$$\begin{aligned} \vec{0} + U &= \alpha_1(w_1 + U) + \cdots + \alpha_m(w_m + U) \\ &= (\alpha_1 w_1 + \cdots + \alpha_m w_m) + U \end{aligned}$$

Daraus folgt dann

$$\alpha_1 w_1 + \cdots + \alpha_m w_m \in U.$$

Deshalb kann dieser Vektor als Linearkombination von B_U dargestellt werden:

$$\alpha_1 w_1 + \cdots + \alpha_m w_m = \beta_1 u_1 + \cdots + \beta_n u_n,$$

es folgt

$$\vec{0} \quad = \quad \alpha_1 w_1 + \cdots + \alpha_m w_m - \beta_1 u_1 - \cdots - \beta_n u_n.$$

Da B_V Basis ist, muss

$$\begin{aligned} \alpha_1 &= \cdots = \alpha_m = 0 \\ \beta_1 &= \cdots = \beta_n = 0 \end{aligned}$$

sein. Die obere Zeile schließt den Beweis schon ab.

7 Lineare Abbildungen

7.1 Definition und Beispiele

7.1.1 Definition und Satz

Es sei $\mathbb{K}$ ein Körper und V, W seien zwei $\mathbb{K}$–Vektorräume.
Die folgenden Aussagen über eine Abbildung $f : V \to W$ sind äquivalent:

(A) (Per definitionem) $f : V \to W$ heißt *linear*, genauer $\mathbb{K}$-*linear*.

(B) Für alle $v, \widetilde{v} \in V$ gilt

$$f(v + \widetilde{v}) \quad = \quad f(v) + f(\widetilde{v})$$

und für alle $v \in V$, $\alpha \in \mathbb{K}$ gilt

$$f(\alpha \cdot v) \quad = \quad \alpha \cdot f(v)$$

(C) Für alle $v, \widetilde{v} \in V$, $\alpha, \widetilde{\alpha} \in \mathbb{K}$ gilt

$$f(\alpha \cdot v + \widetilde{\alpha} \cdot \widetilde{v}) \quad = \quad \alpha \cdot f(v) + \widetilde{\alpha} \cdot f(\widetilde{v})$$

Wir bezeichnen die Menge aller linearen Abbildungen $V \to W$ mit $\mathcal{L}(V, W)$.

7.1.2 Satz Es seien V und W zwei $\mathbb{K}$–Vektorräumen.

(i) Ist $f : V \to W$ eine lineare Abbildung, so ist $f(\vec{0}) \;=\; \vec{0}$.

(ii) Für einen Vektorraum V ist die identische Abbildung id_V immer linear.

(iii) Sind $f : V \to W$ und $g : W \to U$ zwei lineare Abbildungen, so ist die Hintereinanderausführung $g \circ f : V \to U$ wieder linear.

7.1.3 Beweis

(i) Es ist

$$f(\vec{0}) \quad = \quad f(\vec{0} + \vec{0}) \quad = \quad f(\vec{0}) + f(\vec{0})$$

und deshalb — wegen der Eindeutigkeit des additiv-neutralen Elements — $f(\vec{0}) \;=\; \vec{0}$.

(ii) ist trivial, (iii) kann ganz einfach nachgerechnet werden.

7.1.4 Beispiele linearer Abbildungen

(1) Abbildungen der Form

$$\begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & m \cdot x + t \end{cases}$$

werden in der Schule linear genannt. Im Sinne der Linearen Algebra ist eine solche Abbildung nur im Fall $t = 0$ linear.

(2) Es seien eine Gerade, eine Ebene oder der drei-dimensionale ,,Anschauungsraum" mit einem Ursprung O gegeben. Dann sind die geometrischen Abbildungen

- Zentrische Streckung mit Zentrum O
- Achsenspiegelung bzgl. einer Geraden durch O
- Punktspiegelung mit Zentrum O
- und viele andere

lineare Abbildungen.

(3) Für zwei Vektorräume V und W ist die Konstant-Null-Abbildung

$$\begin{cases} V & \to & W \\ v & \mapsto & \vec{0} \end{cases}$$

immer linear.

(4) Es sei X eine Menge und $\mathcal{F}(\mathbb{R}, \mathbb{R})$ der Vektorraum der reellen Funktionen $\mathbb{R} \to \mathbb{R}$. Für $a, b, c \in \mathbb{R}$ ist die Transformation

$$\vartheta_{a,b,c} : \begin{cases} \mathcal{F}(\mathbb{R}, \mathbb{R}) & \to & \mathcal{F}(\mathbb{R}, \mathbb{R}) \\ \big(x \mapsto f(x)\big) & \mapsto & \big(x \mapsto c \cdot f(ax + b)\big) \end{cases}$$

linear.

(5) Es sei $\mathcal{D}(\mathbb{R}, \mathbb{R})$ der Vektorraum der differenzierbaren Funktionen. Die Differentiation

$$\begin{cases} \mathcal{D}(\mathbb{R}, \mathbb{R}) & \to & \mathcal{F}(\mathbb{R}, \mathbb{R}) \\ g & \mapsto & g' \end{cases}$$

ist linear.

(6) Es sei $\mathcal{C}(\mathbb{R}, \mathbb{R})$ der Vektorraum der stetigen Funktionen $\mathbb{R} \to \mathbb{R}$. Für festes $a \in \mathbb{R}$ ist die ,,unbestimmte" Integration

$$\begin{cases} \mathcal{C}(\mathbb{R}, \mathbb{R}) & \to & \mathcal{C}(\mathbb{R}, \mathbb{R}) \\ g & \mapsto & \big(x \mapsto \int_a^x g(t)\, dt\big) \end{cases}$$

eine lineare Abbildung.

7.1.5 Definition: Polynomfunktion

(1) Eine Funktion $p : \mathbb{R} \to \mathbb{R}$ heißt *Polynomfunktion n-ten Grades* (kurz, aber nicht ganz so glücklich: Polynom), wenn es Zahlen

$$a_n \in \mathbb{R} \setminus \{0\}, \qquad a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}$$

gibt, so dass

$$p(x) \quad = \quad a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0 \qquad \text{für alle} \quad x \in \mathbb{R}.$$

(2) Die Null-Funktion $0 : \mathbb{R} \to \mathbb{R}$ wird als Polynomfunktion mit Grad $-\infty$ angesehen.

(3) Für $n \in \mathbb{N}_0$ wird der Vektorraum der Polynomfunktionen des Grades $\leq n$ mit $\mathcal{P}_n(\mathbb{R}, \mathbb{R})$ bezeichnet. Der Vektorraum aller Polynomfunktionen wird mit $\mathcal{P}(\mathbb{R}, \mathbb{R})$ bezeichnet.

(4) Wir werden später noch sehen, dass eine Polynomfunktion n-ten Grades, $n \in \mathbb{N}_0$, höchstens n Nullstellen haben kann. Deshalb ist die Menge der Funktionen

$$\{1, x, x^2, \ldots, x^n\}$$

linear unabhängig und weiter eine Basis von $\mathcal{P}_n$. Es ist also

$$\dim \mathcal{P}_n(\mathbb{R}, \mathbb{R}) \quad = \quad n + 1.$$

(5) Die folgenden Operatoren sind linear:

$$\text{Multiplikation mit der Variablen} \qquad X : \begin{cases} \mathcal{P}(\mathbb{R}, \mathbb{R}) & \to & \mathcal{P}(\mathbb{R}, \mathbb{R}) \\ p & \mapsto & \big(x \mapsto x \cdot p(x)\big) \end{cases}$$

$$\text{Differentiation nach der Variablen} \qquad D : \begin{cases} \mathcal{P}(\mathbb{R}, \mathbb{R}) & \to & \mathcal{P}(\mathbb{R}, \mathbb{R}) \\ p & \mapsto & \big(x \mapsto p'(x)\big) \end{cases}$$

$$\text{Integration nach der Variablen} \qquad I : \begin{cases} \mathcal{P}(\mathbb{R}, \mathbb{R}) & \to & \mathcal{P}(\mathbb{R}, \mathbb{R}) \\ p & \mapsto & \big(x \mapsto \int_0^x p(t)\, dt\big) \end{cases}$$

7.1.6 Kanonische lineare Abbildungen

(1) Ist V ein $\mathbb{K}$-Vektorraum und U ein Unterraum, so ist die kanonische Abbildung

$$\iota = \iota_U : \qquad \begin{cases} U & \to & V \\ v & \mapsto & v \end{cases}$$

linear. Sie heißt die *kanonische Injektion*.

(2) Ist V ein $\mathbb{K}$-Vektorraum und U ein Unterraum, so ist die kanonische Abbildung

$$p = p_{V/U} : \qquad \begin{cases} V & \to & V/U \\ v & \mapsto & v + U \end{cases}$$

linear. Sie heißt die *kanonische Projektion*.

(3) Es sei $V \oplus W$ die äußere direkte Summe zweier $\mathbb{K}$-Vektorräume V und W. Die Abbildungen

$$\begin{cases} V & \to & V \oplus W \\ v & \mapsto & (v, \vec{0}) \end{cases} \qquad\qquad \begin{cases} V \oplus W & \to & V \\ (v, w) & \mapsto & v \end{cases}$$

sind linear. Man könnte sie als *Komponenten-Einbettung* und *Komponenten-Projektion* bezeichnen. Diese Begriffe sind nicht so üblich.

7.1.7 Matrizen als lineare Abbildungen

(1) Eine $m \times n$–Matrix A vermittelt per Matrixmultiplikation von links eine lineare Abbildung

$$\ell_A : \begin{cases} \mathbb{K}^n & \to & \mathbb{K}^m \\ v & \mapsto & A \cdot v. \end{cases}$$

(2) Ist $B \in \mathbb{K}^{n \times \ell}$ eine weitere Matrix, so gilt für $v \in \mathbb{K}^\ell$ aufgrund des Assoziativgesetzes der Matrixmultiplikation

$$\ell_{A \cdot B}(v) \;=\; (A \cdot B) \cdot v \;=\; A \cdot (B \cdot v) \;=\; \ell_A(\ell_B(v)) \;=\; (\ell_A \circ \ell_B)(v),$$

insgesamt also

$$\ell_{A \cdot B} \;=\; \ell_A \circ \ell_B.$$

(3) Ist umgekehrt eine lineare Abbildung $f : \mathbb{K}^n \to \mathbb{K}^m$ gegeben, so definieren wir die Matrix

$$A_f \;:=\; \begin{pmatrix} f(e_1) & \cdots & \cdots & f(e_n) \end{pmatrix},$$

wobei $e_1, \ldots, e_n$ die Einheitsvektoren im $\mathbb{K}^n$ sind.

(4) Damit haben wir zwei „Operatoren”

$$\begin{cases} \mathbb{K}^{m \times n} & \to & \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m) \\ A & \mapsto & \ell_A \end{cases} \qquad \text{und} \qquad \begin{cases} \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m) & \to & \mathbb{K}^{m \times n} \\ f & \mapsto & A_f \end{cases}$$

definiert.

(5) Etwas fieselig, aber doch einfach, kann man nachrechnen, dass für einen beliebigen Vektor $(v_1, \ldots, v_n)^T \in \mathbb{K}^n$

$$f(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}) \;=\; f(\sum_{k=1}^n v_k e_k) \;=\; \sum_{k=1}^n v_k f(e_k) \;=\; A_f \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \;=\; \ell_{A_f}(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix})$$

und

$$\begin{aligned} A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \;&=\; \ell_A(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}) \;=\; \ell_A(\sum_{k=1}^n v_k e_k) \;=\; \sum_{k=1}^n v_k \ell_A(e_k) \\ &=\; \begin{pmatrix} \ell_A(e_1) & \cdots & \ell_A(e_n) \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \;=\; A_{\ell_A} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}. \end{aligned}$$

Das heißt, die beiden Operatoren sind invers zueinander.

(6) Als Fazit können wir feststellen, dass lineare Abbildungen $\mathbb{K}^n \to \mathbb{K}^m$ und Matrizen in $\mathbb{K}^{m \times n}$ zwei Spielarten des gleichen mathematischen Sachverhalts sind.

(7) Wir werden sehen, dass die strenge Unterscheidung der Symbole A und ℓ_A nicht dringend notwendig ist und werden daher — wie fast überall üblich — einfach $\ell_A = A$ schreiben.

7.2 Lineare Abbildungen und Basen

7.2.1 Satz: Lineare Abbildung ist durch Basis eindeutig bestimmt

Für zwei $\mathbb{K}$–Vektorräume V, W seien vorgegeben ...

eine Basis B von V und

eine Abbildung $f_B : B \to W$.

Dann gibt es genau eine lineare Abbildung $f : V \to W$ mit

$$f(v) = f_B(v) \quad \text{für alle} \quad v \in B.$$

Das heißt, eine lineare Abbildung ist durch die Bilder der Basiselemente eindeutig bestimmt.

7.2.2 Beweis

(1) Um f zu definieren, müssen wir zu jedem Vektor $v \in V$ den Bildvektor angeben. Es sei $v = \sum_{j=1}^n \alpha_j v_j$ die eindeutige Linearkombination für v bzgl. der Basis B. Dann definieren wir

$$f(v) := \sum_{j=1}^n \alpha_j f_B(v_j).$$

Ist nun $v \in B$, so ist $v = 1 \cdot v$ die zugehörige Linearkombination und es gilt aufgrund der Definition von f:

$$f(v) = f(1 \cdot v) = 1 \cdot f_B(v) = f_B(v).$$

(2) Wir haben zu zeigen, dass f linear ist. Es seien $\alpha, \widetilde{\alpha} \in \mathbb{K}$ und Vektoren $v, \widetilde{v}$ aus V vorgegeben. Es gibt dann endlich viele Vektoren $v_j \in B$, so dass

$$v = \sum_{j=1}^n \beta_j v_j \quad \text{und} \quad \widetilde{v} = \sum_{j=1}^n \widetilde{\beta}_j v_j.$$

Es gilt dann

$$f(\alpha v + \widetilde{\alpha}\widetilde{v}) = f\left(\sum_{j=1}^n (\alpha\beta_j + \widetilde{\alpha}\widetilde{\beta}_j) v_j\right) =$$

$$\sum_{j=1}^n (\alpha\beta_j + \widetilde{\alpha}\widetilde{\beta}_j) f(v_j) = \alpha \sum_{j=1}^n \beta_j f(v_j) + \widetilde{\alpha} \sum_{j=1}^n \widetilde{\beta}_j f(v_j) = \alpha f(v) + \widetilde{\alpha} f(\widetilde{v}).$$

(3) Würde es zwei verschiedene lineare Abbildungen f und $\widetilde{f}$ mit der geforderten Eigenschaft geben, so gäbe es mindestens ein $v \in V$, so dass $f(v) \neq \widetilde{f}(v)$.

Ist dann $v = \sum_{j=1}^n \alpha_j v_j$ die Basisentwicklung von v, so gilt wegen der Linearität von f

und $\widetilde{f}$

$$\begin{aligned}\vec{0} \;&\neq\; f(v) - \widetilde{f}(v) \;=\; f(\sum_{j=1}^{n} \alpha_j v_j) - \widetilde{f}(\sum_{j=1}^{n} \alpha_j v_j) \;=\; \sum_{j=1}^{n} \alpha_j (f(v_j) - \widetilde{f}(v_j)) \\ &= \sum_{j=1}^{n} \alpha_j (f_B(v_j) - f_B(v_j)) \;=\; \vec{0}.\end{aligned}$$

Das ist ein Widerspruch.

7.2.3 Satz: Das Bild von Basen

Es sei $f : V \to W$ eine lineare Abbildung zwischen zwei $\mathbb{K}$–Vektorräumen. Weiter sei B eine Basis von V und $f(B)$ die Bildmenge.

(i) f ist genau dann injektiv, wenn $f(B)$ linear unabhängig ist.

(ii) f ist genau dann surjektiv, wenn $f(B)$ ein Erzeugendensystem ist.

(iii) f ist genau dann bijektiv, wenn $f(B)$ eine Basis ist.

7.2.4 Beweis

(i)$^{\Rightarrow}$ Es sei f injektiv. Wir wollen zeigen, dass $f(B)$ linear unabhängig ist. Dazu sei

$$\vec{0} \;=\; \alpha_1 w_1 + \cdots + \alpha_n w_n$$

eine Linearkombination von Vektoren aus $f(B)$, die den Nullvektor als Wert hat.

Jeder Vektor $w_j \in f(B)$ hat ein Urbild $v_j \in B$. Wir setzen $f(v_j) = w_j$ in den Nullvektoransatz ein und erhalten insgesamt

$$f(\vec{0}) \;=\; \vec{0} \;=\; \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n) \;=\; f(\alpha_1 v_1 + \cdots + \alpha_n v_n).$$

Wegen der Injektivität von f muss

$$\vec{0} \;=\; \alpha_1 v_1 + \cdots + \alpha_n v_n$$

sein. Die Vektoren v_j sind in der Basis B, deshalb muss $\alpha_j = 0$ sein für alle $j = 1, \ldots, n$.

(i)$^{\Leftarrow}$ Es sei $f(B)$ linear unabhängig. Es seien $v, \widetilde{v} \in V$ mit $f(v) = f(\widetilde{v})$. v und $\widetilde{v}$ sind Linearkombinationen aus B, also

$$\begin{aligned} v \;&=\; \alpha_1 v_1 + \cdots + \alpha_n v_n, \\ \widetilde{v} \;&=\; \widetilde{\alpha}_1 v_1 + \cdots + \widetilde{\alpha}_n v_n, \qquad\qquad v_j \in B. \end{aligned}$$

Es folgt

$$\begin{aligned} & \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n) \\ =\; & f(\alpha_1 v_1 + \cdots + \alpha_n v_n) \\ =\; & f(v) \;=\; f(\widetilde{v}) \\ =\; & f(\widetilde{\alpha}_1 v_1 + \cdots + \widetilde{\alpha}_n v_n) \\ =\; & \widetilde{\alpha}_1 f(v_1) + \cdots + \widetilde{\alpha}_n f(v_n). \end{aligned}$$

Da wegen der linearen Unabhängigkeit von $f(B)$ dieser Vektor eine eindeutige Linearkombination aus $f(B)$ sein muss, folgt

$$\alpha_1 = \widetilde{\alpha}_1, \quad \ldots \quad \alpha_n = \widetilde{\alpha}_n$$

und damit $v = \widetilde{v}$.

(ii)$^{\Rightarrow}$ Es sei f surjektiv. Dann gibt es zu jedem $w \in W$ ein $v \in V$, so dass $w = f(v)$. Ist $v = \sum_{j=1}^{n} \alpha_j v_j$ für v die Linearkombination aus B, so gilt

$$w = f(v) = f(\sum_{j=1}^{n} \alpha_j v_j) = \sum_{j=1}^{n} \alpha_j f(v_j).$$

Also ist $f(B)$ ein Erzeugendensystem.

(ii)$^{\Leftarrow}$ Es sei $f(B)$ ein Erzeugendensystem von W. Dann lässt sich ein beliebiger Vektor $w \in W$ schreiben als

$$w = \alpha_1 w_1 + \cdots + \alpha_n w_n$$

wobei zu jedem w_j ein $v_j \in V$ existiert, so dass $f(v_j) = w_j$. Dann gilt aber

$$w = \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n) = f(\alpha_1 v_1 + \cdots + \alpha_n v_n).$$

Also ist $w \in f(V)$. Das heißt, f ist surjektiv.

Die Aussage (iii) folgt aus den Aussagen (i) und (ii).

7.2.5 Bezeichnungen: Homomorphismen

In stärker algebraisch orientierten Teilgebieten der Mathematik treten — aufgrund der Herausarbeitung von begrifflichen Verallgemeinerungen in der Theorie der so genannten Kategorien — andere Bezeichnungen für bestimmte Typen von Abbildungen in Erscheinung.

In diesem Kontext heißen lineare Abbildungen auch *Homomorphismen*. Ein Homomorphismus $f : V \to W$ heißt genauer ...

Monomorphismus, wenn er injektiv ist,

Epimorphismus, wenn er surjektiv ist,

Isomorphismus, wenn er bijektiv ist,

Endomorphismus, wenn $V = W$ gilt,

Automorphismus, wenn er bijektiv ist und $V = W$ gilt.

Zwei Vektorräume V, W heißen *isomorph*, wenn ein Isomorphismus $f : V \to W$ existiert.

7.2.6 Folgerung

Sind zwei Vektorräume isomorph, so haben sie die gleiche Dimension.

7.2.7 Beweis

Gemäß 7.2.3(iii) werden Basen der beiden Vektorräume bijektiv aufeinander abgebildet.

7.3 Kern und Bild einer linearen Abbildung

7.3.1 Vorbemerkung

Es sei darauf hingewiesen, dass wir in den folgenden Unterkapiteln keinen Gebrauch vom Begriff der Basis machen müssen.

7.3.2 Definition: Kern, Bild Es sei $f : V \to W$ eine lineare Abbildung.

Die Urbildmenge von $\vec{0} \in W$ heißt der *Kern* von f. Die Bezeichnung ist

$$\ker f \quad := \quad f^{-1}(\{\vec{0}\}) \ = \ \Big\{ v \in V \ \Big| \ f(v) = \vec{0} \Big\}.$$

Die Bildmenge von V heißt das *Bild* von f. Die Bezeichnung ist

$$\operatorname{im} f \quad := \quad f(V) \ = \ \Big\{ w \in W \ \Big| \ \text{Es ex. } v \in V \text{ mit } f(v) = w \Big\}.$$

7.3.3 Satz: Kern und Bild sind Unterräume

Es sei $f : V \to W$ eine lineare Abbildung zwischen zwei $\mathbb{K}$–Vektorräumen.

(i) Der Kern von f ist ein Unterraum von V.

(ii) Das Bild von f ist ein Unterraum von W.

7.3.4 Beweis

(i) Es seien $v, \widetilde{v} \in \ker f$ und $\alpha, \widetilde{\alpha} \in \mathbb{K}$. Dann gilt

$$f(\alpha v + \widetilde{\alpha}\widetilde{v}) \ = \ \alpha f(v) + \widetilde{\alpha} f(\widetilde{v}) \ = \ \vec{0},$$

also liegt auch jede beliebige Linearkombination von $\ker f$ in $\ker f$.

(ii) Es seien $w, \widetilde{w} \in \operatorname{im} f$ und $\alpha, \widetilde{\alpha} \in \mathbb{K}$. Dann gibt es Vektoren $v, \widetilde{v} \in V$, so dass

$$f(v) \ = \ w, \qquad f(\widetilde{v}) = \widetilde{w}.$$

Dann gilt aber weiter

$$\alpha w + \widetilde{\alpha}\widetilde{w} \ = \ \alpha f(v) + \widetilde{\alpha} f(\widetilde{v}) \ = \ f(\alpha v + \widetilde{\alpha}\widetilde{v}) \ \in \ \operatorname{im} f.$$

7.3.5 Satz Es sei $f : V \to W$ eine lineare Abbildung zwischen zwei $\mathbb{K}$–Vektorräumen.

(i) f ist genau dann injektiv, wenn $\ker f \ = \ \{\vec{0}\}$.

(ii) f ist genau dann surjektiv, wenn $\operatorname{im} f \ = \ W$.

(iii) f ist genau dann bijektiv, wenn $\ker f \ = \ \{\vec{0}\}$ und $\operatorname{im} f \ = \ W$.

(iv) Ist f bijektiv, so ist auch die Umkehrabbildung $f^{-1} : W \to V$ linear.

7.3.6 Beweis

(i) Ist f injektiv, so hat $\vec{0} \in W$ höchstens ein Urbild, das ist eben der Nullvektor.

Es sei umgekehrt $\ker f = \{\vec{0}\}$. Haben zwei Vektoren $v, \widetilde{v} \in V$ das gleiche Bild, $f(v) = f(\widetilde{v})$, so gilt

$$f(v - \widetilde{v}) = f(v) - f(\widetilde{v}) = \vec{0},$$

deshalb $v - \widetilde{v} = \vec{0}$ und dann $v = \widetilde{v}$.

(ii) und (iii) sind trivial. Die beiden Aussagen sind nur aus ästhetischen Gründen hinzugefügt.

(iv) Es seien $w, \widetilde{w} \in W$, $\alpha, \widetilde{\alpha} \in \mathbb{K}$ beliebig. Es existieren dann eindeutige Vektoren $v, \widetilde{v} \in V$ mit $f(v) = w$ und $f(\widetilde{v}) = \widetilde{w}$. Dann ist

$$\begin{aligned}
\alpha \cdot f^{-1}(w) + \widetilde{\alpha} \cdot f^{-1}(\widetilde{w}) &= \alpha \cdot f^{-1}(f(v)) + \widetilde{\alpha} \cdot f^{-1}(f(\widetilde{v})) \\
&= \alpha \cdot v + \widetilde{\alpha} \cdot \widetilde{v} \\
&= f^{-1}(f(\alpha \cdot v + \widetilde{\alpha} \cdot \widetilde{v})) \\
&= f^{-1}(\alpha \cdot f(v) + \widetilde{\alpha} \cdot f(\widetilde{v})) \\
&= f^{-1}(\alpha \cdot w + \widetilde{\alpha} \cdot \widetilde{w}).
\end{aligned}$$

7.4 Kanonische Zerlegung einer linearen Abbildung

7.4.1 Satz: Kanonische Zerlegung einer linearen Abbildung

Es sei $f : V \to W$ eine lineare Abbildung zwischen zwei $\mathbb{K}$–Vektorräumen.

(i) Es gibt eine bijektive lineare Abbildung $\widehat{f} : V/(\ker f) \to \mathrm{im}(f)$, so dass f wir folgt kanonisch in drei Abbildungen zerlegt (= faktorisiert) werden kann:

$$\begin{tikzcd}
V \arrow[r, "p"] \arrow[rrr, bend left, "f"] & V/(\ker f) \arrow[r, shift left, "\widehat{f}"] & \mathrm{im}\, f \arrow[l, shift left, "\widehat{f}^{-1}"] \arrow[r, "\iota"] & W \\
v \arrow[r, mapsto] & v + \ker f \arrow[r, mapsto, shift left] & w \arrow[l, mapsto, shift left] \arrow[r, mapsto] & w
\end{tikzcd}$$

Es kann also jede lineare Abbildung $f : V \to W$ durch

Faktorisierung des Definitions-Vektorraums V nach $\ker f$ und
Einschränkung des Werte-Vektorraums W auf $\mathrm{im}\, f$

,,bijektiv gemacht" werden.

(ii) Die zu $\widehat{f}$ inverse lineare Abbildung $\widehat{f}^{-1}$ gibt zu jedem Element $b \in \mathrm{im}\, f$ die Urbildmenge an:

$$\widehat{f}^{-1} : \begin{cases} \mathrm{im}\, f & \to & V/(\ker f) \\ w & \mapsto & f^{-1}(\{w\}). \end{cases}$$

7.4.2 Beweis

(1) Wir definieren die Abbildung $\widehat{f} : V/(\ker f) \to \mathrm{im}\, f$ durch

$$\widehat{f}(v + \ker f) \;=\; f(v).$$

(2) Wir zeigen, dass $\widehat{f}$ so wohldefiniert ist, d.h. dass die Definition unabhängig von der Auswahl des Vektors v ist. Dazu sei $\widetilde{v} \in v + \ker f$ ein beliebiger Vektor in der Äquivalenzklasse. Dann gilt $\widetilde{v} - v \in \ker f$ und deshalb

$$f(\widetilde{v}) \;=\; f(\widetilde{v} - v + v) \;=\; f(\widetilde{v} - v) + f(v) \;=\; \vec{0} + f(v) \;=\; f(v).$$

Also kann in der obigen Definition die rechte Seite $f(v)$ durch $f(\widetilde{v})$ ersetzt werden.

(3) Wir zeigen als nächstes, dass $\widehat{f}$ injektiv ist. Angenommen, es existieren zwei Vektoren $v + \ker f, \widetilde{v} + \ker f \in V/(\ker f)$ mit $\widehat{f}(v + \ker f) \;=\; \widehat{f}(\widetilde{v} + \ker f)$. Dann gilt

$$f(v - \widetilde{v}) \;=\; f(v) - f(\widetilde{v}) \;=\; \widehat{f}(v + \ker f) - \widehat{f}(\widetilde{v} + \ker f) \;=\; \vec{0}.$$

Das aber bedeutet $v - \widetilde{v} \in \ker f$ und deshalb $v + \ker f \;=\; \widetilde{v} + \ker f$.

(4) Es bleibt noch die Surjektivität zu zeigen. Ist $w \in \mathrm{im}\, f$ beliebig, so gibt es aufgrund der Definition des Bildes eines Vektors $v \in V$ mit $f(v) = w$. Dann gilt aber

$$\widehat{f}(v + \ker f) \;=\; f(v) \;=\; w.$$

Also ist w auch im Bild von $\widehat{f}$ enthalten.

7.4.3 Beispiel aus der Analysis: Der Differentiationsoperator

Es seien (vgl. Abschnitt 7.1.4)

$\mathcal{F}(\mathbb{R},\mathbb{R})$ den Vektorraum der Funktionen $\mathbb{R} \to \mathbb{R}$, dann

$\mathcal{C}(\mathbb{R},\mathbb{R})$ der Unterraum der stetigen Funktionen und

$\mathcal{D}(\mathbb{R},\mathbb{R})$ der Unterraum der differenzierbaren Funktionen.

Weiter sei

$$D : \begin{cases} \mathcal{D}(\mathbb{R},\mathbb{R}) & \to & \mathcal{F}(\mathbb{R},\mathbb{R}) \\ f & \mapsto & f' \end{cases}$$

der Differentiationsoperator, er ordnet jeder differenzierbaren Funktion ihre Ableitungsfunktion zu. Er ist — wie Ihnen bekannt — linear.

Wir betrachten für $g \in \mathcal{D}(\mathbb{R},\mathbb{R})$ und $h \in \mathcal{F}(\mathbb{R},\mathbb{R})$ die linear-inhomogene Gleichung

$$Dg = h. \qquad (*)$$

Eine Lösung dieser Gleichung ist nichts anderes als eine Stammfunktion g von h auf $\mathbb{R}$.

7.4.4 „Bijektiv-Machen" des Differentiationsoperators

Wir wollen jetzt mit Hilfe des Diagramms der kanonischen Zerlegung des Differentiationsoperators

$$\begin{tikzcd} \mathcal{D}(\mathbb{R},\mathbb{R}) \arrow[r, "p"] \arrow[rrr, bend left, "D"] & \mathcal{D}(\mathbb{R},\mathbb{R})/(\ker D) \arrow[r, shift left, "\widehat{D}"] & \operatorname{im} D \arrow[l, shift left, "\widehat{D}^{-1}"] \arrow[r, "\iota"] & \mathcal{F}(\mathbb{R},\mathbb{R}) \\ g \arrow[r, mapsto] & g + \ker D \arrow[r, mapsto, shift left] & h \arrow[l, mapsto, shift left] \arrow[r, mapsto] & h \end{tikzcd}$$

die in Abschnitt 7.4.3 geschilderte Situation genauer analysieren.

(1) Der Kern von D ist der Unterraum der konstanten Funktionen

$$\ker D = C := \Big\{ g : \mathbb{R} \to \mathbb{R} \,\Big|\, \text{Es ex. } c \in \mathbb{R} \text{ mit } g(x) = c \text{ für alle } x \in \mathbb{R} \Big\},$$

wie in der Analysis mit Hilfe des Mittelwertsatzes bewiesen wird.

(2) Für das Bild $\operatorname{im} D$ gibt es keine gute explizite Beschreibung. Man weiss aus der Analysis, dass

$$\mathcal{C}(\mathbb{R},\mathbb{R}) \subsetneqq \operatorname{im} D \subsetneqq \mathcal{F}(\mathbb{R},\mathbb{R}).$$

(3) Für $h \in \operatorname{im} D$ ist der Umkehroperator $\widehat{D}^{-1}$ gegeben durch

$$\mathcal{L}(D|h) = \widehat{D}^{-1}(h) = \widetilde{g} + C,$$

wobei $\widetilde{g}$ irgendeine Stammfunktion von h ist. Man nennt diese Restklasse im Faktorraum $\mathcal{D}(\mathbb{R},\mathbb{R})/(\ker D)$ das unbestimmte Integral von h.

Beachte, dass eine Stammfunktion g eindeutig die Restklasse $g + C$ bestimmt, aber nicht umgekehrt.

(4) Wir haben durch Faktorisierung von $\mathcal{D}(\mathbb{R},\mathbb{R})$ nach dem Unterraum C der konstanten Funktionen und Einschränkung von $\mathcal{F}(\mathbb{R},\mathbb{R})$ auf $\operatorname{im} D$ den Differentiationsoperator „bijektiv gemacht".

Die Schulmathematik gibt diesen Prozess seit neuestem sprachlich durch die Begriffs-Paarung „Ableiten–Aufleiten" verkürzt wieder.

(5) Für $h \in \mathcal{C}(\mathbb{R},\mathbb{R}) \subsetneqq \operatorname{im} D$ kann eine Stammfunktion von h mit Hilfe des Hauptsatzes der Differential- und Integralrechnung angegeben werden. Es ist dann

$$\widetilde{g}_a(x) \quad = \quad \int_a^x h(t)\,dt,$$

wobei a irgendeine Stelle in der Definitionsmenge $\mathbb{R}$ ist. Der Umkehroperator hat die Form

$$\mathcal{L}(D|h) \quad = \quad \widehat{D}^{-1}(h) \;=\; \widetilde{g}_a + C.$$

Bei Auswahl eines anderen $a \in \mathbb{R}$ bleibt die Restklasse gleich.

7.5 Der Rang einer linearen Abbildung

7.5.1 Einstieg

In diesem Kapitel seien alle Vektorräume endlich-dimensional.

Für eine lineare Abbildung $f : V \to W$ hat der Satz 7.4.1 gezeigt, dass ein Isomorphismus

$$\widehat{f} : V/(\ker f) \to \operatorname{im} f$$

besteht. Aus Folgerung 7.2.6 wissen wir, dass die beiden beteiligten Räume die gleiche Dimension haben.

Diese Zahl hat für die lineare Abbildung eine große Bedeutung, weshalb sie einen eigenen Namen erhält.

7.5.2 Definition: Rang einer linearen Abbildung

Es sei $f : V \to W$ eine lineare Abbildung. Die Zahl

$$\operatorname{rang} f \quad := \quad \dim(\operatorname{im} f) \;=\; \dim V/(\ker f) \;=\; \dim V - \dim \ker f \quad \in \mathbb{N}_0$$

heißt *Rang* der linearen Abbildung.

Hat eine lineare Abbildung den größtmöglichen Rang, d.h.

$$\operatorname{rang} A \quad = \quad \min \big\{ \dim V, \dim W \big\},$$

so sagt man, sie hat *Vollrang*.

7.5.3 Satz: Rang bei Komposition von linearen Abbildungen

Es seien $f : V \to W$ eine lineare Abbildung. $h : \widetilde{V} \to V$ und $g : W \to \widetilde{W}$ seien weitere lineare Abbildungen.

$$\widetilde{V} \xrightarrow{h} V \xrightarrow{f} W \xrightarrow{g} \widetilde{W}$$

(i) Es gilt allgemein

$$\begin{aligned} \operatorname{rang}(g \circ f) &\le \operatorname{rang} f \\ \operatorname{rang}(f \circ h) &\le \operatorname{rang} f \end{aligned}$$

(ii) Ist h surjektiv, so gilt

$$\operatorname{rang}(f \circ h) \quad = \quad \operatorname{rang} f$$

(iii) Ist g injektiv, so gilt

$$\operatorname{rang}(g \circ f) \quad = \quad \operatorname{rang} f$$

(iv) Sind g und h bijektiv, so gilt

$$\operatorname{rang}(g \circ f \circ h) \quad = \quad \operatorname{rang} f$$

7.5.4 Beweis

(1) Es sei $B = \{w_1, \ldots, w_n\}$ eine Basis von $\operatorname{im} f$. Es ist dann die Menge

$$g(B) \;=\; \{g(w_1), \ldots, g(w_n)\}$$

ein Erzeugendensystem von $\operatorname{im}(g \circ f)$. Deshalb ist

$$\begin{aligned} \operatorname{rang}(g \circ f) &= \dim(\operatorname{im}(g \circ f)) \;\leq\; |\{g(w_1), \ldots, g(w_n)\}| \\ &\leq\; n \;=\; \dim(\operatorname{im} f) \;=\; \operatorname{rang} f. \end{aligned}$$

(2) Ist g zusätzlich injektiv, so ist $g(B)$ sogar Basis von $\operatorname{im}(g \circ f)$, vgl. Satz 7.2.3(i). Es ist dann

$$\begin{aligned} \operatorname{rang}(g \circ f) &= \dim(\operatorname{im}(g \circ f)) \;=\; |\{g(w_1), \ldots, g(w_n)\}| \\ &=\; n \;=\; \dim(\operatorname{im} f) \;=\; \operatorname{rang} f. \end{aligned}$$

(3) Es ist $\operatorname{im} h \subseteq V$, deshalb $\operatorname{im}(f \circ h) \subseteq \operatorname{im} f$ und deswegen

$$\operatorname{rang}(f \circ h) \;=\; \dim(\operatorname{im}(f \circ h)) \;\leq\; \dim(\operatorname{im} f) \;=\; \operatorname{rang} f.$$

(4) Ist h zusätzlich surjektiv, so ist $\operatorname{im}(f \circ h) \;=\; \operatorname{im} f$ und dann

$$\operatorname{rang}(f \circ h) \;=\; \dim(\operatorname{im}(f \circ h)) \;=\; \dim(\operatorname{im} f) \;=\; \operatorname{rang} f.$$

7.5.5 Satz: Rang bei Erweiterung von linearen Abbildungen

Es seien eine lineare Abbildung $f : V \to W$ und ein $b \in W$ gegeben.

In Bezug zu diesen Daten definieren wir die so genannte *erweiterte* Abbildung

$$f|b : \begin{cases} V \oplus \mathbb{K} & \to \quad W \\ (v, \alpha) & \mapsto \quad f(v) + \alpha\, b. \end{cases}$$

Dann gelten die folgenden Aussagen:

(i) $\operatorname{rang} f \;\leq\; \operatorname{rang} f|b$

(ii) $\operatorname{rang} f \;=\; \operatorname{rang} f|b \qquad \Longleftrightarrow \qquad b \in \operatorname{im} f.$

7.5.6 Beweis

Es ist sofort zu sehen, dass

$$\operatorname{im} f \;\subseteq\; \operatorname{im} f|b, \qquad (*)$$

woraus sofort die Aussage (i) folgt. Die zweite Aussage kann man der folgenden Äquivalenzkette entnehmen

$$\begin{aligned} & \operatorname{rang} f \;=\; \operatorname{rang} f|b \\ \Longleftrightarrow\quad & \dim(\operatorname{im} f) \;=\; \dim(\operatorname{im} f|b) \\ \overset{(*)}{\Longleftrightarrow}\quad & \operatorname{im} f \;=\; \operatorname{im} f|b \\ \overset{\text{def } f|b}{\Longleftrightarrow}\quad & b \in \operatorname{im} f. \end{aligned}$$

7.6 Der Rang einer Matrix

Nachdem wir eine $m \times n$-Matrix A als lineare Abbildung $\ell_A : \mathbb{K}^n \to \mathbb{K}^m$ auffassen können, ist der Rang auch für Matrizen definiert.

7.6.1 Satz: Rang einer Matrix

Es sei $A \in \mathbb{K}^{m \times n}$ eine Matrix. Die folgenden Aussagen bestimmen den Rang:

(A) $\operatorname{rang} A \;=\; \dim(\operatorname{im} A)$

(B) $\operatorname{rang} A \;=\; n - \dim(\ker A)$

(C) Der Rang ist gleich dem *Spaltenrang*, das ist die Maximalzahl linear unabhängiger Spaltenvektoren von A.

(D) Der Rang ist gleich dem *Zeilenrang*, das ist die Maximalzahl linear unabhängiger Zeilenvektoren von A.

7.6.2 Beweis

Die Äquivalenz von (A) und (B) wurde bereits in Abschnitt 7.5.2 konstatiert.

Die Äquivalenz von (A) und (C) folgt daraus, dass die Spaltenvektoren von A als Bilder der Einheitsvektoren aus $\mathbb{K}^n$ das Bild von A aufspannen.

Die Äquivalenz von (C) und (D) wird im Verlauf dieses Abschnitts noch bewiesen.

7.6.3 Satz: Rang-Stabilität Es sei $A \in \mathbb{K}^{m \times n}$.

(i) Sind $B \in \mathbb{K}^{n \times n}$ und $C \in \mathbb{K}^{m \times m}$ zwei invertierbare Matrizen, so gilt

$$\operatorname{rang} CAB \;=\; \operatorname{rang} A.$$

(ii) Wird die Matrix A durch elementare Zeilenumformungen oder Spaltenumformungen in eine andere Matrix $\widetilde{A}$ umgeformt, so bleibt dabei der Rang gleich:

$$\operatorname{rang} \widetilde{A} \;=\; \operatorname{rang} A.$$

7.6.4 Beweis

(i) Die Aussage ist eine direkte Umsetzung der Aussage (iv) aus Satz 7.5.3.

(ii) Hier müssen wir nur daran erinnern, dass Zeilen- und Spaltenumformungen bei einer gegebenen Matrix durch Links- bzw. Rechtsmultiplikation mit den invertierbaren Matrizen $Q_{j|\alpha}$, $\alpha \in \mathbb{K} \setminus \{0\}$, T_{jk} bzw. R_{jk} aus Kapitel 2.7 realisiert werden können.

7.6.5 Satz: Spaltenrang und Zeilenrang bei Erweiterung

Wir betrachten die Matrix

$$A|b \quad = \quad \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array} \right),$$

sie besteht aus der $m \times n$ –Matrix A und dem Spaltenvektor $b \in \mathbb{K}^m$.

Dann gelten die folgenden Aussagen:

(i) Spaltenrang $A \quad \leq \quad$ Spaltenrang $A|b$

(ii) Zeilenrang $A \quad \leq \quad$ Zeilenrang $A|b$

Ist der Spaltenvektor b eine Linearkombination der Spaltenvektoren von A, so gelten die folgenden Aussagen:

(iii) Spaltenrang $A \quad = \quad$ Spaltenrang $A|b$

(iv) Zeilenrang $A \quad = \quad$ Zeilenrang $A|b$

Die entsprechend dualen Aussagen gelten genauso für das Weglassen bzw. Hinzufügen einer Zeile bei einer Matrix

$$\frac{A}{b} \quad = \quad \left(\begin{array}{ccc} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \\ \hline b_1 & \cdots & b_n \end{array} \right).$$

7.6.6 Beweis

Die Aussagen (i) und (iii) sind trivial. Die letzte Aussage wird, wie gesagt, dual zu den anderen bewiesen.

Zu (ii): Es sei $r \leq m$ der Zeilenrang von A. Wir können **O**hne **B**eschränkung **d**er **A**llgemeinheit (O.B.d.A) annehmen, dass gerade die oberen r Zeilen

$$(a_{j1}, \ldots, a_{jn}), \qquad j = 1, \ldots, r$$

von A linear unabhängig sind. Anderenfalls führen wir Zeilenvertauschungen durch, die ja den Zeilenrang nicht verändern.

Es sei nun

$$(0, \ldots, 0) \quad = \quad \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}, b_j) \qquad \in \mathbb{K}^{1 \times (n+1)}$$

eine Linearkombination der ersten Zeilen von $A|b$, die die ,,Nullzeile” ergibt. Durch Weglassen der letzten Koordinate in der Linearkombination folgt

$$(0, \ldots, 0) \quad = \quad \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}) \qquad \in \mathbb{K}^{1 \times n}.$$

Da aber diese Zeilenvektoren linear unabhängig sind, folgt

$$\beta_j \;=\; 0 \qquad j = 1, \ldots, r.$$

Das bedeutet, dass auch die ersten r Zeilenvektoren von $A|b$ linear unabhängig sind.

Zu (iv): Es sei jetzt $r \leq m$ der Zeilenrang von $A|b$. Wir können wieder O.B.d.A. annehmen, dass gerade die oberen r Zeilen

$$(a_{j1}, \ldots, a_{jn}, b_j), \qquad j = 1, \ldots, r$$

von $A|b$ linear unabhängig sind. Es sei nun

$$(0, \ldots, 0) \;=\; \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}) \qquad \in \mathbb{K}^{1 \times n} \qquad (*)$$

eine Linearkombination der oberen r Zeilen von A, die die „Nullzeile" ergibt. Da b eine Linearkombination der Spaltenvektoren von A ist, können wir schreiben:

$$b \;=\; \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \;=\; \sum_{k=1}^{n} \gamma_k \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix}.$$

Daraus folgt, dass

$$\begin{aligned} \sum_{j=1}^{r} \beta_j b_j \;&=\; \sum_{j=1}^{r} \beta_j \cdot \big(\sum_{k=1}^{n} \gamma_k a_{jk} \big) \\ &=\; \sum_{j=1}^{r} \sum_{k=1}^{n} \beta_j \gamma_k \cdot a_{jk} \;=\; \sum_{k=1}^{n} \sum_{j=1}^{r} \gamma_k \beta_j \cdot a_{jk} \qquad \text{(Doppelsumme mit } r \cdot n \text{ Summanden)} \\ &=\; \sum_{k=1}^{n} \gamma_k \cdot \big(\sum_{j=1}^{r} \beta_j \cdot a_{jk} \big) \;=\; \sum_{k=1}^{n} \gamma_k \cdot 0 \;=\; 0. \end{aligned}$$

Das bedeutet aber, dass die Gleichung $(*)$ zu

$$(0, \ldots, 0) \;=\; \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}, b_j) \qquad \in \mathbb{K}^{1 \times (n+1)}$$

erweitert werden kann. Wegen der linearen Unabhängigkeit der Zeilenvektoren auf der rechten Seite dieser Gleichung folgt

$$\beta_j \;=\; 0 \quad \text{für} \quad j = 1, \ldots, r,$$

also sind auch die oberen r Zeilenvektoren von A linear unabhängig und damit hat A den Zeilenrang r.

7.6.7 Satz: Spaltenrang gleich Zeilenrang

Für eine beliebige $m \times n$–Matrix A gilt: $\qquad$ Zeilenrang $A \;=\;$ Spaltenrang A.

7.6.8 Beweis

(1) Wir lassen, bis es nicht mehr weiter möglich ist, nacheinander in der $m \times n$–Matrix A Spaltenvektoren oder Zeilenvektoren weg, die Linearkombinationen der anderen Spaltenvektoren bzw. Zeilenvektoren sind. Es entsteht eine $p \times q$–Matrix A', deren Spalten– bzw. Zeilenrang mit dem von A aufgrund von Satz 7.6.5 (iii),(iv) übereinstimmt.

(2) A' enthält nur noch linear unabhängige Spaltenvektoren und linear unabhängige Zeilenvektoren.

Im Fall $q > p$ hätte man $q > p$ linear unabhängige Vektoren im Raum $\mathbb{K}^{p\times 1}$ der Spaltenvektoren. Widerspruch.

Im Fall $p > q$ hätte man $p > q$ linear unabhängige Vektoren im Raum $\mathbb{K}^{1\times q}$ der Zeilenvektoren. Widerspruch.

Es muss also $p = q$ sein.

(3) Zusammengefasst gilt nun

$$\text{Spaltenrang } A \;=\; \text{Spaltenrang } A' \;=\; q \;=\; p \;=\; \text{Zeilenrang } A' \;=\; \text{Zeilenrang } A.$$

7.7 Struktur und Dimension von Lösungsmengen

7.7.1 Definitionen

Es sei $f : V \to W$ eine lineare Abbildung zwischen zwei $\mathbb{K}$-Vektorräumen V und W.

Man denke im folgenden vor allem an den Fall, dass es sich bei f um eine als lineare Abbildung aufgefasste Matrix $A : \mathbb{K}^n \to \mathbb{K}^m$ handelt.

Ist zusätzlich $b \in W$ vorgegeben, so entsteht eine Gleichung

$$f(x) \quad = \quad b \qquad\qquad \text{(iLG)}$$

Ersetzt man in der linearen Gleichung b durch $\vec{0} \in W$, so entsteht die zur Gleichung (iLG) gehörige *homogene* Gleichung

$$f(x) \quad = \quad \vec{0} \qquad\qquad \text{(hLG)}$$

Diesbezüglich heißt dann die Gleichung (iLG) auch *inhomogen*.

Wie im Kapitel 3.1 über LGSe bezeichnen wir die Lösungsmenge mit

$$\mathcal{L}(f|b) \quad = \quad \Big\{ x \in \mathbb{K}^n \Big| f(x) = b \Big\}.$$

Wir können jetzt verschiedene Begriffe und Einsichten, die wir über lineare Abbildungen gewonnen haben, zur Beschreibung von Lösungsmengen verwenden. Das bedeutet nicht, dass die Verfahren zur konkreten Lösung von LGSen in Kapitel 3.3 überflüssig oder vereinfacht werden, sie werden aber ,,einsichtiger".

7.7.2 Satz: Struktur und Dimension der Lösungsmenge bei homogenen Gleichungen

Es sei $f : V \to W$ eine lineare Abbildung.

(i) Die Lösungsmenge der homogenen Gleichung (hLG) ist gleich dem Kern der linearen Abbildung f

$$\mathcal{L}(f|\vec{0}) \quad = \quad \ker f.$$

Insbesondere ist $\mathcal{L}(f|\vec{0})$ ein Unterraum von V und damit auch nicht-leer.

(ii) Im endlich-dimensionalen Fall ist

$$\dim \ker f \quad = \quad \dim V - \operatorname{rang} f.$$

7.7.3 Beweis

Die erste Aussage ist nur eine Umschreibung der Definition. Die zweite beruht auf der Definition 7.5.2 des Rangs und damit auf Satz 7.4.1(iii).

7.7.4 Satz: Existenz von Lösungen bei inhomogenen Gleichungen

Im endlich-dimensionalen Fall ist

$$\mathcal{L}(f|b) \quad \neq \quad \varnothing \qquad \Longleftrightarrow \qquad \operatorname{rang} f \ = \ \operatorname{rang}(f|b).$$

7.7.5 Beweis

Das geht unmittelbar aus Satz 7.5.5(ii) hervor.

7.7.6 Satz: Struktur der Lösungsmenge bei inhomogenen Gleichungen

Es sei $f : V \to W$ eine lineare Abbildung und $b \in W$. Wir nehmen an, dass die inhomogene Gleichung eine Lösung x hat, was auch ausgedrückt werden kann als

$$\mathcal{L}(f|b) \quad \neq \quad \varnothing \qquad\qquad \text{oder} \qquad\qquad b \in \operatorname{im} f.$$

Die kanonische Zerlegung von f gemäß Satz 7.4.1(iii) wirkt sich wie folgt auf die Elemente x der Lösungsmenge aus:

$$\begin{tikzcd}
V \arrow[r, "p"] \arrow[rrr, bend left, "f"] & V/(\ker f) \arrow[r, shift left, "\widehat{f}"] & \operatorname{im} f \arrow[l, shift left, "\widehat{f}^{-1}"] \arrow[r, "\iota"] & W \\
x \arrow[r, mapsto] & x + \ker f \arrow[r, mapsto, shift left] & b \arrow[l, mapsto, shift left] \arrow[r, mapsto] & b
\end{tikzcd}$$

Das bedeutet genauer:

(i) Ist $x \in V$ irgendeine spezielle Lösung der inhomogenen Gleichung (iLG), so ist die gesamte Lösungsmenge gegeben durch

$$\mathcal{L}(f|b) \quad = \quad \widehat{f}^{-1}(b) \; = \; x + \ker f.$$

(ii) Anders ausgedrückt: Ein Vektor $\widetilde{x} \in V$ ist genau dann

eine Lösung der inhomogenen Gleichung (iLG), wenn er

sich darstellen lässt als Summe der speziellen Lösung x der inhomogenen Gleichung (iLG) und einer Lösung der homogenen Gleichung (hLG).

(iii) Die Abbildung $\widehat{f}^{-1}$ ist linear

$$\alpha\,\mathcal{L}(f|b) + \widetilde{\alpha}\,\mathcal{L}(f|\widetilde{b}) \quad = \quad \mathcal{L}(f|\alpha\, b + \widetilde{\alpha}\,\widetilde{b})$$

Anders ausgedrückt: Ist v eine Lösung der Gleichung $f(x) = b$ und $\widetilde{v}$ eine Lösung der Gleichung $f(x) = \widetilde{b}$, so ist $\alpha\, v + \widetilde{\alpha}\,\widetilde{v}$ eine Lösung der Gleichung $f(x) = \alpha\, b + \widetilde{\alpha}\,\widetilde{b}$.

(iv) Die Differenz zweier Lösungen der inhomogenen Gleichung (iLG) ist eine Lösung der homogenen Gleichung (hLG).

7.7.7 Beweis Es müssen nur bisherige Ergebnisse und Definitionen genau umgesetzt werden.

7.8 Beispiele

7.8.1 Beispiel Betrachte das LGS

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Es ist leicht zu sehen, dass

$$\ker A = \operatorname{span}\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} = \left\{ k_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + k_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \middle| k_1, k_2 \in \mathbb{R} \right\}$$

$$\operatorname{im} A = \operatorname{span}\left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\} = \left\{ k \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \middle| k \in \mathbb{R} \right\}$$

Die Vektoren

$$v = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \qquad v' = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad v'' = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

sind Beispiele für spezielle Lösungen, deshalb hat die Lösungsmenge die Form

$$\mathcal{L}(A|b) = v + \ker A = v' + \ker A = v'' + \ker A.$$

7.8.2 Beispiel Betrachte das LGS

$$\begin{pmatrix} 6 & -12 & 2 \\ -2 & 4 & -\frac{2}{3} \\ 4 & -8 & \frac{4}{3} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \\ 2 \end{pmatrix}$$

Es ist leicht zu sehen, dass

$$\ker A = \operatorname{span}\left\{ \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} \right\}, \qquad \operatorname{im} A = \operatorname{span}\left\{ \begin{pmatrix} 3 \\ -1 \\ 2 \end{pmatrix} \right\}.$$

Die Vektoren

$$v = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}, \qquad v' = \begin{pmatrix} 0 \\ -\frac{1}{4} \\ 0 \end{pmatrix}, \qquad v'' = \begin{pmatrix} 0 \\ 0 \\ \frac{3}{2} \end{pmatrix}$$

sind spezielle Lösungen, deshalb hat die Lösungsmenge die Form

$$\mathcal{L}(A|b) = v + \ker A = v' + \ker A = v'' + \ker A.$$

8 Permutationen

8.1 Einführung

8.1.1 Definition: Permutationen

1. Es sei X eine Menge. Eine bijektive Abbildung $f : X \to X$ heißt auch *Permutation von* X.

2. Die Menge aller Permutationen einer Menge X bezeichnen wir mit

$$\mathcal{S}(X) \ := \ \left\{ f : X \to X \ \middle| \ f \text{ ist bijektiv} \right\}.$$

8.1.2 Beobachtung

Die Menge $\mathcal{S}(X)$ bildet mit der Hintereinanderausführung als Verknüpfung

$$\circ : \begin{cases} \mathcal{S}(X) \times \mathcal{S}(X) & \to & \mathcal{S}(X) \\ (f, g) & \mapsto & f \circ g \end{cases}$$

eine Gruppe. Das neutrale Element ist durch die identische Abbildung id_X gegeben. Die zu einer Abbildung $f \in \mathcal{S}(X)$ inverse Abbildung ist gegeben durch die Umkehrabbildung f^{-1}. Für $|X| > 2$ ist die Gruppe nicht-kommutativ.

8.1.3 Definition: Die Symmetrische Gruppe

Ist X eine endliche Menge der Mächtigkeit n, so heißt $\mathcal{S}(X)$ die *Symmetrische Gruppe auf* n *Elementen (oder* n *Buchstaben) oder* n *Symbolen.*

Im allgemeinen hat man es mit der Menge $X = \{1, 2, \ldots, n\}$ zu tun.

Man kürzt $\mathcal{S}_n = \mathcal{S}(\{1, 2, \ldots, n\})$ ab. Die Elemente von $\mathcal{S}_n$ werden im allgemeinen durch den Buchstaben π gekennzeichnet. Die Hintereinanderausführung zweier Permutationen schreiben wir ab jetzt als Multiplikation:

$$\pi_1 \cdot \pi_2 \ = \ \pi_1 \circ \pi_2.$$

Wie sonst auch üblich, kann das Multiplikationszeichen $\cdot$ auch weggelassen werden.

8.1.4 Beispiele

- $\mathcal{S}_1$ besteht nur aus der identischen Abbildung $\mathrm{id} : \{1\} \to \{1\}$. Als Gruppe ist dies wieder die triviale Gruppe. $\mathcal{S}_1 = \{\mathrm{id}\}$.

- $\mathcal{S}_2$ enthält zwei Abbildungen, nämlich die identische Abbildung $\iota = \mathrm{id}_X$ und die Vertauschung der beiden Elemente 1 und 2. Bezeichnen wir letztere mit τ, so gilt für die Verknüpfungen:

$\cdot$	ι	τ
ι	ι	τ
τ	τ	ι

  Diese Struktur ist wieder die gleiche wie die von $\mathbb{Z}_2 = \{g, u\}$. Man sagt, die Gruppen $(\mathbb{Z}_2, \oplus)$ und $(\mathcal{S}_2, \circ)$ sind *isomorph (gleichstrukturiert)*. Auch die Gruppe $(\{-1, +1\}, \cdot)$ ist isomorph zu diesen beiden Gruppen.

- Wir betrachten jetzt die Gruppe $\mathcal{S}_3$ der bijektiven Abbildungen in $\{1,2,3\}$. Wir bezeichnen für $a,b,c \in \{1,2,3\}$ die Abbildung

$$\pi : \begin{cases} 1 \mapsto a \\ 2 \mapsto b \\ 3 \mapsto c \end{cases} \qquad \text{mit} \qquad \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}.$$

  Dann gilt:

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

  Die Gruppe $\mathcal{S}_3$ ist nicht kommutativ.

- Allgemeiner bezeichnen wir ein Element $\pi \in \mathcal{S}_n$

$$\pi : \begin{cases} 1 & \mapsto & x_1 \\ 2 & \mapsto & x_2 \\ & \vdots & \\ n & \mapsto & x_n \end{cases} \qquad \text{mit} \qquad \begin{pmatrix} 1 & 2 & \cdots & n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}.$$

- Mit Hilfe eines Induktionsbeweises kann gezeigt werden, dass $|\mathcal{S}_n| = n!$

8.2 Zyklen und Transpositionen

8.2.1 Definitionen

1. Eine Permutation $\pi \in \mathcal{S}_n$ heißt *Zyklus (der Länge k)*, wenn die Menge $\{1, 2, \ldots, n\}$ in zwei disjunkte Teilmengen zerfällt

$$\{1, 2, \ldots, n\} \;=\; \{m_1, m_2, \ldots, m_k\} \,\dot\cup\, \{\ell_1, \ell_2, \ldots, \ell_{n-k}\}, \qquad k \geq 2,$$

so dass

$$\begin{aligned} \pi(m_i) &= m_{i+1} \quad \text{für } i = 1, \ldots, k-1, \qquad \pi(m_k) = m_1 \\ \pi(\ell_i) &= \ell_i \quad \text{für } i = 1, \ldots, n-k. \end{aligned}$$

2. Die Zahlen $m_1, m_2, \ldots, m_k$ heißen die *Elemente* des Zyklus.

3. Zwei Zyklen heißen *disjunkt*, wenn ihre Elemente paarweise verschieden sind.

4. Ein Zyklus der Länge 2 heißt *Transposition*.

5. In diesem Zusammenhang wird die identische Permutation als Zyklus der Länge 1 aufgefasst.

8.2.2 Zyklen-Schreibweise

Wenn die Zahl n aus dem Kontext bekannt ist, wird hier eine andere Schreibweise verwendet:

$$\begin{aligned} (1\,3) &:= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{(Transposition)} \\ (1\,4\,5) = (4\,5\,1) = (5\,1\,4) &:= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix} \\ (2\,5\,3\,7\,4) &:= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 7 & 2 & 3 & 6 & 4 & 8 \end{pmatrix} \\ (1) &:= \text{id.} \end{aligned}$$

8.2.3 Beobachtung

Sind zwei Zyklen disjunkt, so ist ihr Produkt von der Reihenfolge unabhängig:

$$(p_1\, p_2, \ldots, p_k) \cdot (q_1\, q_2, \ldots, q_j) \;=\; (q_1\, q_2, \ldots, q_j) \cdot (p_1\, p_2, \ldots, p_k).$$

Bei der Multiplikation von nicht disjunkten Zyklen muss man ,,höllisch" aufpassen. Dies wollen wir aber nur für Transpositionen ausprobieren:

$$(2\,3)(3\,5) \;=\; (2\,3\,5).$$

Teste dabei nacheinander die Wirkung dieser Abbildung auf die einzelnen Zahlen aus $\{1, 2, \ldots, n\}$ aus. Beachte, dass Permutationen Abbildungen sind und daher von rechts nach links ausgeführt werden.

$$(3\,5)(2\,3) \;=\; (2\,5\,3).$$

Innerhalb eines Zyklus erfolgt dagegen die Zuordnung in Links-Rechts-Richtung.

8.3 Zerlegung von Permutationen

8.3.1 Satz: Zerlegung von Permutationen

(i) Jede Permutation π kann als Produkt von paarweise disjunkten Zyklen geschrieben werden. Die Faktoren sind eindeutig.

(ii) Jeder Zyklus der Länge k kann als Produkt von $k-1$ Transpositionen geschrieben werden.

(iii) Folgerung: Jede Permutation π kann als Produkt von Transpositionen geschrieben werden.

8.3.2 Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 2 & 7 & 1 & 6 & 4 & 3 \end{pmatrix} = (1\,5)\cdot(2\,8\,3)\cdot(4\,7).$$

8.3.3 Beweis

Zu (i): (1) Für die gegebene Permutation π bestimme man zunächst die Menge M der Zahlen, die nicht auf sich selbst abgebildet werden.

(2) Wähle eine Zahl $j \in M$ und ,,starte" den zugehörigen Zyklus

$$j \mapsto \pi(j) \mapsto \pi^2(j) \mapsto \ldots \mapsto \pi^k(j) \mapsto \ldots$$

(3) Da für die Werte dieser Folge nur die Zahlen aus $\{1,\ldots,n\}$ zur Verfügung stehen, muss irgendwann eine der Zahlen zum zweiten Mal auftreten. Es sei

$$\ell := \min\Big\{k \in \mathbb{N} \mid \text{Es ex. } \widetilde{k} \in \{0,\ldots,k-1\} \text{ mit } \pi^{\widetilde{k}}(j) = \pi^k(j)\Big\}$$

die Zahl, bei der dieses ,,zweite Auftreten zum ersten Mal" passiert, und $\widetilde{\ell} < \ell$ die zugehörige kleinere Zahl, also

$$\pi^{\widetilde{\ell}}(j) = \pi^{\ell}(j).$$

(4) Wäre $\widetilde{\ell} > 0$, so können wir π^{-1} auf diese Gleichung anwenden,

$$\pi^{\widetilde{\ell}-1}(j) = \pi^{\ell-1}(j),$$

was der Minimalität von ℓ widerspricht. Es gilt also $\widetilde{\ell} = 0$ und $\pi^{\ell}(j) = j$, d.h. die erste Zahl j der Folge in (2) tritt als erste zum zweiten Mal auf. Das bedeutet, dass der Zyklus

$$\big(\, j \quad \pi(j) \quad \pi^2(j) \quad \cdots \quad \pi^{\ell-1}(j)\, \big)$$

ein ,,Bestandteil" der Permutation ist.

(5) Wähle aus M solange weitere Zahlen aus und konstruiere die zugehörigen Zyklen, bis alle Zahlen aus M erfasst sind.

Zu (ii): Es ist

$$\big(\, j_1 \quad j_2 \quad \cdots \quad j_k\, \big) = \big(\, j_1 \quad j_2\, \big)\cdot\big(\, j_2 \quad j_3\, \big)\cdots\big(\, j_{k-2} \quad j_{k-1}\, \big)\cdot\big(\, j_{k-1} \quad j_k\, \big).$$

8.4 Das Signum einer Permutation

8.4.1 Definition: Signum

Für eine Permutation $\pi \in \mathcal{S}_n$ definieren wir das *Signum* durch

$$\sigma(\pi) \ := \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i}.$$

Für jede zwei-elementige Teilmenge $\{i, j\} \subseteq \{1, \dots, n\}$ tritt in dem Produkt ein Faktor $\frac{\pi(j)-\pi(i)}{j-i}$ auf. Die Reihenfolge von i und j ist dabei unwesentlich, da eine Vertauschung eine Erweiterung mit -1 in dem Bruch bedeutet.

8.4.2 Beispiele

- Für $\pi = \big(1\,2\,3\big) \in \mathcal{S}_3$ ergibt sich

$$\sigma(\pi) \ = \ \frac{\pi(2) - \pi(1)}{2 - 1} \cdot \frac{\pi(3) - \pi(1)}{3 - 1} \cdot \frac{\pi(3) - \pi(2)}{3 - 2} = \frac{3 - 2}{2 - 1} \cdot \frac{1 - 2}{3 - 1} \cdot \frac{1 - 3}{3 - 2} \ = \ 1.$$

- Für $\pi = \big(1\,4\big) \in \mathcal{S}_4$ gilt

$$\sigma(\pi) \ =$$

$$\frac{\pi(2) - \pi(1)}{2 - 1} \cdot \frac{\pi(3) - \pi(1)}{3 - 1} \cdot \frac{\pi(4) - \pi(1)}{4 - 1} \cdot \frac{\pi(3) - \pi(2)}{3 - 2} \cdot \frac{\pi(4) - \pi(2)}{4 - 2} \cdot \frac{\pi(4) - \pi(3)}{4 - 3} \ =$$

$$\frac{2 - 4}{2 - 1} \cdot \frac{3 - 4}{3 - 1} \cdot \frac{1 - 4}{4 - 1} \cdot \frac{3 - 2}{3 - 2} \cdot \frac{1 - 2}{4 - 2} \cdot \frac{1 - 3}{4 - 3} \ =$$

$$\frac{-2}{1} \cdot \frac{-1}{2} \cdot \frac{-3}{3} \cdot \frac{1}{1} \cdot \frac{-1}{2} \cdot \frac{-2}{1} \ = \ -1.$$

8.4.3 Eigenschaften des Signums

(i) Es gilt für eine beliebige Permutation π:

$$\sigma(\pi) \in \{-1, +1\}.$$

(ii) Für zwei Permutationen $\pi_1, \pi_2 \in \mathcal{S}_n$ gilt

$$\sigma(\pi_1 \cdot \pi_2) \ = \ \sigma(\pi_1) \cdot \sigma(\pi_2).$$

(iii) Für die identische Permutation gilt $\sigma((1)) = +1$.

(iv) Für eine Permutation π und ihre Umkehr–Permutation π^{-1} gilt

$$\sigma(\pi) \ = \ \sigma(\pi^{-1}).$$

(v) Für eine Transposition $(k\,\ell)$ gilt

$$\sigma((k\,\ell)) \ = \ -1.$$

8.4.4 Beweis

(i) Betrachte die definierende Formel in Abschnitt 8.4.1. Da π bijektiv ist, gibt es zu jedem Paar (i,j) mit $i<j$ zwei Zahlen $k,\ell \in \{1,\ldots,n\}$, so dass $\pi(k)=i$ und $\pi(\ell)=j$. Also gibt es zu jeder Nenner–Kombination $j-i$ die Zählerkombination $\pi(k)-\pi(\ell)=i-j$ oder $\pi(\ell)-\pi(k)=j-i$. Diese Zuordnung ist umkehrbar eindeutig. Also kürzen sich alle Beträge ungleich 1 heraus. Es bleibt ,,nur das Vorzeichen" übrig.

(ii) Es gilt:

$$\begin{aligned}\sigma(\pi_1\cdot\pi_2) &\overset{\text{def}}{=} \prod_{1\le i<j\le n}\frac{\pi_1(\pi_2(j))-\pi_1(\pi_2(i))}{j-i}\\ &= \underbrace{\prod_{1\le i<j\le n}\frac{\pi_1(\pi_2(j))-\pi_1(\pi_2(i))}{\pi_2(j)-\pi_2(i)}}_{\sigma(\pi_1)}\cdot\underbrace{\prod_{1\le i<j\le n}\frac{\pi_2(j)-\pi_2(i)}{j-i}}_{\sigma(\pi_2)}.\end{aligned}$$

Dass auch die erste geschweifte Unterklammer stimmt, liegt daran, dass man statt über alle Paare $\{i,j\}$ zu multiplizieren, auch über alle Paare $\{\pi_2(i),\pi_2(j)\}$ multiplizieren kann.

(iii)

$$\sigma((1)) \;=\; \sigma((1)\cdot(1)) \;=\; \sigma((1))\cdot\sigma((1)) \quad\Longrightarrow\quad \sigma((1)) \;=\; 1.$$

(iv) Es gilt

$$\sigma(\pi)\cdot\sigma(\pi^{-1}) \;=\; \sigma(\pi\cdot\pi^{-1}) \;=\; \sigma((1)) \;=\; +1.$$

(v) Dies erfordert mehrere Schritte.

(1) Zunächst zeigen wir per Induktion über $n\in\mathbb{N}$, $n\ge 2$, dass $\sigma((12)_n)=-1$. Der Index n zeigt an, dass die Permutation als Element von $\mathcal{S}_n$ anzusehen ist.

(2a) Für $n=2$ ist

$$\sigma((12)_2) \;=\; \prod_{1\le i<j\le 2}\frac{(12)_2(j)-(12)_2(i)}{j-i} \;=\; \frac{1-2}{2-1} \;=\; -1.$$

(2b) Wenn die Aussage für $n-1$ gezeigt ist, so folgt

$$\begin{aligned}\sigma((12)_n) &= \prod_{1\le i<j\le n}\frac{(12)_n(j)-(12)_n(i)}{j-i}\\ &= \prod_{1\le i<j<n}\frac{(12)_n(j)-(12)_n(i)}{j-i}\cdot\prod_{1\le i<j=n}\frac{(12)_n(j)-(12)_n(i)}{j-i}\\ &= \prod_{1\le i<j\le n-1}\frac{(12)_n(j)-(12)_n(i)}{j-i}\cdot\underbrace{\prod_{1\le i\le n-1}\frac{n-(12)_n(i)}{n-i}}_{=1}\\ &= \sigma((12)_{n-1}) \;=\; -1.\end{aligned}$$

(3) Für eine beliebige Transposition $(k\,\ell)$ sei jetzt π eine Permutation mit $\pi(1)=k$ und $\pi(2)=\ell$. Dann gilt

$$\pi\cdot(1\,2)\cdot\pi^{-1} \;=\; (k\,\ell).$$

(4) Mit Eigenschaft (iv) des Satzes folgt:

$$\sigma((k\,\ell)) \;=\; \sigma(\pi\cdot(1\,2)\cdot\pi^{-1}) \;=\; \sigma(\pi)\cdot\sigma((1\,2))\cdot\sigma(\pi^{-1}) \;=\; \sigma((1\,2)) \;=\; -1.$$

8.4.5 Folgerung und Definition

Für eine Permutation π sind die folgenden Aussagen äquivalent:

(A) (Def) π heißt gerade.

(B) Es ist $\sigma(\pi) = +1$.

(C) π lässt sich als Produkt einer geraden Anzahl von Transpositionen darstellen.

(D) π lässt sich nicht als Produkt einer ungeraden Anzahl von Transpositionen darstellen.

8.4.6 Beweis

Nach Satz 8.3.1 kann π als Produkt von Transpositionen geschrieben werden:

$$\pi = \vartheta_1 \cdot \vartheta_2 \cdot \ldots \cdot \vartheta_m.$$

Dann folgt mit den Eigenschaften (iii) und (v) aus Satz 8.4.3:

$$\sigma(\pi) = \sigma(\vartheta_1) \cdot \sigma(\vartheta_2) \cdot \ldots \cdot \sigma(\vartheta_m) = (-1)^m.$$

Dieser Gleichung lassen sich die Äquivalenzen entnehmen.

8.4.7 Folgerungen

- Für einen Zyklus der Länge k gilt

  $$\sigma(\begin{pmatrix} m_1 & m_2 & \cdots & m_k \end{pmatrix}) = (-1)^{k+1}.$$

  d.h. das Signum ist genau dann gerade, wenn die Länge ungerade ist.

- Die Menge der geraden Permutationen

  $$\mathcal{A}_n := \{\pi \in \mathcal{S}_n | \sigma(\pi) = +1\}$$

  bildet eine Untergruppe von $\mathcal{S}_n$, d.h. das Produkt zweier Permutationen aus $\mathcal{A}_n$ liegt wieder in $\mathcal{A}_n$.

9 Determinanten

9.1 Definition

9.1.1 Der Graph einer Permutation

Es sei $n \in \mathbb{N}$ fixiert und wieder $X = \{1, \ldots, n\}$. Zu einer Permutation $\pi \in \mathcal{S}_n$ betrachten wir den Graphen

$$G_\pi \quad = \quad \big\{(1, \pi(1)), (2, \pi(2)), \ldots, (n, \pi(n))\big\} \ \subseteq \ X \times X.$$

Die Menge $X \times X$ kann man sich als quadratisch angeordnetes Gitter mit n^2 Elementen vorstellen:

$$X \times X \quad = \quad \left\{ \begin{array}{cccc} (1,1) & (1,2) & \cdots & (1,n) \\ (2,1) & (2,2) & \cdots & (2,n) \\ \vdots & \vdots & & \vdots \\ (n,1) & (n,2) & \cdots & (n,n) \end{array} \right\}.$$

Der Graph G_π ist dann eine n-Teilmenge dieses Gitters, so dass jede Zeilennummer als erste Koordinate und jede Spaltennummer als zweite Koordinate genau einmal vorkommt.

In diesem Zusammenhang deutet man die Permutation π so, dass jeder Zeilennummer aus $\{1, \ldots, n\}$ durch π ein-eindeutig eine Spaltennummer aus $\{1, \ldots, n\}$ zugeordnet wird.

Umgekehrt kann man den Standpunkt einnehmen, dass jeder Spaltennummer durch π^{-1} ein-eindeutig eine Zeilennummer zugeordnet wird. Das bedeutet, dass der Graph der Permutation auch geschrieben werden kann als

$$G_\pi \quad = \quad \{(\pi^{-1}(1), 1), (\pi^{-1}(2), 2), \ldots, (\pi^{-1}(n), n)\}.$$

9.1.2 Definition Determinante Wir betrachten eine quadratische Matrix

$$A \quad = \quad (a_{jk}) \quad = \quad \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathbb{K}^{n \times n}.$$

und entwickeln die Definition der Determinante mittels einer ,,Bastelanleitung”

$\boxed{\text{A}}$ Auswahl: Wähle aus den n^2 Einträgen a_{jk} der Matrix n Einträge so aus, dass jede Zeilennummer genau einmal als erster und jede Spaltennummer genau einmal als zweiter Index vorkommt.

Dieser Auswahl entspricht der Graph G_π einer Permutation $\pi \in \mathcal{S}_n$, siehe Abschnitt 9.1.1.

$\boxed{\text{M}}$ Multiplikation: Die ausgewählten n Einträge werden multipliziert:

$$\prod_{(j,k) \in G_\pi} a_{jk}$$

$\boxed{\text{S}}$ Signum: Dieses Produkt wird mit dem Signum $\sigma(\pi)$ der Permutation versehen:

$$\sigma(\pi) \cdot \prod_{(j,k) \in G_\pi} a_{jk}.$$

$\boxed{\text{A}}$ Addition: Dann werden alle nach diesem Verfahren herstellbaren Produkte aufaddiert. Das heißt, man muss über alle möglichen Permutationen $\pi \in \mathcal{S}_n$ addieren.

Damit ergibt sich die Gesamtformel für die *Determinante* der Matrix A.

$$\det A \quad := \quad \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{(j,k) \in G_\pi} a_{jk}.$$

Die zugehörige Abbildung

$$\det : \mathbb{K}^{n \times n} \to \mathbb{K}$$

heißt *Determinantenfunktion.*

9.1.3 Leibniz-Formel (zeilenweise)

Für eine feste Permutation π gilt aufgrund der Vorüberlegungen aus Abschnitt 9.1.1.

$$\prod_{(j,k) \in G_\pi} a_{jk} \quad = \quad a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)}. \qquad \text{(von oben nach unten)}$$

Diese Reihenfolge im Produkt entspricht der zeilenweisen Abarbeitung der Permutation — von oben nach unten. Es folgt die (zeilenweise) *Leibniz–Formel*

$$\det A \quad = \quad \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)}.$$

9.1.4 Leibniz-Formel (spaltenweise)

Für eine feste Permutation π gilt aufgrund der Vorüberlegungen aus Abschnitt 9.1.1 auch

$$\prod_{(j,k) \in G_\pi} a_{jk} \quad = \quad a_{\pi^{-1}(1),1} \cdot a_{\pi^{-1}(2),2} \cdot \ldots \cdot a_{\pi^{-1}(n),n}.$$

Diese Reihenfolge im Produkt entspricht der spaltenweisen Abarbeitung der Permutation — von links nach rechts. Es folgt dann

$$\begin{aligned}
\det A \quad &= \quad \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a_{\pi^{-1}(1),1} \cdot a_{\pi^{-1}(2),2} \cdot \ldots \cdot a_{\pi^{-1}(n),n} \\
&\qquad \text{(Das Signum einer Permutation ist gleich dem der inversen Permutation, vgl. Satz 8.4.3(iv))} \\
&= \quad \sum_{\pi \in \mathcal{S}_n} \sigma(\pi^{-1}) \cdot a_{\pi^{-1}(1),1} \cdot a_{\pi^{-1}(2),2} \cdot \ldots \cdot a_{\pi^{-1}(n),n} \\
&\qquad \text{(Summation über alle inversen Permutationen ist das gleiche wie Summation über alle Permutationen)} \\
&= \quad \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}.
\end{aligned}$$

Die letzte Zeile beinhaltet die (spaltenweise) Leibniz–Formel

$$\det A \quad = \quad \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}.$$

9.1.5 Beispiele

(1) Im Fall $n = 1$ ist die Matrix $A = (a)$ einfach eine Zahl. Es gilt

$$\det A \;=\; a.$$

(2) Es sei $n = 2$ und $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Dann gilt

$$\begin{aligned} \det A \;&=\; \sum_{\pi \in \mathcal{S}_2} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{j,\pi(j)} \;=\; \underbrace{(+1) \cdot a_{11}a_{22}}_{\pi=(1)} + \underbrace{(-1) \cdot a_{12}a_{21}}_{\pi=(1\,2)} \\ &=\; a_{11} \cdot a_{22} - a_{12} \cdot a_{21}. \end{aligned}$$

(3) $n = 3$ und $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$. Die Gruppe $\mathcal{S}_3$ enthält sechs Permutationen, nämlich

$$\mathcal{S}_3 \;=\; \big\{(1), (1\,2\,3), (1\,3\,2), (1\,2)(1\,3), (2\,3)\big\}.$$

Damit ergibt sich

$$\begin{aligned} \det(A) \;=\; &+ a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} \\ &- a_{12}a_{21}a_{33} - a_{13}a_{31}a_{22} - a_{23}a_{32}a_{11}. \end{aligned}$$

Diese Formel lässt sich graphisch durch die *Regel von Sarrus* repräsentieren:

$$\begin{array}{ccccc} + & + & + \;\; - & - & - \end{array}$$
$$\left(\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}\right)$$

9.2 Eigenschaften

9.2.1 Satz: Eigenschaften der Determinantenfunktion

(i) Die Determinantenfunktion hat folgende Eigenschaften:

(M) Sie ist multilinear, d.h. linear in jeder **einzelnen** Spalte. Das heißt, für jedes $\ell \in \{1, \ldots, n\}$ und $\alpha \in \mathbb{K}$ gilt:

$$\begin{aligned} & \det \begin{pmatrix} a_1 & \cdots & a_{\ell-1} & a_\ell + \widetilde{a}_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \\ = & \det \begin{pmatrix} a_1 & \cdots & a_{\ell-1} & a_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \\ & \qquad + \det \begin{pmatrix} a_1 & \cdots & a_{\ell-1} & \widetilde{a}_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \end{aligned}$$

$$\begin{aligned} & \det \begin{pmatrix} a_1 & \cdots & a_{\ell-1} & \alpha \cdot a_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \\ = & \alpha \cdot \det \begin{pmatrix} a_1 & \cdots & a_{\ell-1} & a_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix}. \end{aligned}$$

(A) Sie ist alternierend in den Spalten, d.h. sie wechselt bei der Vertauschung zweier Spalten das Vorzeichen:

$$\begin{aligned} & \det \begin{pmatrix} a_1 & \cdots & a_m & \cdots & a_\ell & \cdots & a_n \end{pmatrix} \\ = & -\det \begin{pmatrix} a_1 & \cdots & a_\ell & \cdots & a_m & \cdots & a_n \end{pmatrix}. \end{aligned}$$

(N) Sie ist normiert, das heißt die Determinante der Einheitsmatrix I ist gleich 1

$$\det I = 1.$$

(ii) Die Regeln (M) und (A) gelten analog bzgl. der Zeilen.

(iii) Erfüllt eine Abbildung

$$\vartheta : \begin{cases} \mathbb{K}^{n \times n} & \to \mathbb{K} \\ A & \mapsto \vartheta(A) \end{cases}$$

die Eigenschaften (M), (A) und (N), so ist sie gleich der Determinante:

$$\vartheta(A) = \det A.$$

9.2.2 Beweis

Eine Multiplikation über alle Indices $j \in \{1, \dots, n\}$ außer $j = \ell$ schreiben wir mit dem Zeichen $\prod_{j\neq\ell}$.

(M) Die Behauptungen werden mit der „spaltenweisen Leibnizformel" 9.1.4 einfach nachgerechnet:

$$\begin{aligned}
& \det\begin{pmatrix} a_1 & \cdots & a_{\ell-1} & a_\ell + \widetilde{a}_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \\
= {} & \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot(a_{\pi(\ell),\ell} + \widetilde{a}_{\pi(\ell),\ell})\cdot\prod_{j\neq\ell} a_{\pi(j),j} \\
= {} & \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot a_{\pi(\ell),\ell}\cdot\prod_{j\neq\ell} a_{\pi(j),j} + \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot \widetilde{a}_{\pi(\ell),\ell}\cdot\prod_{j\neq\ell} a_{\pi(j),j} \\
= {} & \det\begin{pmatrix} a_1 & \cdots & a_{\ell-1} & a_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \\
& \qquad + \det\begin{pmatrix} a_1 & \cdots & a_{\ell-1} & \widetilde{a}_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
& \det\begin{pmatrix} a_1 & \cdots & a_{\ell-1} & \alpha\cdot a_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix} \\
= {} & \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot\alpha\cdot a_{\pi(\ell),\ell}\cdot\prod_{j\neq\ell} a_{\pi(j),j} \\
= {} & \alpha\cdot\sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot a_{\pi(\ell),\ell}\cdot\prod_{j\neq\ell} a_{\pi(j),j} \\
= {} & \alpha\cdot\det\begin{pmatrix} a_1 & \cdots & a_{\ell-1} & a_\ell & a_{\ell+1} & \cdots & a_n \end{pmatrix}.
\end{aligned}$$

(A) Es sei $\vartheta = (m\,\ell) \in \mathcal{S}_n$ eine Transposition und $\widetilde{A}$ die durch Vertauschung von m-ter und ℓ-ter Spalte aus A hervorgehende Matrix, ihre Einträge sind

$$\widetilde{a}_{jk} \;=\; a_{j,\vartheta(k)}.$$

Dann gilt

$$\begin{aligned}
\det\widetilde{A} &= \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot\prod_{j=1}^{n} \widetilde{a}_{j,\pi(j)} = \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot\prod_{j=1}^{n} a_{j,\vartheta(\pi(j))} \\
&= \underbrace{\sum_{\pi\in\mathcal{S}_n} (-\sigma(\vartheta\circ\pi))\cdot\prod_{j=1}^{n} a_{j,\vartheta\circ\pi(j)}}_{\text{(Die Summe über alle } \vartheta\circ\pi \text{ ist gleich der Summe über alle } \pi)} \\
&= -\sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot\prod_{j=1}^{n} a_{j,\pi(j)} \;=\; -\det A.
\end{aligned}$$

(N) Es gibt nur eine Permutation, nämlich die identische, bei der das zugehörige Produkt der Matrix-Einträge ungleich Null ist. Dies ist

$$a_{11}\cdot a_{22}\cdot\ldots\cdot a_{nn} \;=\; 1,$$

alle anderen Produkte enthalten mindestens einen Eintrag a_{jk} mit $j \neq k$, also $a_{jk} = 0$. Das bedeutet aber:

$$\det A \;=\; \sum_{\pi\in\mathcal{S}_n} \sigma(\pi)\cdot\prod_{j=1}^{n} a_{j,\pi(j)} \;=\; \sum_{\pi=(1)} \sigma(\pi)\cdot\prod_{j=1}^{n} a_{j,\pi(j)} \;=\; 1.$$

(ii) Der Beweis erfolgt genau analog zu dem von (i). Man verwendet jeweils die zeilenweise Leibniz–Formel 9.1.3 anstelle der spaltenweisen Leibniz-Formel 9.1.4.

(iii) Wir können jeden einzelnen Spaltenvektor a_k von A als Linearkombination der Einheitsvektoren e_j darstellen. Es gilt

$$a_1 \;=\; \sum_{j=1}^{n} a_{j1} e_j, \quad a_2 \;=\; \sum_{j=1}^{n} a_{j2} e_j, \quad \ldots \quad a_n \;=\; \sum_{j=1}^{n} a_{jn} e_j.$$

Da bei den Umformungen weiter unten alle diese Linearkombinationen simultan verwendet werden sollen, ist es notwendig, n verschiedene Summationsindizes $j_1, \ldots, j_n$ zu verwenden, also die Linearkombinationen zu schreiben als

$$a_1 \;=\; \sum_{j_1=1}^{n} a_{j_1 1} e_{j_1}, \quad a_2 = \sum_{j_2=1}^{n} a_{j_2 2} e_{j_2}, \quad \ldots \quad a_n = \sum_{j_n=1}^{n} a_{j_n n} e_{j_n}.$$

Nur unter Verwendung der Aussagen (M), (A) und (N) für ϑ rechnen wir schrittweise aus

$$\begin{aligned}
\vartheta(A) &= \vartheta(a_1, a_2, \ldots, a_n) \\
& \quad \text{(Entwicklung der Vektoren } a_1, \ldots, a_n \text{ nach den kanonischen Einheitsvektoren)} \\
&= \vartheta\Big(\sum_{j_1=1}^{n} a_{j_1,1}\, e_{j_1}, \sum_{j_2=1}^{n} a_{j_2,2}\, e_{j_2}, \ldots, \sum_{j_n=1}^{n} a_{j_n,n}\, e_{j_n}\Big) \\
& \quad \text{(Linearität von } \vartheta \text{ in der 1. Spalte)} \\
&= \sum_{j_1=1}^{n} a_{j_1,1} \cdot \vartheta\Big(e_{j_1}, \sum_{j_2=1}^{n} a_{j_2,2}\, e_{j_2}, \ldots, \sum_{j_n=1}^{n} a_{j_n,n}\, e_{j_n}\Big) \\
& \quad \text{(Linearität von } \vartheta \text{ in den Spalten } 2, \ldots, n) \\
&= \sum_{j_1=1}^{n} a_{j_1,1} \sum_{j_2=1}^{n} a_{j_2,2} \ldots \sum_{j_1=1}^{n} a_{j_n,n}\, \vartheta(e_{j_1}, e_{j_2}, \ldots, e_{j_n}) \\
& \quad \text{(Die } n \text{ Summationen werden zu einer einzigen Summation zusammengefasst)} \\
&= \sum_{(j_1,\ldots,j_n)\in\{1,\ldots,n\}^n} a_{j_1,1} \cdot a_{j_2,2} \cdot \ldots \cdot a_{j_n,n} \cdot \vartheta(e_{j_1}, e_{j_2}, \ldots, e_{j_n}) \\
& \quad \text{(Die Summanden mit } j_s = j_t \text{ für } s \neq t \text{ sind Null, da dann die Matrix rechts zwei gleiche Spalten enthält)} \\
&= \sum_{\substack{(j_1,\ldots,j_n)\in\{1,\ldots,n\}^n \\ j_s \neq j_t \text{ für } s\neq t}} a_{j_1,1} \cdot a_{j_2,2} \cdot \ldots \cdot a_{j_n,n} \cdot \vartheta(e_{j_1}, e_{j_2}, \ldots, e_{j_n}) \\
& \quad \text{(Umbenennung } \pi(i) = j_i \text{ definiert eine Permutation } \pi) \\
&= \sum_{\pi\in\mathcal{S}_n} a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \cdot \vartheta(e_{\pi(1)}, e_{\pi(2)}, \ldots, e_{\pi(n)}) \\
& \quad \text{(Umsortierung der Spalten } e_k \text{ führt zu einem Vorzeichen } \sigma(\pi) \text{ der Determinante)} \\
&= \sum_{\pi\in\mathcal{S}_n} a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \cdot \sigma(\pi) \cdot \vartheta(I) \\
& \quad \text{(Normierung: } \vartheta(I) = 1) \\
&= \sum_{\pi\in\mathcal{S}_n} \sigma(\pi) \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \\
& \quad \text{(Leibniz-Formel spaltenweise 9.1.4)} \\
&= \det A.
\end{aligned}$$

9.2.3 Satz: Weitere Eigenschaften der Determinante

Es sei $A \in \mathbb{K}^{n \times n}$. Die Determinantenfunktion hat die folgenden weiteren Eigenschaften:

(i) Für jedes $\alpha \in \mathbb{K}$ gilt

$$\det(\alpha \cdot A) = \alpha^n \cdot \det A.$$

(ii) Ist eine Zeile oder Spalte von A gleich Null, so gilt

$$\det A = 0.$$

(iii) Hat A zwei gleiche Zeilen oder zwei gleiche Spalten, so gilt

$$\det A = 0.$$

(iv) Entsteht die Matrix $\widetilde{A}$ aus der Matrix A dadurch, dass eine Zeile (Spalte) von A zu einer anderen Zeile (Spalte) von A addiert wird, so gilt

$$\det \widetilde{A} = \det A.$$

(v) Es gilt

$$\det A^T = \det A.$$

(vi) Die Gleichung

$$\det(A + B) \stackrel{\leadsto}{=} \det A + \det B$$

für zwei $n \times n$–Matrizen A, B ist im allgemeinen nicht richtig.

9.2.4 Beweis

Die Aussagen (i) und (ii) folgen sofort aus der Aussage (i) des Satzes 9.2.1.

Die Aussage (iii) ist eine Konsequenz von Aussage (ii) dieses Satzes.

Die Aussage (iv) folgt aus (iv) in Satz 9.2.1 und (iii) des aktuellen Satzes.

(v) folgt sofort aus den beiden Formeln in 9.1.3 und 9.1.4.

(vi) Wähle als Gegenbeispiel $A = B = I$ mit $n \geq 2$.

9.3 Der Determinantenmultiplikationssatz

9.3.1 Satz: Multiplikation von Determinanten

Es seien A, B zwei $n \times n$–Matrizen. Dann gilt

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

9.3.2 Beweis

Wir fassen die Matrix B als gegebenes Objekt auf, das durch die Matrix A als Operator von links verändert wird. Es ist

$$\begin{aligned}
\det(A \cdot B) &= \det(A\,b_1, A\,b_2, \ldots, A\,b_n) \\
&\quad \text{(Entwicklung der Vektoren } b_1, \ldots, b_n \text{ nach den kanonischen Einheitsvektoren)} \\
&= \det(A \sum_{j_1=1}^{n} b_{j_1,1} e_{j_1}, A \sum_{j_2=1}^{n} b_{j_2,2} e_{j_2}, \ldots, A \sum_{j_n=1}^{n} b_{j_n,n} e_{j_n}) \\
&\quad \text{(Die Multiplikation mit } A \text{ von links ist linear)} \\
&= \det(\sum_{j_1=1}^{n} b_{j_1,1} A\,e_{j_1}, \sum_{j_2=1}^{n} b_{j_2,2} A\,e_{j_2}, \ldots, \sum_{j_n=1}^{n} b_{j_n,n} A\,e_{j_n}) \\
&\quad \text{(Linearität von det in der 1. Spalte)} \\
&= \sum_{j_1=1}^{n} b_{j_1,1} \cdot \det(A\,e_{j_1}, \sum_{j_2=1}^{n} b_{j_2,2} A\,e_{j_2}, \ldots, \sum_{j_n=1}^{n} b_{j_n,n} A\,e_{j_n}) \\
&\quad \text{(Linearität von det in den Spalten } 2, \ldots, n) \\
&= \sum_{j_1=1}^{n} b_{j_1,1} \sum_{j_2=1}^{n} b_{j_2,2} \ldots \sum_{j_1=1}^{n} b_{j_n,n} \det(A\,e_{j_1}, A\,e_{j_2}, \ldots, A\,e_{j_n}) \\
&\quad \text{(Die } n \text{ Summationen werden zu einer einzigen Summation zusammengefasst)} \\
&= \sum_{(j_1,\ldots,j_n) \in \{1,\ldots,n\}^n} b_{j_1,1} \cdot b_{j_2,2} \cdot \ldots \cdot b_{j_n,n} \cdot \det(A\,e_{j_1}, A\,e_{j_2}, \ldots, A\,e_{j_n}) \\
&\quad \text{(Die Summanden mit } j_s = j_t \text{ für } s \neq t \text{ sind Null, da dann die Matrix rechts zwei gleiche Spalten enthält)} \\
&= \sum_{\substack{(j_1,\ldots,j_n) \in \{1,\ldots,n\}^n \\ j_s \neq j_t \text{ für } s \neq t}} b_{j_1,1} \cdot b_{j_2,2} \cdot \ldots \cdot b_{j_n,n} \cdot \det(A\,e_{j_1}, A\,e_{j_2}, \ldots, A\,e_{j_n}) \\
&\quad \text{(Umbenennung } \pi(i) = j_i \text{ definiert eine Permutation } \pi) \\
&= \sum_{\pi \in \mathcal{S}_n} b_{\pi(1),1} \cdot b_{\pi(2),2} \cdot \ldots \cdot b_{\pi(n),n} \cdot \det(A\,e_{\pi(1)}, A\,e_{\pi(2)}, \ldots, A\,e_{\pi(n)}) \\
&\quad \text{(Umsortierung der Spalten } Ae_k \text{ führt zu einem Vorzeichen } \sigma(\pi) \text{ der Determinante)} \\
&= \sum_{\pi \in \mathcal{S}_n} b_{\pi(1),1} \cdot b_{\pi(2),2} \cdot \ldots \cdot b_{\pi(n),n} \cdot \sigma(\pi) \cdot \det A \\
&\quad \text{(Ausklammern von } \det A) \\
&= \det A \cdot \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot b_{\pi(1),1} \cdot b_{\pi(2),2} \cdot \ldots \cdot b_{\pi(n),n} \\
&\quad \text{(Leibniz-Formel spaltenweise 9.1.4)} \\
&= \det A \cdot \det B.
\end{aligned}$$

9.3.3 Beispiel: Produkt zweier 2×2–Matrizen

$$\begin{pmatrix} 2 & -3 \\ 1 & 6 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -3 & 12 \\ 6 & -9 \end{pmatrix}$$

Entsprechend gilt für die Determinanten:

$$15 \cdot (-3) = -45.$$

9.3.4 Beispiel: Produkt zweier 3×3–Matrizen

$$\begin{pmatrix} 1 & 3 & -2 \\ 5 & -1 & -4 \\ 2 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 4 & -3 & 0 \\ 0 & 1 & -5 \\ 3 & 2 & -6 \end{pmatrix} = \begin{pmatrix} -2 & -4 & -3 \\ 8 & -24 & 29 \\ 23 & 4 & -30 \end{pmatrix}$$

Die drei Determinanten haben die Werte

$$-5 - 24 - 4 - 75 = -108$$
$$-24 + 45 + 40 = 61$$
$$-1440 - 2668 - 96 - 1656 + 232 - 960 = -6588$$

9.4 Die Entwicklung einer Determinante

9.4.1 Definition Streichungsmatrix

Es seien die quadratische Matrix $A \in \mathbb{K}^{n\times n}$ und zwei Zahlen $m, \ell \in \{1, \dots, n\}$ gegeben.

Die *Streichungsmatrix* $A^{(m\ell)} \in \mathbb{K}^{(n-1)\times(n-1)}$ entsteht aus A dadurch, dass die m-te Zeile und ℓ-te Spalte gestrichen werden.

9.4.2 Satz: Entwicklung einer Determinante

(i) Für eine Zeilennummer m gilt:

$$\det A \;=\; \sum_{k=1}^{n} a_{mk} \cdot (-1)^{m+k} \det A^{(mk)}.$$

(ii) Für eine Spaltennummer ℓ gilt:

$$\det A \;=\; \sum_{j=1}^{n} a_{j\ell} \cdot (-1)^{j+\ell} \det A^{(j\ell)}.$$

9.4.3 Beispiele

Wir entwickeln die Determinante einer 4×4–Matrix. Dabei benutzen wir eine vereinfachende Schreibweise für Determinanten.

Entwicklung nach der zweiten Spalte:

$$\begin{aligned}
\begin{vmatrix} 0 & 2 & 3 & 0 \\ 2 & -1 & 0 & -2 \\ 4 & 0 & 0 & -3 \\ 1 & 1 & 2 & 0 \end{vmatrix}
&= -2 \cdot \begin{vmatrix} 2 & 0 & -2 \\ 4 & 0 & -3 \\ 1 & 2 & 0 \end{vmatrix} - \begin{vmatrix} 0 & 3 & 0 \\ 4 & 0 & -3 \\ 1 & 2 & 0 \end{vmatrix} + \begin{vmatrix} 0 & 3 & 0 \\ 2 & 0 & -2 \\ 4 & 0 & -3 \end{vmatrix} \\
&= (-2)\cdot(-2) \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} - (-3) \cdot \begin{vmatrix} 4 & -3 \\ 1 & 0 \end{vmatrix} + (-3) \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} \\
&= 8 + 9 - 6 \;=\; 11.
\end{aligned}$$

Entwicklung nach der ersten Zeile:

$$\begin{aligned}
\begin{vmatrix} 0 & 2 & 3 & 0 \\ 2 & -1 & 0 & -2 \\ 4 & 0 & 0 & -3 \\ 1 & 1 & 2 & 0 \end{vmatrix}
&= -2 \cdot \begin{vmatrix} 2 & 0 & -2 \\ 4 & 0 & -3 \\ 1 & 2 & 0 \end{vmatrix} + 3 \cdot \begin{vmatrix} 2 & -1 & -2 \\ 4 & 0 & -3 \\ 1 & 1 & 0 \end{vmatrix} \\
&= (-2)\cdot(-2) \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} + 3 \cdot \left[1 \cdot \begin{vmatrix} -1 & -2 \\ 0 & -3 \end{vmatrix} - 1 \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} \right] \\
&= 8 + 3 \cdot [3 - 2] \;=\; 11.
\end{aligned}$$

9.4.4 Beweis

Wir zeigen die Aussage (i) für $m = n$. Die allgemeine Aussage folgt dann mit Satz 9.2.1 (ii).

$$\begin{aligned}
\det A &= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{j,\pi(j)} = \sum_{k=1}^{n} \sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{j,\pi(j)} \\
&= \sum_{k=1}^{n} \sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot a_{nk} \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)} \\
&= \sum_{k=1}^{n} a_{nk} \cdot \sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)}
\end{aligned}$$

Es bleibt zu zeigen, dass

$$\sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)} \;=\; (-1)^{n+k} \cdot \det A^{(nk)}.$$

Dazu sei ϑ die Permutation, die die Spaltennummer k an die letzte Stelle mit Spaltennummer n „verschiebt":

$$\begin{aligned}
\vartheta \;&:=\; \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n \\ 1 & 2 & \cdots & k-1 & n & k & \cdots & n-1 \end{pmatrix} \\
&= \begin{pmatrix} n & n-1 \end{pmatrix} \ldots \begin{pmatrix} k+2 & k+1 \end{pmatrix} \begin{pmatrix} k+1 & k \end{pmatrix},
\end{aligned}$$

Es ist dann

$$\sigma(\vartheta) \;=\; (-1)^{n-k} \;=\; (-1)^{n-k} \cdot (-1)^{2k} \;=\; (-1)^{n+k}.$$

Dann sind die Einträge von $A^{(nk)}$ gegeben durch

$$a_{j\ell}^{(nk)} \;=\; a_{j,\vartheta^{-1}(\ell)}, \qquad 1 \le j, \ell \le n-1.$$

Es gilt dann:

$$\begin{aligned}
&\sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)} \;= \qquad\qquad \text{(Transformation } \pi = \vartheta^{-1}\widetilde{\pi}\text{)} \\
&\sum_{\widetilde{\pi} \in \mathcal{S}_n, \vartheta^{-1}\widetilde{\pi}(n)=k} \sigma(\vartheta^{-1}\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\vartheta^{-1}\widetilde{\pi}(j)} \;= \\
&(-1)^{n+k} \cdot \sum_{\widetilde{\pi} \in \mathcal{S}_n, \widetilde{\pi}(n)=n} \sigma(\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\vartheta^{-1}\widetilde{\pi}(j)} \;= \\
&(-1)^{n+k} \cdot \sum_{\widetilde{\pi} \in \mathcal{S}_n, \widetilde{\pi}(n)=n} \sigma(\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\widetilde{\pi}(j)}^{(nk)} \;= \\
&(-1)^{n+k} \cdot \sum_{\widetilde{\pi} \in \mathcal{S}_{n-1}} \sigma(\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\widetilde{\pi}(j)}^{(nk)} \;= \\
&(-1)^{n+k} \cdot \det A^{(nk)}.
\end{aligned}$$

9.5 Die Kofaktor-Matrix

9.5.1 Definition Kofaktor-Matrix

Zu einer gegebenen quadratischen Matrix A sei die Matrix $A^\diamond$ definiert durch die Einträge

$$a^\diamond_{jk} = (-1)^{j+k} \det A^{(jk)}.$$

Ausgeschrieben ergibt sich die Matrix mit einer Vorzeichen–Schachbrettverteilung:

$$A^\diamond = \begin{pmatrix} +\det A^{(11)} & -\det A^{(12)} & \cdots & \cdots & (-1)^{1+n}\det A^{(1n)} \\ -\det A^{(12)} & +\det A^{(22)} & \cdots & \cdots & (-1)^{2+n}\det A^{(2n)} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ (-1)^{n+1}\det A^{(n1)} & (-1)^{n+2}\det A^{(n2)} & \cdots & \cdots & +\det A^{(nn)} \end{pmatrix}$$

9.5.2 Satz über die Kofaktor-Matrix

Für das Produkt der Matrizen A und $A^{\diamond T}$ gilt

$$A \cdot A^{\diamond T} = A^{\diamond T} \cdot A = \det A \cdot I = \begin{pmatrix} \det A & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \det A & \ddots & & & \vdots \\ \vdots & \ddots & \det A & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & \det A \end{pmatrix}.$$

9.5.3 Beweis

Wir rechnen einfach den Eintrag an der Stelle (jk) aus:

$$(A \cdot A^{\diamond T})_{jk} = \sum_{i=1}^{n} (A)_{ji}(A^{\diamond T})_{ik} = \sum_{i=1}^{n} a_{ji} \cdot (-1)^{k+i} \det A^{(ki)}$$

(Entwicklung der folgenden Determinante nach der k–ten Zeile)

$$= \det \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & & \vdots \\ a_{k-1,1} & \cdots & \cdots & a_{k-1,n} \\ a_{j1} & \cdots & \cdots & a_{jn} \\ a_{k+1,1} & \cdots & \cdots & a_{k+1,n} \\ \vdots & & & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \longleftarrow k\text{–te Zeile}$$

$$= \begin{cases} \det A, & \text{falls } j = k, \\ 0, & \text{falls } j \neq k. \end{cases}$$

Die Matrix in der vorletzten Zeile entsteht aus der Matrix A dadurch, dass die k-te Zeile von A durch die j-te Zeile von A ersetzt ist.

Für $j = k$ ist diese Matrix gleich der Matrix A.

Für $j \neq k$ sind in dieser Matrix die Zeilen j und k gleich. Deshalb ist die Determinante Null, vgl. Satz 9.2.3(iii).

Die andere Eigenschaft $A^{\diamond T} \cdot A = \det A \cdot I$ folgt mit einer dualen Betrachtung, d.h. einer Spaltenentwicklung.

10 Matrixgruppen

10.1 Reguläre Matrizen

10.1.1 Satz und Definition: Reguläre Matrizen

Für eine quadratische Matrix $A \in \mathbb{K}^{n \times n}$ bzw. die zugehörige lineare Abbildung $\ell_A : \mathbb{K}^n \to \mathbb{K}^n$ sind die folgenden Aussagen äquivalent:

(A) Die Matrix heißt *regulär*.

(B) A ist (multiplikativ) invertierbar, d.h. es existiert eine Matrix A^{-1} mit

$$A \cdot A^{-1} \;=\; I \qquad \text{und} \qquad A^{-1} \cdot A \;=\; I.$$

(C) Die zugehörige lineare Abbildung ℓ_A ist bijektiv.

(D) Die zugehörige lineare Abbildung ℓ_A ist injektiv.

(E) Die zugehörige lineare Abbildung ℓ_A ist surjektiv.

(F) Der Rang von A ist gleich n.

(G) Für beliebiges $b \in \mathbb{K}^n$ ist das LGS $A \cdot x = b$ eindeutig lösbar.

(H) Die Matrix A lässt sich durch elementare Zeilenumformungen in die Einheitsmatrix I überführen.

(J) Die Determinante von A ist ungleich Null.

Eine Matrix, die nicht regulär ist, heißt auch *singulär*.

10.1.2 Beweis

(1) Die Äquivalenz $(B) \Leftrightarrow (C)$ ist offensichtlich. Man erinnere sich an Satz 1.7.14.

(2) Für den Rang einer Matrix A gilt nach Satz und Definition 7.6.1:

$$\operatorname{rang} A \;=\; \dim(\operatorname{im} A) \;=\; n - \dim(\ker A)$$

Daraus folgt direkt die Äquivalenz $(D) \Leftrightarrow (E) \Leftrightarrow (F) \Leftrightarrow$ und damit auch die zu (C).

(3) Die Äquivalenz $(B) \Leftrightarrow (G)$ ist ebenfalls direkt einsehbar.

$(F) \Rightarrow (H)$: Gemäß Satz 2.3.2 (i) kann die Matrix A durch elementare Zeilenumformungen in eine Matrix $\widetilde{A}$ überführt werden, so dass

die Matrix $\widetilde{A}$ eine obere Dreiecksmatrix ist,

die Diagonaleinträge $\widetilde{a}_{jj}$ gleich Null oder Eins sind,

falls ein Diagonaleintrag $\widetilde{a}_{jj} = 1$ ist, auch alle Einträge oberhalb dieses Eintrags gleich Null sind.

Wir wissen aus Satz 7.6.3(ii) dass bei diesen elementaren Zeilenumformungen der Rang gleich bleibt, also

$$\operatorname{rang} \widetilde{A} \;=\; n.$$

Eine quadratische obere Dreiecksmatrix kann aber nur dann Vollrang n haben, wenn alle Diagonalelemente ungleich Null sind. Man kann also die Einheitsmatrix erreichen.

$(H) \Rightarrow (F)$: Gemäß (D) lässt sich die erweiterte Matrix $(A|b)$ durch elementare Zeilen-Äquivalenzumformungen in die erweiterte Matrix $(I|\widetilde{b})$ überführen. $\widetilde{b}$ ist dann die einzige Lösung des zugehörigen LGS $I \cdot x = \widetilde{b}$ und damit die einzige Lösung des ursprünglichen LGS.

$(G) \Rightarrow (C)$ ist direkt einsehbar.

$(B) \Rightarrow (J)$: Wenn A invertierbar ist, so gilt

$$\det A \cdot \det(A^{-1}) \;=\; \det(A \cdot A^{-1}) \;=\; \det I \;=\; 1,$$

also muss $\det A \neq 0$ sein.
$(J) \Rightarrow (B)$: Gemäß Satz 9.5.2 gilt für die Kofaktor-Matrix

$$A^{\diamond T} \cdot A \;=\; \det A \cdot I.$$

Setzt man also

$$A^{-1} \;=\; \frac{1}{\det A} \cdot A^{\diamond T},$$

so haben wir die inverse Matrix gefunden.

Im Beweis sind — mehr oder weniger versteckt — einige Berechnungsmethoden aufgetreten, die wir noch einmal eigens beschreiben wollen.

10.2 Berechnung von inversen Matrizen

10.2.1 Satz: Inverse Matrix mittels Determinante

Die Inverse einer regulären Matrix A ist gegeben durch

$$\begin{aligned} A^{-1} &= \frac{1}{\det A} \cdot A^{\diamond T} \\ &= \frac{1}{\det A} \cdot \begin{pmatrix} +\det A^{(11)} & -\det A^{(21)} & \cdots & \cdots & (-1)^{n+1}\det A^{(n1)} \\ -\det A^{(21)} & +\det A^{(22)} & \cdots & \cdots & (-1)^{n+2}\det A^{(n2)} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ (-1)^{1+n}\det A^{(1n)} & (-1)^{2+n}\det A^{(2n)} & \cdots & \cdots & +\det A^{(nn)} \end{pmatrix} \end{aligned}$$

Der Eintrag an der Position (j,k) der inversen Matrix ist

$$(A^{-1})_{jk} = (-1)^{j+k} \cdot \frac{\det A^{(kj)}}{\det A}.$$

Beachte die Vertauschung $(jk) \to (kj)$ in dieser Formel.

10.2.2 Die Cramer'sche Regel

Ist die Matrix $A \in \mathbb{K}^{n\times n}$ in dem LGS

$$A\,x = b$$

regulär, so ist die eindeutige Lösung x gegeben durch

$$x_j = \frac{1}{\det A} \cdot \det \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix}, \qquad j = 1,\ldots,n.$$

10.2.3 Beweis Der Beweis besteht im Nachrechnen:

$$\frac{1}{\det A} \cdot \det \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix} =$$

(Entwicklung nach der j–ten Spalte)

$$\frac{1}{\det A} \cdot \sum_{i=1}^n b_i \cdot (-1)^{i+j} \det A^{(ij)} =$$

$$\frac{1}{\det A} \cdot \sum_{i=1}^n (A^{\diamond T})_{ji}\, b_i = \frac{1}{\det A} \cdot (A^{\diamond T} b)_j = (A^{-1}\, b)_j = x_j.$$

10.2.4 Satz: Inverse Matrix mittels Gauß-Jordan-Algorithmus

(i) Ist die Matrix $A \in \mathbb{K}^{n\times n}$ regulär, so lässt sich in $\mathbb{K}^{n\times 2n}$ durch elementare Zeilenumformungen die Transformation

$$(A|I) \quad \longrightarrow \quad (I|A^{-1})$$

durchführen.

(ii) Die Zeilenumformungen entsprechen der Multiplikation mit A^{-1} von links.

(iii) Jede reguläre Matrix lässt sich als (endliches) Produkt von Matrizen

$$T_{jk}, Q_{j,\alpha}, R_{jk} \qquad \text{oder sogar nur von} \qquad Q_{j,\alpha}, R_{jk}$$

(vgl. Abschnitt 2.2.2) darstellen.

10.2.5 Beweis

(1) Betrachte dazu das LGS mit n^2 in der Matrix X zusammengefassten unbekannten Zahlen:

$$A \cdot X \;=\; I$$

(2) Gemäß Satz 10.1.1 (H) kann die Matrix A durch eine Abfolge geeigneter Zeilenumformungen in die Einheitsmatrix überführt werden.

(3) Diese Abfolge von Zeilenumformungen entspricht der Multiplikation von A mit einer Matrix T von links. Multiplizieren wir das LGS mit T von links, so stellt sich heraus:

$$T \cdot A \cdot X \;=\; T$$

Wegen $T \cdot A = I$ bedeutet dies aber $X = T = A^{-1}$.

(4) Das bedeutet aber, dass sich die rechte Seite I in der erweiterten Matrix $(A|I)$ durch Multiplikation mit T, das heißt durch die durchgeführten Zeilenumformungen in die Matrix A^{-1} verwandelt hat.

(5) Zunächst ist, wie gerade bemerkt, $A = T^{-1}$ eine Abfolge von Zeilenumformungen und deshalb ein Produkt von Matrizen $T_{jk}, Q_{j,\alpha}, R_{jk}$.

Bezeichnen wir die Vektoren der j-ten bzw. k-ten Zeile in A mit b bzw. c, so wirken sich die Linksmultiplikationen mit den angegebenen Matrizen wie folgt aus:

$$\begin{pmatrix} * \\ b \\ * \\ c \\ * \end{pmatrix} \xrightarrow{R_{kj}} \begin{pmatrix} * \\ b \\ * \\ c+b \\ * \end{pmatrix} \xrightarrow{Q_{k,-1}} \begin{pmatrix} * \\ b \\ * \\ -c-b \\ * \end{pmatrix} \xrightarrow{R_{jk}} \begin{pmatrix} * \\ -c \\ * \\ -c-b \\ * \end{pmatrix} \xrightarrow{Q_{j,-1}} \begin{pmatrix} * \\ c \\ * \\ -c-b \\ * \end{pmatrix} \xrightarrow{R_{kj}} \begin{pmatrix} * \\ c \\ * \\ -b \\ * \end{pmatrix} \xrightarrow{Q_{k,-1}} \begin{pmatrix} * \\ c \\ * \\ b \\ * \end{pmatrix}$$

Insgesamt wurden also die j-te und k-te Zeile getauscht. Es ist

$$T_{jk} \;=\; Q_{k,-1} \cdot R_{kj} \cdot Q_{j,-1} \cdot R_{jk} \cdot Q_{k,-1} \cdot R_{kj}.$$

10.2.6 Beispiel: Berechnung der Inversen mittels Determinante

Als Beispiel betrachten wir die Matrix

$$A = \begin{pmatrix} 5 & 2 & -1 \\ 0 & 1 & -4 \\ -3 & 4 & 2 \end{pmatrix}$$

Ihre Determinante ist gemäß Regel von Sarrus

$$\det A = 10 + 24 + 0 - 3 + 80 - 0 = 111.$$

Die Matrizen $A^\diamond$, $A^{\diamond T}$ und A^{-1} sind dann

$$A^\diamond = \begin{pmatrix} 18 & 12 & 3 \\ -8 & 7 & -26 \\ -7 & 20 & 5 \end{pmatrix}, \quad A^{\diamond T} = \begin{pmatrix} 18 & -8 & -7 \\ 12 & 7 & 20 \\ 3 & -26 & 5 \end{pmatrix},$$

$$A^{-1} = \begin{pmatrix} \frac{18}{111} & -\frac{8}{111} & -\frac{7}{111} \\ \frac{12}{111} & \frac{7}{111} & \frac{20}{111} \\ \frac{3}{111} & -\frac{26}{111} & \frac{5}{111} \end{pmatrix}.$$

Es empfiehlt sich, diese drei Schritte trotz erhöhten Schreibaufwands tatsächlich durchzuführen. Eine Abkürzung ist mit deutlich erhöhter Fehlergefahr verbunden.

10.2.7 Beispiel: Berechnung der Inversen mittels Gauß-Jordan-Algorithmus

$$
\begin{array}{rrr|rrr||r}
5 & 2 & -1 & 1 & 0 & 0 & \\
0 & 1 & -4 & 0 & 1 & 0 & \\
-3 & 4 & 2 & 0 & 0 & 1 & +\frac{3}{5}\ \mathrm{I} \\
\hline
5 & 2 & -1 & 1 & 0 & 0 & \\
0 & 1 & -4 & 0 & 1 & 0 & \\
0 & \frac{26}{5} & \frac{7}{5} & \frac{3}{5} & 0 & 1 & 5\,\cdot \\
\hline
5 & 2 & -1 & 1 & 0 & 0 & \\
0 & 1 & -4 & 0 & 1 & 0 & \\
0 & 26 & 7 & 3 & 0 & 5 & -26\ \mathrm{II} \\
\hline
5 & 2 & -1 & 1 & 0 & 0 & \\
0 & 1 & -4 & 0 & 1 & 0 & \\
0 & 0 & 111 & 3 & -26 & 5 & \frac{1}{111}\,\cdot \\
\hline
5 & 2 & -1 & 1 & 0 & 0 & +\ \mathrm{III} \\
0 & 1 & -4 & 0 & 1 & 0 & +4\ \mathrm{II} \\
0 & 0 & 1 & \frac{3}{111} & -\frac{26}{111} & \frac{5}{111} & \\
\hline
5 & 2 & 0 & \frac{114}{111} & -\frac{26}{111} & \frac{5}{111} & -2\ \mathrm{II} \\
0 & 1 & 0 & \frac{12}{111} & \frac{7}{111} & \frac{20}{111} & \\
0 & 0 & 1 & \frac{3}{111} & -\frac{26}{111} & \frac{5}{111} & \\
\hline
5 & 0 & 0 & \frac{90}{111} & -\frac{40}{111} & -\frac{35}{111} & \frac{1}{5}\,\cdot \\
0 & 1 & 0 & \frac{12}{111} & \frac{7}{111} & \frac{20}{111} & \\
0 & 0 & 1 & \frac{3}{111} & -\frac{26}{111} & \frac{5}{111} & \\
\hline
1 & 0 & 0 & \frac{18}{111} & -\frac{8}{111} & -\frac{7}{111} & \\
0 & 1 & 0 & \frac{12}{111} & \frac{7}{111} & \frac{20}{111} & \\
0 & 0 & 1 & \frac{3}{111} & -\frac{26}{111} & \frac{5}{111} & \\
\hline
\end{array}
$$