Skript zu den Vorlesungen Lineare Algebra I und II am KIT im Wintersemester 2023/24 und Sommersemester 2024

Tobias Hartnick

30. August 2024

Danksagung. Dieses Skript entsteht parallel zu den Vorlesungen im Wintersemester 2023/24 und Sommersemester 2024. Es basiert auf meinem älteren Skript aus dem Wintersemester 2020/21, das sich wiederum an meiner Ausarbeitung zu einer Vorlesung an der Justus-Liebig-Universität Gießen im Wintersemester 2018/19 orientiert. In der Erstellung dieser Ausarbeitungen habe ich von älteren Skripten von PROF. DR. JOACHIM HILGERT, PROF. DR. RALF KÖHL, PROF. DR. BERNHARD MÜHLHERR, DR. RAFAEL DAHMEN und PD DR. STEFAN KÜHNLEIN profitiert. Ich danke den genannten Kollegen für das bereitwillige Teilen ihrer Skripte.

Am meisten zu Dank verpflichtet bin ich den Hörerinnen und Hörern meiner Gießener und Karlsruher Vorlesungen für ihre (meist) konstruktive Kritik und den an den Vorlesungen beteiligten Mitarbeitern ALEXANDER BLATZ, LLUIS USO I CUBERTORER, JASPER GRÄFLICH, MAXIMILIAN WACKENHUTH, DR. MARTIN GÜNTHER, DR. ELISA HARTMANN, DR. ANNETTE KARRER und DR. FABIAN RUOFF, die mir insbesondere mit den Übungsaufgaben und einigen der Abbildungen geholfen haben.

Da das Skript neu erstellt wird, wird es sicherlich zahlreiche Fehler – Tippfehler und inhaltliche Fehler – enthalten. Ich freue mich darüber, wenn Sie mich unter `tobias.hartnick@kit.edu` auf Fehler aufmerksam machen und werde mich bemühen, diese zu korrigieren.

Für Korrekturen zum aktuellen Skript danke ich[1] ANASTASIA AUGUST, GABRIEL BAUMANN, IAGO BISCHOFF MONTENEGRO, ROUWEN BOROWSKI, DANIIL DEMIDOV, EMIL ENGLER, SIMON ENGLERT, HANNAH FUCHS, OLIVER GRÜNLING, DANIEL HAASE, LENNART FRIEBEL, LARS GROSS, MAXIMILIAN HEPPNER, MICHAEL LE, BERTHOLD NIEMANN, IMMANUEL REITZ, GABRIEL SCHIFFNER, FINN SCHNEIDER, ALEKSANDR SILKIN, CHRISTOPHER STEMANN, JANNIS WEISBRODT, MAXIMILIAN WITTMER, MOSE WOLF.

[1] Hier könnte Ihr Name stehen!

Inhaltsverzeichnis

1 Zur Sprache der Mathematik **5**
- 1.1 Elementare Aussagenlogik . . . 5
- 1.2 Naive Mengenlehre . . . 10
- 1.3 Relationen und Funktionen . . . 16
- 1.4 Partitionen und Äquivalenzrelationen . . . 22
- 1.5 Mengenvergleiche* . . . 27

2 Von linearen Gleichungssystemen zu abstrakten Vektorräumen **31**
- 2.1 Motivation: Lineare Gleichungssysteme in zwei Veränderlichen . . . 31
- 2.2 Abstrakte Vektorräume . . . 49
- 2.3 Erzeugendensysteme und lineare Hüllen . . . 57
- 2.4 Basen und Koordinaten . . . 62
- 2.5 Dimension endlichdimensionaler Vektorräume . . . 73
- 2.6 Affine Unterräume und Quotientenvektorräume . . . 78

3 Lineare Abbildungen und Matrizen **83**
- 3.1 Matrizenformalismus . . . 83
- 3.2 Kanonische Zerlegungen linearer Abbildungen . . . 93
- 3.3 Rang und Smith-Normalform . . . 96
- 3.4 Matrixalgorithmen . . . 101
- 3.5 Zerlegungen von linearen Abbildungen und Matrizen . . . 109

4 Determinanten **117**
- 4.1 Prolog: Permutationen endlicher Mengen . . . 117
- 4.2 Determinantenformen . . . 123
- 4.3 Die Determinante eines Endomorphismus . . . 133
- 4.4 Laplace-Entwicklung und die Cramersche Regel . . . 141
- 4.5 Eigenwerte und Eigenvektoren . . . 146

5 Algebraische Strukturen **157**
- 5.1 Universelle Algebra . . . 157
- 5.2 Gruppen und ihre Wirkungen . . . 160
- 5.3 Ringe und Körper . . . 174
- 5.4 Polynomringe und Algebren . . . 184

6 Normalformen von Endomorphismen **197**
- 6.1 Charakteristisches Polynom und Trigonalisierbarkeit . . . 197
- 6.2 Diagonalisierbarkeit . . . 209
- 6.3 Simultane Diagonalisierbarkeit . . . 215
- 6.4 Die Koeffizienten des charakteristischen Polynoms . . . 231
- 6.5 Normalform nilpotenter Endomorphismen . . . 238

6.6 Fitting–Zerlegung und Jordannormalform 248
6.7 Ergänzungen zur Jordan-Theorie 259

7 Sesquilinearformen **273**
7.1 Motivation: Skalarprodukte 273
7.2 Orthogonale Zerlegungen 296
7.3 Automorphismen 313
7.4 Witt-Theorie für orthogonale Vektorräume 326

8 Der Spektralsatz und seine Folgerungen **335**
8.1 Normale Endomorphismen 335
8.2 Unitäre Diagonalisierbarkeit und Spektralkalkül 341
8.3 Orthogonale Diagonalisierung und Isometrie-Normalform 353
8.4 Polar- und Singulärwertzerlegung 357

9 Affine Quadriken **371**
9.1 Quadriken und Hauptachsentransformation 371
9.2 Ebene und räumliche Quadriken 383
9.2.1 Ebene Quadriken 383
9.2.2 Räumliche Quadriken 392
9.3 Ebene Schnitte räumlicher Quadriken 396
9.4 Affine Quadriken über allgemeinen Körpern 401

10 Tensorprodukte und Tensoralgebra **409**
10.1 Tensorprodukte endlichdimensionaler Vektorräume 409
10.2 Einschub: Unendlichdimensionale Vektorräume 421
10.3 Tensoralgebren und ihre Quotientenalgebren 429

11 Die Matrizenexponentialfunktion **439**
11.1 Matrizen und Potenzreihen 439
11.2 Einparameteruntergruppen von $\mathrm{GL}_n(\mathbb{R})$ 445
11.3 Lokale Invertierbarkeit der Matrizenexponentialfunktion 451
11.4 Ausblick: Lie-Algebren 455

1 Zur Sprache der Mathematik

[25.10.23]

Vorbemerkung: Mathematik als Sprache und die Sprache der Mathematik

Die Mathematik bildet eine *Sprache*, die unsere Alltagssprache verfeinert und daher geeignet ist, Phänomene z.B. der Wissenschaften präzise zu beschreiben. Dazu bedient Sie sich selbst einer Sprache aus Formeln, Symbolen und Alltagssprache. Bevor wir beginnen können, Mathematik zu diskutieren, müssen wir die Grundzüge dieser *Metasprache* erlernen. Dies ist der Zweck dieses ersten Kapitels. Die eigentliche Lineare Algebra beginnt dann im Kapitel 2.

Warnung: Dieses Kapitel ist sehr trocken und abstrakt und hat im Grunde keinen Inhalt. Die hier eingeführte Sprache ist aber für alles weitere absolut unerlässlich.

Man kann die mathematische Metasprache sehr weit formalisieren und damit „computerlesbar“ machen. Dies ist sowohl aus philosophischer Sicht als auch für gewisse Anwendungen (vor allem in der Informatik) nützlich, aber eine extrem formale Sprache ist für die Kommunikation zwischen Menschen hinderlich und für viele Zwecke auch unnötig.

In dieser Vorlesung werden wir uns einer halb-formalen Metasprache bedienen, die neben der (deutschen) Alltagssprache auf Symbolen der *Logik* und *Mengenlehre* beruht. Es ist möglich Logik und Mengenlehre vollständig zu formalisieren und so eine saubere Grundlage der Mathematik zu schaffen, aber das werden wir an dieser Stelle[1] nicht tun. Stattdessen führen wir in diesem Kapitel eine *pragmatische mathematische Umgangssprache* ein, die das Ziel hat, so formal zu sein wie nötig, um grobe Missverständnisse zu vermeiden, aber dabei so weit wie möglich an die Alltagssprache angelehnt ist.

1.1 Elementare Aussagenlogik

Bemerkung 1.1.1 (Aussagen)**.** Unter einer *(logischen) Aussage* verstehen wir einen Ausdruck, von dem eindeutig bestimmt ist, ob er *wahr* (w) oder *falsch* (f) ist. Beispiele für Aussagen sind z.B. „A ist der erste Buchstabe des lateinischen Alphabets“ (w), „3 ist eine Primzahl“ (w), „$3 > 5$“ (f), „$1 + 1 = 4$“ (f). Der Ausdruck „Nachts ist es kälter als draußen.“ ist keine Aussage in diesem Sinne, da unklar ist, was es bedeuten soll, der Ausdruck „Alle Personen in diesem Raum sind sympathisch.“ ist ebenfalls keine Aussage in diesem Sinne, weil verschiedene Beobachter ihr verschiedene Wahrheitswerte zuweisen würden. Wir werden den Begriff einer Aussage hier nicht weiter präzisieren; für unseren Kalkül ist nur entscheidend, dass Aussagen stets einen von zwei möglichen Wahrheitswerten annehmen.

[1] Wir empfehlen Ihnen ausdrücklich sich in einigen Semestern, nachdem Sie einige Erfahrungen mit Mathematik gemacht haben, noch einmal mit den logischen und mengentheoretischen Grundlagen der Mathematik zu beschäftigen. Es ist aber schwer und frustrierend, sich intensiv mit einer Sprache zu beschäftigen, solange man noch nicht genügend Inhalte hat, über die man reden könnte.

Wir können Aussagen miteinander verknüpfen, um aus ihnen neue Aussage zu gewinnen:

Definition 1.1.2 (Verknüpfung von Aussagen)**.** Seien A und B zwei Aussagen.

(a) Die Aussage $(\neg A)$ ist die Aussage „Die Aussage A ist falsch." und heißt die *Negation* von A.

(b) Die Aussage $(A \wedge B)$ ist die Aussage „Die Aussage A ist wahr und die Aussage B ist wahr." und heißt die *Konjunktion* von A und B.

(c) Die Aussage $(A \vee B)$ ist die Aussage „Mindestens eine der beiden Aussagen A und B ist wahr." Sie heißt die *(nicht-exklusive) Disjunktion* von A und B.

Nach Definition sind die Wahrheitswerte dieser Aussagen durch die folgende Tabelle (eine sogenannte *Wahrheitstafel*) gegeben.

A	B	$(\neg A)$	$(A \wedge B)$	$(A \vee B)$
w	w	f	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	f

Die Konjunktion ist also ein logisches „und" und die Disjunktion ist ein logisches (nicht-exklusives) „oder". Durch wiederholtes Anwenden dieser elementaren Verknüpfungen auf eine oder mehrere Aussagen, kann man weitere Aussagen definieren. Wenn wir einer solchen zusammengesetzten Aussage einen neuen Namen geben wollen, dann verwenden wir das Zuweisungssymbol „$:\Longleftrightarrow$". Z.B. schreiben wir

$$C \quad :\Longleftrightarrow \quad ((A \wedge B) \vee ((\neg A) \wedge (\neg B))) \tag{1.1.1}$$

um die Aussage „$((A \wedge B) \vee ((\neg A) \wedge (\neg B)))$" durch den Buchstaben C abzukürzen. Der Wahrheitswert dieser Aussage ist gegeben durch die folgende Tabelle

A	B	$(A \wedge B)$	$(\neg A)$	$(\neg B)$	$((\neg A) \wedge (\neg B))$	C
w	w	w	f	f	f	w
w	f	f	f	w	f	f
f	w	f	w	f	f	f
f	f	f	w	w	w	w

Definition 1.1.3. Seien A, B Aussagen.

(a) Die Aussage

$$(A \Longrightarrow B) \quad :\Longleftrightarrow \quad ((\neg A) \vee B)$$

heißt die *Implikation* von A nach B. Ist diese Aussage wahr, so sagen wir „A impliziert B".

(b) Die Aussage

$$(A \Longleftrightarrow B) \quad :\Longleftrightarrow \quad ((A \Longrightarrow B) \wedge (B \Longrightarrow A))$$

heißt die *Äquivalenz* von A und B. Ist diese Aussage wahr, so sagen wir „A ist äquivalent zu B".

Gelegentlich werden auch andere Sprechweisen verwendet: Statt „A impliziert B" sagt man auch „wenn A, dann B", „B folgt aus A", „A ist hinreichend für B" oder „B ist notwendig für A". Statt „A ist äquivalent zu B" sagt man auch „A gilt genau dann, wenn B gilt".

Bemerkung 1.1.4. Die Wahrheitswerte der Implikation ($A \Longrightarrow B$) bzw. Äquivalenz ($A \Longleftrightarrow B$) werden durch die folgende Wahrheitstafel beschrieben:

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

Beachten Sie:

- Ist die Aussage A falsch, so ist die Implikation $A \Longrightarrow B$ stets wahr; man kann also aus einer falschen Aussage folgern, was immer man möchte[2].
- Die Aussage $A \Longleftrightarrow B$ hat dieselbe Wahrheitstafel wie die Aussage C in (1.1.1), d.h. zwei Aussagen sind genau dann äquivalent wenn sie denselben Wahrheitswert besitzen[3].

Bemerkung 1.1.5 (Semantische Bedeutung der Implikation)**.** Wenn wir in der Alltagssprache sagen „A impliziert B“, dann meinen wir damit oft, dass A der Grund oder die Ursache für B ist. Es ist wichtig zu verstehen, dass dies in der hier verwendeten (und in der Mathematik allgemein gebräuchlichen) Version der Aussagenlogik *nicht* die Bedeutung der Implikation ist. Es gibt in der klassischen Aussagenlogik kein Konzept von Kausalität! Um diesen Sachverhalt zu illustrieren, betrachten wir die Implikation

$$((0 = 1) \Longrightarrow (1 = 1))$$

Nach Bemerkung 1.1.4 ist diese Implikation wahr, aber natürlich ist die falsche Aussage $0 = 1$ nicht der „Grund“ für die wahre Aussage $1 = 1$.

Satz 1.1.6 (Elementare logische Umformungen)**.** *Für beliebige Aussagen A, B, C sind die folgenden Aussagen stets wahr:*

(i) $(A \Longrightarrow A)$ *(oder anders ausgedrückt,* $A \vee (\neg A)$*).* (Tertium non datur.)

(ii) $(((A \Longrightarrow B) \wedge (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C))$. (Transitivität)

(iii) $(((A \wedge B) \wedge C) \Longleftrightarrow (A \wedge (B \wedge C)))$ *und* $(((A \vee B) \vee C) \Longleftrightarrow (A \vee (B \vee C)))$. (Assoziativität)

(iv) $((A \wedge B) \Longleftrightarrow (B \wedge A))$ *und* $((A \vee B) \Longleftrightarrow (B \vee A))$. (Kommutativität)

(v) $((A \wedge (B \vee C)) \Longleftrightarrow ((A \wedge B) \vee (A \wedge C)))$ *und* $((A \vee (B \wedge C)) \Longleftrightarrow ((A \vee B) \wedge (A \vee C)))$. (Distributivität)

(vi) $((B \Longrightarrow C) \Longrightarrow ((A \wedge B) \Longrightarrow (A \wedge C)))$. (Monotonie)

(vii) $((\neg(A \wedge B)) \Longleftrightarrow ((\neg A) \vee (\neg B)))$ *und* $((\neg(A \vee B)) \Longleftrightarrow ((\neg A) \wedge (\neg B)))$. (de Morgansche[4] Regeln)

(viii) $(\neg(\neg A)) \Longleftrightarrow A$. (doppelte Negation)

Beweis. Zum Beweis muss man die folgenden Wahrheitstafeln ausfüllen und die entsprechenden Spalten vergleichen:

[2] lat. „Ex falso quodlibet.“

[3] Mit anderen Worten: Für die in (1.1.1) definierte Aussage C ist die Aussage $(A \Longleftrightarrow B) \Longleftrightarrow C$ wahr.

[4] nach AUGUSTUS DE MORGAN, engl. Mathematiker, 1806-1871

A	$(\neg A)$	$(A \implies A)$	$(\neg(\neg A))$
w			
f			

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

A	B	$(\neg A)$	$(\neg B)$	$((\neg(A \wedge B))$	$((\neg A) \vee (\neg B)))$	$((\neg(A \vee B))$	$((\neg A) \wedge (\neg B)))$
w	w						
w	f						
f	w						
f	f						

A	B	C	$(A \implies B)$	$(B \implies C)$	$(((A \implies B) \wedge (B \implies C))$	$(A \implies C)$
w	w	w				
w	w	f				
w	f	w				
w	f	f				
f	w	w				
f	w	f				
f	f	w				
f	f	f				

A	B	C	$(((A \wedge B) \wedge C)$	$(A \wedge (B \wedge C)))$	$(((A \vee B) \vee C)$	$(A \vee (B \vee C)))$
w	w	w				
w	w	f				
w	f	w				
w	f	f				
f	w	w				
f	w	f				
f	f	w				
f	f	f				

A	B	C	$((A \wedge (B \vee C))$	$((A \wedge B) \vee (A \wedge C)))$	$((A \vee (B \wedge C))$	$((A \vee B) \wedge (A \vee C)))$
w	w	w				
w	w	f				
w	f	w				
w	f	f				
f	w	w				
f	w	f				
f	f	w				
f	f	f				

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

Tun Sie dies! □

Notation 1.1.7 (Bindungsregeln)**.** Um bei komplizierteren Ausdrücken den Überblick zu behalten, wollen wir Klammern wenn möglich weglassen. Außenklammern können stets gefahrlos weggelassen werden, also schreiben wir $A \wedge (B \vee C)$ statt $(A \wedge (B \vee C))$. Aufgrund der Assoziativität können wir auch bei mehreren aufeinanderfolgenden Konjunktionen bzw. mehreren aufeinanderfolgenden Disjunktionen Klammern weglassen. Um weitere Klammern zu sparen, vereinbaren wir, dass Negation stärker bindet als Konjunktion und Disjunktion, und dass alle drei Verknüpfungen stärker binden als Implikation und Äquivalenz. Wir schreiben also $A \wedge B \wedge \neg C \Longrightarrow A \wedge \neg C$ statt $(((A \wedge B) \wedge (\neg C)) \Longrightarrow (A \wedge (\neg C)))$.

Der Beweis von Satz 1.1.6 ist sehr leicht, aber sehr viel Schreibarbeit und sehr fehleranfällig. Deutlich kompliziertere Aussagen können wir als Menschen nicht mehr sinnvoll mittels Wahrheitstafeln auf Äquivalenz untersuchen. Der Computer ist uns in diesem Punkt voraus, aber auch er muss irgendwann aufgeben. Ausgehend von den grundlegenden Umformungsregeln aus Satz 1.1.6 können wir aber neue Umformungsregeln beweisen, indem wir bereits bekannte Regeln wiederholt anwenden. Hier ist ein typisches Anwendungsbeispiel[5]:

Korollar 1.1.8 (Kontrapositionsprinzip)**.** *Für beliebige Aussagen A und B gilt*

$$(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A).$$

Beweis. Für beliebige Aussagen A und B gilt:

$$\begin{aligned}
(A \Longrightarrow B) &\Longleftrightarrow \neg A \vee B && \text{(nach Definition der Implikation)}\\
&\Longleftrightarrow B \vee \neg A && \text{(wegen Kommutativität von } \vee)\\
&\Longleftrightarrow \neg(\neg B) \vee \neg A && \text{(doppelte Negation)}\\
&\Longleftrightarrow (\neg B \Longrightarrow \neg A) && \text{(nach Definition der Implikation)}
\end{aligned}$$

Wegen der Transitivität der Implikation folgt daraus das Korollar. □

Bemerkung 1.1.9 (Beweis durch Kontraposition)**.** Kontraposition ist häufig eine nützliche Beweismethode: Angenommen, es ist die Wahrheit der Implikation $A \Longrightarrow B$ zu zeigen. Man nimmt zunächst an, B sei falsch. Mit etwas Glück kann man vielleicht daraus folgern, dass dann auch A falsch sein muss. In diesem Fall hat man dann die Implikation $(\neg B) \Longrightarrow (\neg A)$, und daher wegen des Kontrapositionsprinzip auch die Implikation $A \Longrightarrow B$ gezeigt. Beispiele für diese Art zu schließen werden wir noch häufig zu sehen bekommen. Hilfreich ist diese Beweistechnik dann, wenn die Annahme der Falschheit von B eine Denkrichtung vorgibt, die man unter der Annahme der Wahrheit von A vielleicht nicht einschlagen würde.

[5] Eine unmittelbare Folgerung aus einem Satz bezeichnet man in der Mathematik als ein „Korollar“.

Bemerkung 1.1.10. Im Beweis von Korollar 1.1.8 haben wir ausschließlich Äquivalenzumformungen gemacht. Bei komplizierteren Beweisen werden wir so nicht vorgehen können. In den meisten Fällen wird man, um die Äquivalenz zweier Aussage A und B zu zeigen, zunächst die Implikation $A \Longrightarrow B$ und anschließend die Implikation $B \Longrightarrow A$ zeigen. Dies wird im Beweis oft dadurch kenntlich gemacht, dass man den Äquivalenzpfeil in zwei Implikationspfeile zerlegt und eben einmal „$\Longrightarrow$“ zeigt, das ist die Implikation von links nach rechts, und dann auch noch „$\Longleftarrow$“, die andere Implikation.

Übung 1.1.11. Zeigen Sie, analog zu Korollar 1.1.8, dass für beliebige Aussagen A und B die folgende Implikation gilt:

$$\neg(A \wedge \neg B) \Longleftrightarrow (A \Longrightarrow B). \tag{1.1.2}$$

Bemerkung 1.1.12 (Widerspruchsbeweis)**.** Um die Implikation $A \Longrightarrow B$ zu zeigen, können wir also wie folgt vorgehen: Wir nehmen an, dass A und die Negation von B gelten[6]. Können wir daraus eine falsche Aussage (einen sogenannten *Widerspruch*) herleiten, so gilt $\neg(A \wedge \neg B)$, und daher haben wir nach (1.1.2) die gewünschte Implikation bewiesen. Auch hierfür werden wir noch viele Beispiele sehen.

Zusammenfassung von Abschnitt 1.1

(1) Aussagen sind Ausdrücke, denen ein eindeutiger Wahrheitswert („wahr“ oder „falsch“) zugeordnet werden kann.

(2) Aussagen können negiert und mittels Konjunktion und Disjunktion zu komplizierteren verknüpft werden.

(3) Aussagen sind äquivalent, wenn sie den gleichen Wahrheitswert besitzen. Mittels elementarer logischer Umformungen kann man Aussagen in äquivalente Aussagen umformen.

(4) Anstatt die Wahrheit einer Implikation direkt nachzuweisen, kann man die Wahrheit der Kontraposition nachweisen oder einen Widerspruchsbeweis führen.

1.2 Naive Mengenlehre

Bemerkung 1.2.1 (Wie man nicht definiert, was eine Menge ist)**.** In der Mathematik haben wir es oft mit Zusammenfassungen von Objekten, sogenannten *Mengen* und *Klassen* zu tun. GEORG CANTOR[7] schlug 1883 die folgende Definition vor: Eine *Menge* M ist eine Zusammenfassung von „Objekten“ so dass für jedes „denkbare Objekt“ x eindeutig geklärt ist, ob x zu M gehört oder nicht. Im ersten Fall schreibt man dann „$x \in M$“ und nennen x ein *Element* von M, und im zweiten Fall schreiben wir „$x \notin M$“. Nach Definition sind zwei Mengen M und N genau dann gleich, wenn sie dieselben Elemente besitzen.

Aus Sicht der modernen Mathematik ist das keine brauchbare Definition, denn es ist unklar, was ein „denkbares Objekt“ ist. Pragmatiker werden einwenden, dass dies wohl eher ein philosophisches Problem ist und in der Praxis immer klar sein wird, welche Objekte gemeint sind.

[6] Man nennt dies die *Widerspruchsannahme*

[7] kurz für GEORG FERDINAND LUDWIG PHILIPP CANTOR, dt. Mathematiker, 1845-1918

Dies war gegen Ende des 19. Jahrhunderts wohl auch die Mehrheitsmeinung unter den Mathematikern. Lassen wir uns also zunächst einmal auf Cantors „Definition“ ein, und schauen wir, wie weit wir damit kommen.

Bemerkung 1.2.2 (Konkrete Beschreibung von Mengen)**.** Wie können wir konkret eine Menge M angeben?

(i) Wir können bei endlichen Mengen (d.h. Mengen, die nur endlich viele Elemente enthalten) einfach alle Elemente der Menge angeben. Dazu benutzen wir die folgende Schreibweise:

$$M := \{1, a, \alpha\}$$

Hier ist „:=“ das *Zuweisungssymbol*; auf der linken Seite steht der Name der Menge („Definiendum“) und auf der rechten Seite („Definiens“) werden die Elemente der Menge von den Mengenklammern „{“ und „}“ eingerahmt. Nach Definition gilt dann

$$M = \{1, a, \alpha, a\} = \{\alpha, 1, 1, a\}.$$

(ii) Unendliche Mengen können wir auf diese Weise natürlich nicht beschreiben, aber wenn wir schreiben

$$\mathbb{N} := \{1,2,3,4,5,\dots\} \quad \text{bzw.} \quad \mathbb{Z} := \{\dots,-3,-2,-1,0,1,2,3,\dots\}$$

dann werden Sie sicher verstehen, dass hier die Menge der *natürlichen Zahlen*[8] bzw. der *ganzen Zahlen* gemeint ist.

(iii) Wir können Mengen auch in beschreibender oder *impliziter Form* angeben: Für die Menge aller Menschen schreiben wir z.B.

$$M := \{x \mid x \text{ ist Mensch}\}$$

Vor dem Trennstrich wird hier eine Variable eingeführt, und nach dem Trennstrich werden die Eigenschaften aufgezählt, die diese Variable erfüllen muss.

(iv) Eine Menge muss keine Elemente enthalten! Wir bezeichen mit $\emptyset := \{\}$ die *leere Menge*.

Bemerkung 1.2.3 (Aussagen in Mengensprache formulieren)**.** Die Aussage „4 ist eine natürliche Zahl“ können wir in Mengensprache formulieren als „$4 \in \mathbb{N}$“. Fast alle[9] Aussagen, die uns interessieren, können in Mengensprache formuliert werden, z.B. gilt

$$(b \text{ ist ein blaues Auto}) \iff (b \in \{x \mid x \text{ ist ein blaues Auto}\}).$$

Unter dieser Umformulierung entsprechen die elementaren logischen Umformungen den folgenden Operationen auf Mengen.

Definition 1.2.4. Seien M und N Mengen.

(i) $M \cap N := \{x \mid (x \in M) \wedge (x \in N)\}$ heißt der *Schnitt von M und N*.

(ii) $M \cup N := \{x \mid (x \in M) \vee (x \in N)\}$ heißt die *Vereinigung von M und N*.

(iii) $M \setminus N := \{x \mid (x \in M) \wedge (x \notin N)\}$ *h*eißt das *Komplement von N in M*.

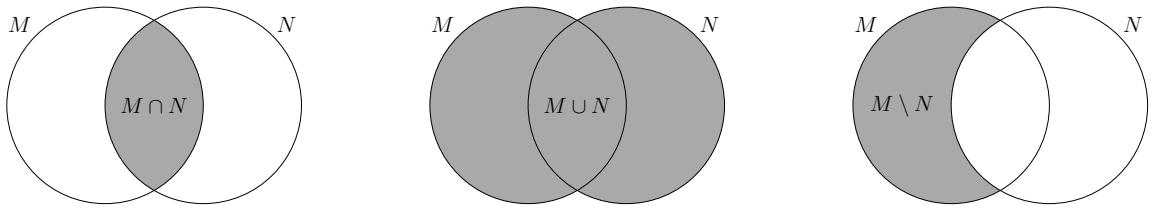


Abbildung 1.1: Mengenoperationen

Wir können diese Definitionen anhand sogenannter Venn-Diagramme veranschaulichen, wie in Abbildung 1.1 dargestellt.

Bemerkung 1.2.5. Schnitt entspricht also in der Mengensprache der Konjunktion, und Vereinigung entspricht der Disjunktion. Man würde gerne auch eine direkte Entsprechung der Negation haben, also zu einer Menge N die Menge $\{x \mid x \notin N\}$ definieren. Wir werden aber noch sehen, dass dies zu Problemen führt, da nicht klar ist, aus welcher Grundgesamtheit von Objekten x kommen soll, vgl. Bemerkung 1.2.15.

Wir können nun auch noch die Implikation in Mengensprache formulieren:

Definition 1.2.6. Eine Menge M heißt *Teilmenge* einer Menge N, geschrieben $M \subseteq N$, falls gilt $((x \in M) \Longrightarrow (x \in N))$. Wir schreiben dann $M \subseteq N$.

Der Strich in „$\subseteq$“ deutet an, dass M und N auch gleich sein dürfen. Wenn wir sagen wollen, dass M eine Teilmenge von N, aber nicht gleich ist, so schreiben wir

$$M \subsetneq N :\Longleftrightarrow (M \subseteq N) \wedge (M \neq N).$$

Bemerkung 1.2.7 (Logische Umformungen vs. Mengenumformungen)**.** Wir können nun alle elementaren logischen Umformungen aus Satz 1.1.6 in Mengensprache übersetzen. Als Beispiel betrachten wir Punkt (v): Es gilt für beliebige Mengen M,N,O, dass

$$\begin{aligned} x \in M \cap (N \cup O) &\iff (x \in M) \wedge (x \in (N \cup O)) \\ &\iff (x \in M) \wedge ((x \in N) \vee (x \in O)) \\ &\overset{\text{Satz 1.1.6.(v)}}{\iff} (x \in M \wedge x \in N) \vee ((x \in M) \wedge (x \in O)) \\ &\iff (x \in (M \cap N)) \vee (x \in (M \cap O)) \\ &\iff x \in (M \cap N) \cup (M \cap O). \end{aligned}$$

Dies zeigt, dass $M \cap (N \cup O) = (M \cap N) \cup (M \cap O)$. Beachte, dass wir in allen Beweisschritten außer dem markierten lediglich die Definitionen ausgeschrieben haben.

Durch Umschreiben der anderen Aussagen aus Satz 1.1.6 erhält man analog:

Satz 1.2.8 (Rechenregeln für Mengen)**.** *Für beliebige Mengen M,N,O gilt:*

(i) $M \subseteq M$.

(ii) $M \subseteq N \subseteq O \Longrightarrow M \subseteq O$.

[8] Für uns gehört 0 nicht zu den natürlichen Zahlen.

[9] Aber nicht alle, vgl. Bemerkung 1.2.15!

(iii) $(M \cap N) \cap O = M \cap (N \cap O)$ *und* $(M \cup N) \cup O = M \cup (N \cup O)$.

(iv) $M \cap N = N \cap M$ *und* $M \cup N = N \cup M$.

(v) $M \cap (N \cup O) = (M \cap N) \cup (M \cap O)$ *und* $M \cup (N \cap O) = (M \cup N) \cap (M \cup O)$.

(vi) $N \subseteq O \Longrightarrow (M \cap N) \subseteq (M \cap O)$.

(vii) $O \setminus (M \cap N) = (O \setminus M) \cup (O \setminus N)$ *und* $O \setminus (M \cup N) = (O \setminus M) \cap (O \setminus N)$.

(viii) $O \setminus (O \setminus M) = M \cap O$.

Die Aussagen (i)-(vi) entsprechen hier genau den Aussagen (i)-(vi) aus Satz 1.1.6. Die Aussagen (vii) und (viii) mussten wir leicht abwandeln, da es in der Mengensprache keine direkte Entsprechung der Negation gibt.

Übung 1.2.9. Beweisen Sie Satz 1.2.8, indem Sie jede Aussage auf die entsprechende(n) Aussage(n) von Satz 1.1.6 zurückführen.

Bemerkung 1.2.10 (Gleichheit vs. Inklusion von Mengen)**.** Für zwei Mengen M und N gilt:

$$M = N \Leftrightarrow (x \in M \Leftrightarrow x \in N) \Leftrightarrow ((x \in M \Longrightarrow x \in N) \wedge (x \in N \Longrightarrow x \in M)) \Leftrightarrow (M \subseteq N) \wedge (N \subseteq M).$$

Um zu zeigen, dass zwei Mengen gleich sind, kann man also zeigen, dass sie jeweils ineinander enthalten sind (genauso, wie man eine Äquivalenz beweist, indem man zwei Implikationen zeigt). Das ist oftmals eine wichtige Beweismethode.

Bemerkung 1.2.11 (Mengen von Mengen)**.** Für die moderne Mathematik ist es ganz entscheidend, dass Elemente von Mengen selbst wieder Mengen sein dürfen. So konstruiert etwa von Neumann[10] augehend von der leeren Menge ein Modell der natürlichen Zahlen mittels der endlichen Mengen

$$\mathbb{1} := \{\emptyset\}, \quad \mathbb{2} := \{\emptyset, \mathbb{1}\} = \{\emptyset, \{\emptyset\}\}, \quad \mathbb{3} := \{\emptyset, \mathbb{1}, \mathbb{2}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots$$

Beachten Sie, dass $\emptyset \neq \mathbb{1}$, denn $\emptyset$ enthält keine Elemente, aber $\mathbb{1}$ enthält genau ein Element (nämlich die leere Menge).

Bei Umgang mit Mengen von Mengen muss man sehr genau zwischen den Symbolen „$\subseteq$“ und „$\in$“ unterscheiden. Ist $M := \{1, \{2\}\}$, so gilt $\{1\} \subseteq M$ und $\{2\} \in M$, aber die Aussagen $\{1\} \in M$ und $\{2\} \subseteq M$ sind falsch.

Ein wichtiges Beispiel für eine Menge von Mengen ist die folgende:

Definition 1.2.12. Ist M eine Menge, so heißt

$$\mathscr{P}(M) := \{N \mid N \text{ ist Teilmenge von } M\}$$

die *Potenzmenge* von M. Eine Teilmenge $\mathscr{A} \subseteq \mathscr{P}(M)$ heißt ein *Mengensystem* über M.

[10] JOHN VON NEUMANN, am. Universalgenie mit ungarischen Wurzeln und Autor bahnbrechender Arbeiten zur Mathematik, Physik, Informatik, Logik und Ökonomie, 1903–1957

Beispiel 1.2.13 (Russelsche Antinomie)**.** Wir präsentieren nun ein berühmtes Beispiel von BERTRAND RUSSELL[11], mit dem dieser im Jahr 1901 die Cantorsche Mengenlehre zum Einsturz brachte. Nach Cantor können wir eine Menge von Mengen definieren durch

$$R := \{M \mid M \text{ ist Menge und } M \notin M\}. \tag{1.2.1}$$

Russell stellt nun die scheinbar harmlose Frage: Ist R ein Element von R? Beide möglichen Antworten führen auf einen Widerspruch[12]:

Wäre $R \in R$, so wäre die Aussage $R \notin R$ falsch, und daher erfüllt R die definierende Bedingung von R nicht, also $R \notin R$.

Wäre $R \notin R$, so erfüllt die Menge R die definierende Bedingung von R, also wäre $R \in R$.

Bemerkung 1.2.14 (Wege aus der Krise)**.** Die Cantorsche Mengenlehre enthält also unauflösbare Widersprüche. Diese Entdeckung führte um die Jahrhunderwende zu einer Grundlagenkrise der Mengenlehre. Um dieser Krise zu entkommen, haben die Mathematiker die Mengenlehre axiomatisiert und genau festgelegt[13], welche Zusammenfassungen von Objekten Mengen sind, und welche nicht. Die Axiome sind zu kompliziert um hier vollständig wiedergegeben zu werden; wir begnügen uns mit einer Skizze

(i) In der modernen Mengenlehre unterscheidet man *Klassen* (gewisse Zusammenfassungen von Objekten im Sinne von Cantor) und *Mengen*. Klassen sind grob gesagt Ansammlungen von Objekten, die durch Eigenschaften beschrieben werden. Mengen sind genau diejenigen Klassen, die selbst Element einer Klasse sind.

(ii) Schnitte, Vereinigungen, Komplemente, Teilmengen und Potenzmengen von Mengen sind wieder Mengen und es gelten die aus Satz 1.2.8 bekannten Identitäten.

(iii) Durch (1.2.1) wird eine Klasse definiert, die keine Menge ist. Damit löst sich das Paradox aus Beispiel 1.2.13 auf. Da Teilmengen von Mengen wieder Mengen sind, ist jede Klasse, die R enthält keine Menge. Insbesondere ist die Klasse $\mathscr{M} := \{M \mid M \text{ ist eine Menge}\}$ aller Mengen keine Menge.

Bemerkung 1.2.15 (Zwei Randbemerkungen[14])**.** Ist N eine Menge, so ist die Klasse $\{x \mid x \notin N\}$ keine Menge im Sinne der axiomatischen Mengenlehre; dies ist der Grund, warum es in der Mengensprache keine direkte Entsprechung der Negation gibt. Die Aussage „M ist eine Menge und $M \notin M$“ lässt sich in Klassensprache formulieren als $M \in R$ mit R wie in (1.2.1); da R keine Menge ist, lässt sie sich aber nicht in Mengensprache formulieren. Dies erklärt unsere Bemerkung, dass sich *fast alle, aber nicht alle* Aussagen in Mengensprache ausdrücken lassen.

[11] engl. Philosoph und Logiker, 1872-1970, Literaturnobelpreisträger(!) 1950

[12] Die hinter diesem Beispiel stehende Idee der *Selbstreferentialität* kennt man vielleicht aus dem berühmten „Barbier-Paradox“, das die folgende Frage stellt: „Wenn der Barbier genau diejenigen Männer des Dorfes rasiert, die sich nicht selbst rasieren, rasiert der Barbier sich dann selbst?“

[13] Genauer gesagt: Es gibt in der modernen Mathematik verschiedene Formalisierungen des Mengenbegriffs, die sich aber nur so subtil unterscheiden, dass die Unterschiede für die Fragen dieser Vorlesung keine Rolle spielen.

[14] Kleingedruckte Abschnitte im Skript sind nicht offizieller Teil der Vorlesung und dienen nur der Information

[27.10.23]

Bemerkung 1.2.16 (Aussageformen über Mengen)**.** Die Ausdrücke „Das Auto ist blau." und „$x^2 = 4$" sind keine Aussagen, weil ihr Wahrheitswert davon abhängt, welches Auto gemeint ist bzw. welche Zahl man in die Variable x einsetzt. Man nennt einen solchen Ausdruck eine *Aussageform* und die darin vorkommenden nicht erkärten Begriffe *freie Variablen*.

Wenn man in einer Aussageform jede freie Variable durch einen passenden Begriff ersetzt, erhält man eine Aussage. Z.B. sind $2^2 = 4$ und $3^2 = 4$ Aussagen. Ist $\mathscr{A}(x)$ eine Aussageform mit freier Variablen x, und ergibt sich eine Aussage, wenn man für x ein Element einer Menge M einsetzt, so nennt man $\mathscr{A}(x)$ eine *Aussageform über* M. Z.B. ist „Das Auto ist blau." eine Aussageform über der Menge aller Autos.

Notation 1.2.17 (Teilmengen mittels Aussageformen)**.** Ist M eine Menge und $\mathscr{A}(x)$ eine Aussageform über M, so schreiben wir

$$\{x \in M \mid \mathscr{A}(x)\} := \{x \mid (x \in M) \wedge (\mathscr{A}(x) \text{ ist wahr})\}$$

für die Menge aller x aus M, die $\mathscr{A}(x)$ erfüllen. Als Teilmenge von M ist dies stets wieder eine Menge. Z.B. ist

$$\{x \in \mathbb{N} \mid x < 4\} = \{1,2,3\}.$$

Bemerkung 1.2.18 (Quantoren)**.** Ist $\mathscr{A}(x)$ eine Aussageform über einer Menge M so können wir drei neue Aussagen definieren:

(i) Die *All-Aussage:* „Für jedes Element $x \in M$ ist $\mathscr{A}(x)$ wahr."

(ii) Die *Existenz-Aussage:* „Es gibt mindestens ein Element $x \in M$, für das $\mathscr{A}(x)$ wahr ist."

(iii) Die *Existenz-und-Eindeutigkeits-Aussage*: „Es gibt genau ein Element $x \in M$, für das $\mathscr{A}(x)$ wahr ist."

Wir schreiben diese Aussagen symbolisch als

$$\forall\, x \in M : \mathscr{A}(x) \quad \text{bzw.} \quad \exists\, x \in M : \mathscr{A}(x) \quad \text{bzw.} \quad \exists!\, x \in M : \mathscr{A}(x).$$

Das Symbol $\forall$ heißt der *Allquantor*, das Symbol $\exists$ heißt der *Existenzquantor*.

Beispiel 1.2.19. Die Aussage $\forall\, x \in \mathbb{N} : x^2 = 4$ ist falsch und die Aussage $\exists\, x \in \mathbb{N} : x^2 = 4$ ist wahr. Es gilt sogar die stärkere Aussage $\exists!\, x \in \mathbb{N} : x^2 = 4$.

Bemerkung 1.2.20 (Quantoren und Negation)**.** Quantoren „drehen sich bei Negation um", es gelten also die *Negationsregeln*

$$\neg(\forall\, x \in M : \mathscr{A}(x)) \iff \exists\, x \in M : \neg\mathscr{A}(x) \quad \text{und} \quad \neg(\exists\, x \in M : \mathscr{A}(x)) \iff \forall\, x \in M : \neg\mathscr{A}(x).$$

Bemerkung 1.2.21 (Äquivalenz von Aussageformen)**.** Wir sagen, dass zwei Aussageformen über einer Menge M äquivalent sind, wenn sie für alle möglichen Belegungen äquivalent sind:

$$(\mathscr{A}(x) \iff \mathscr{B}(x)) \quad :\iff \quad (\forall\, x \in M : \mathscr{A}(x) \iff \mathscr{B}(x)))$$

Caveat 1.2.22 (Mehrere freie Variable)**.** Bei Aussageformen mit mehreren freien Variablen führt das Anwenden eines Quantors auf eine freie Variable zunächst auf eine neue Aussageform; erst wenn alle Variablen quantifiziert sind, erhält man eine Aussage. Dabei ist die Reihenfolge der Quantoren zu beachten: Die Aussage $\forall\, x \in \mathbb{N}\, \exists\, y \in \mathbb{N} : x < y$ ist wahr, aber die Aussage $\exists\, y \in \mathbb{N}\, \forall\, x \in \mathbb{N} : x < y$ ist falsch.

Mittels Quantoren können wir nun definieren:

Definition 1.2.23. Ist M eine Menge und $\mathscr{A} \subseteq \mathscr{P}(M)$ ein Mengensystem, so heißen

$$\bigcap \mathscr{A} := \bigcap_{A \in \mathscr{A}} A := \{x \in M \mid \forall\, A \in \mathscr{A} : x \in A\} \quad \text{und} \quad \bigcup \mathscr{A} := \bigcup_{A \in \mathscr{A}} A := \{x \in M \mid \exists A \in \mathscr{A} : x \in A\}$$

der *Schnitt* bzw. die *Vereinigung* über $\mathscr{A}$.

Schnitte und Vereinigungen über beliebige Mengensyteme sind stets wieder Mengen.

Notation 1.2.24. Ist M eine endliche Menge, so bezeichne $|M|$ die Anzahl der Elemente von M.

Übung 1.2.25. Es seien M und N endliche Mengen. Machen Sie sich klar, dass

$$|M \cup N| = |M| + |N| - |M \cap N| \quad \text{und} \quad |\mathscr{P}(M)| = 2^{|M|}.$$

Zusammenfassung von Abschnitt 1.2

(1) Mengen sind gewisse gutartige Zusammenfassungen von Objekten; auf eine formale Definition verzichten wir.

(2) Durch die Operationen Schnitt, Vereinigung, Komplementbildung und Potenzmengenbildung kann man aus gegebenen Mengen neue Mengen erzeugen. Die Rechenregeln für diese Operationen ergeben sich aus den Regeln der Aussagenlogik.

(3) Um Gleichheit zweier Mengen zu zeigen, genügt es zu zeigen, dass sie wechselseitig ineinander enthalten sind.

1.3 Relationen und Funktionen

Nachdem wir im letzten Abschnitt Ansammlungen von Objekten studiert haben, wollen wir nun verschiedene solche Ansammlungen miteinander in Beziehung setzen. Beziehungen zwischen Mengen werden in der Mathematik durch sogenannte Relationen ausgedrückt. Dieser Begriff ist extrem allgemein (zu allgemein für unsere Zwecke) und formal.

Notation 1.3.1. Sind M und N Mengen, und ist $m \in M$ und $n \in N$, so bezeichnet $(m,n) := \{m,\{m,n\}\}$ das *geordnete Paar* bestehend aus $m \in M$ und $n \in N$. Für $m_1, m_2 \in M$ und $n_1, n_2 \in N$ gilt dann

$$(m_1,n_1) = (m_2,n_2) \iff (m_1 = m_2) \wedge (n_1 = n_2).$$

Dann ist

$$M \times N := \{(m,n) \mid m \in M, n \in N\}$$

wieder eine Menge, genannt das *kartesische*[15] *Produkt* von M und N.

Definition 1.3.2. Eine *Relation* $R = (M,N,G_R)$ besteht aus einer Menge M, genannt die *Definitionsmenge* von R, einer Menge N, genannt die *Zielmenge* von R, und einer Teilmenge $G_R \subseteq M \times N$, genannt der *Graph* von R. Zwei Relationen sind *gleich*, wenn sie dieselbe Definitionsmenge und Zielmenge und denselben Graphen haben.

[15] nach RENÉ DESCARTES, 1596-1650, französischer Philosoph, Mathematiker und Naturgelehrter

Bemerkung 1.3.3 (Sprechweisen)**.** Ist $R = (M, N, G_R)$ eine Relation, so sagt man auch, R ist eine Relation *von* M *nach* N. Ist $M = N$, so nennt man R auch eine Relation *auf* M. Ist $(m,n) \in G_R$, so sagt man auch „m ist R-verwandt zu n“ und schreibt mRn.

Beispiel 1.3.4. „ist Mutter von“ $:= (\{x \mid x \text{ ist Frau}\}, \{y \mid y \text{ ist Mensch}\}, \{(x,y) \mid x \text{ ist Mutter von } y\})$ ist eine Relation.

Die für uns wichtigsten Relationen sind *Funktionen* und *Äquivalenzrelationen*. In der Analysis werden Sie einiges über sogenannte *Ordnungsrelationen* lernen, und in der Informatik benötigt man sehr viel allgemeinere Klassen von Relationen. Wir werden uns auf diejenigen Klassen von Relationen beschränken, die wir benötigen und hier keine allgemeine Theorie von Relationen entwickeln.

Definition 1.3.5. Eine Relation $f = (M, N, G_f)$ heißt *Funktion* oder[16] *Abbildung*, wenn

$$\forall\, m \in M\ \exists!\, n \in N : (m,n) \in G_f.$$

Ist $m \in M$, so heißt das eindeutige Elemente $n \in N$ mit $(m,n) \in G_f$ das *Bild* von m unter f, und man schreibt $f(m) := n$.

Notation 1.3.6 (Pfeilnotation)**.** Der französische Mathematiker JEAN LERAY[17] schlug in den 1940er Jahren vor, eine Funktion f von M nach N durch einen Pfeil zu symbolisieren. Es gibt die beiden konkurrierenden Schreibweisen

$$f : M \to N \quad \text{oder} \quad M \xrightarrow{f} N.$$

Um eine solche Funktion zu beschreiben genügt es, für jedes Element $x \in M$ das Bildelement $f(x)$ anzugeben. Statt $f(x) := y$ schreibt man manchmal auch $x \mapsto y$.

Beispiel 1.3.7 (Eine numerische Funktion)**.** Die Funktion

$$p : \mathbb{Z} \to \mathbb{Z}, \quad n \mapsto 3n^2 + 7.$$

bildet jede ganze Zahl n auf die ganze Zahl $3n^2 + 7$ ab. Sie ist von der Funktion

$$q : \mathbb{Z} \to \mathbb{N}, \quad n \mapsto 3n^2 + 7$$

verschieden, weil sie einen anderen Zielbereich hat.

Bis ins 19. Jahrhundert wurden in der Mathematik vorwiegend Funktionen betrachtet, die durch Formeln wie im obigen Beispiel gegeben waren. Für die moderne Mathematik und Informatik ist es aber entscheidend, dass Funktionen *nicht* durch Formeln beschreibbar sein müssen.

Notation 1.3.8. Im Folgenden seinen M und N zwei beliebige Mengen und $f : M \to N$ eine Funktion.

(i) Ist $A \subseteq M$, so heißt $f[A] := \{n \in N \mid \exists a \in A : f(a) = n\}$ das *Bild* von A.

(ii) Speziell heißt $\text{Bild}(f) := f[M]$ das *Bild* der Funktion $f : M \to N$.

[16] Die beiden Begriffe sind vollkommen synonym und werden leider beide verwendet.
[17] frz. Mathematiker, 1906-1998

(iii) Ist $B \subseteq N$, so heißt $f^{-1}[B] := \{m \in M \mid f(m) \in B\}$ das *Urbild* von B.

(iv) Ist $n \in N$, so heißt $f^{-1}[n] := f^{-1}[\{n\}]$ die *Faser* über n, und die Elemente von $f^{-1}[n]$ heißen *Urbilder* von n.

Definition 1.3.9. Die Funktion $f : M \to N$ heißt

(i) *injektiv*, falls $\forall\, m_1, m_2 \in M : f(m_1) = f(m_2) \implies m_1 = m_2$;

(ii) *surjektiv*, falls $\mathrm{Bild}(f) = N$;

(iii) *bijektiv*, falls sie injektiv und surjektiv ist.

Man schreibt in diesen Fällen auch

$$f : M \hookrightarrow N, \quad f : M \twoheadrightarrow N \quad \text{bzw.} \quad f : M \rightarrowtail N.$$

Bemerkung 1.3.10. Sei $f : M \to N$ eine Funktion.

(a) f ist injektiv, wenn man m eindeutig daran erkennen kann, was $f(m)$ ist, d.h. für jedes $n \in N$ gibt es *höchstens* ein m mit $f(m) = n$. Man kann diese Bedingung mittels der Fasern von f ausdrücken als

$$\forall\, n \in N : |f^{-1}[n]| \leq 1.$$

Nach dem Kontrapositionsprinzip (Korollar 1.1.8) ist die Injektivität von f äquivalent zu der Bedingung

$$\forall m_1, m_2 \in M : m_1 \neq m_2 \implies f(m_1) \neq f(m_2).$$

(b) f ist surjektiv, wenn jedes Element von N ein Urbild hat, d.h. für jedes $n \in N$ gibt es *mindestens* ein $m \in M$ mit $f(m) = n$. Dies bedeutet, dass die Fasern von f nicht leer sind, also

$$\forall\, n \in N : f^{-1}[n] \neq \emptyset.$$

(c) Aus (a) und (b) ergibt sich, dass die Bijektivität von gleichbedeutend ist mit

$$\forall\, n \in N : |f^{-1}[\{n\}]| = 1.$$

Für jedes $n \in N$ gibt es also *genau* ein Urbild m. Wir bezeichnen dieses mit $f^{-1}(n) := m$, so dass $f^{-1}[n] = \{f^{-1}(n)\}$ für alle $n \in \mathbb{N}$ gilt. Die Elemente von M und N entsprechen sich unter f also Eins-zu-Eins.

Definition 1.3.11. Ist $f : M \to N$ eine bijektive Funktion, so heißt die Funktion

$$f^{-1} : N \to M, \quad n \mapsto f^{-1}(n)$$

die *Umkehrfunktion* von f.

Um ein interessantes Beispiel diskutieren zu können, führen wir die folgende Notation ein.

Notation 1.3.12. Sei $f : M \to N$ eine Funktion.

(i) Ist $A \subseteq M$, so heißt die Funktion

$$f|_A : A \to N, \quad a \mapsto f(a)$$

die *Restriktion* von f auf A.

(ii) Ist $B \subseteq N$ mit $\mathrm{Bild}(f) \subseteq B$, so heißt die Funktion

$$f|^B : M \to B, \quad m \mapsto f(m)$$

die *Korestriktion* von f auf B.

Beispiel 1.3.13. (i) Die (hier als aus der Schule bekannt vorausgesetzte, aber im Folgenden nicht benötigte) Cosinus-Funktion $\cos : \mathbb{R} \to \mathbb{R}$ ist weder injektiv (wegen $f(0) = f(2\pi)$) noch surjektiv (da $3 \notin \mathrm{Bild}(f)$).

(ii) Die Restriktion $\cos|_{[0,\pi]}$ ist injektiv, aber nicht surjektiv.

(iii) Die Korestriktion $(\cos|_{[0,\pi]})|^{[-1,1]}$ ist bijektiv. Ihre Umkehrfunktion wird in der Analysis mit arccos („arcus cosinus“) bezeichnet.

Durch geeignete Restriktion und Korestriktion kann man jede Funktion bijektiv machen; z.B. ist für jede Funktion f die Korestriktion $f|^{\mathrm{Bild}(f)}$ surjektiv. Wir wollen nun injektive, surjektive und bijektive Funktionen algebraisch charakterisieren. Im Folgenden seien M, N, O, P beliebige Mengen.

Definition 1.3.14. Sind $f : M \to N$ und $g : N \to O$ Funktionen, so ist ihre *Komposition* oder *Verkettung* die durch

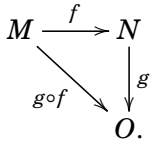
$$g \circ f : M \to O, \quad m \mapsto g(f(m)).$$

gegebene[18] Funktion.

Übung 1.3.15. Seien $f : M \to N$ und $g : N \to O$ Funktionen. Zeigen Sie, dass

$$G_{g \circ f} = \{(m, o) \in M \times O \mid \exists n \in N : (m, n) \in G_f \text{ und } (n, o) \in G_g\}.$$

Notation 1.3.16 (Kommutatives Diagramm)**.** Sind $f : M \to N$ und $g : N \to O$ Funktionen, so erhalten wir ein Diagramm



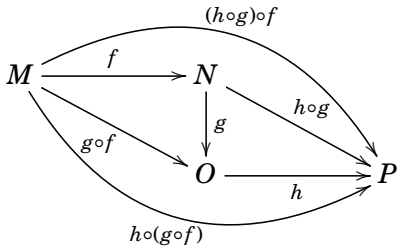
Starten wir von einem Element in M, so ist es egal, ob wir erst mittels f nach rechts und dann mit g nach unten laufen, oder ob wir mittels $g \circ f$ diagonal abkürzen. Wir sagen daher, dass „das Diagramm kommutiert“. Viele wichtige Sätze der Algebra lassen sich durch solche „kommutativen Diagramme“ ausdrücken.

Lemma 1.3.17 (Assoziativität der Verkettung[19])**.** *Seien $f : M \to N$, $g : N \to O$ und $h : O \to P$ Abbildungen. Dann gilt*

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

[18] Man beachte, dass *zuerst* f und dann g angewendet wird; man liest daher $g \circ f$ auch als „g nach f“.
[19] Ein „Lemma“ ist ein Hilfssatz, der vor allem zum Beweis anderer Sätze verwendet wird.

d.h. das Diagramm



kommutiert.

Beweis. Nach Definition sind $(h \circ g) \circ f$ und $h \circ (g \circ f)$ zwei Funktionen von M nach P. Für alle $m \in M$ gilt nun

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

Folglich haben die beiden zwei Funktionen dieselbe Zuordnungsvorschrift und sind daher gleich. □

Übung 1.3.18. Sei $\mathrm{Id}_M : M \to M$ die *identische Abbildung* gegeben durch $\mathrm{Id}_M(m) := m$. Zeigen Sie, dass für alle Funktionen $f : M \to N$ gilt:

$$f \circ \mathrm{Id}_M = f \quad \text{und} \quad \mathrm{Id}_N \circ f = f.$$

[3.11.23]

Satz 1.3.19 (Existenz von Links-/Rechtsinversen)**.** *Es sei $M \neq \emptyset$ und $f : M \longrightarrow N$ eine Funktion. Dann gelten die folgenden Äquivalenzen:*

(i) f *ist injektiv* $\iff (\exists g : N \longrightarrow M$ *mit* $g \circ f = \mathrm{Id}_M)$.

(ii) f *ist surjektiv* $\iff (\exists h : N \longrightarrow M$ *mit* $f \circ h = \mathrm{Id}_N)$.

(iii) f *ist bijektiv* $\iff$ *Es gibt g und h wie in (i) und (ii).*
In diesem Fall gilt automatisch $g = h = f^{-1}$.

Beweis. (i) „$\Longrightarrow$“: Wir gehen von der Voraussetzung aus, dass f injektiv ist. Zu zeigen ist die Existenz einer Abbildung g mit den gewünschten Eigenschaften. Um diese zu konstruieren, wählen wir zunächst ein $m_0 \in M$. Dies ist möglich, weil die Menge M nicht leer ist. Ist $n \in N \setminus \mathrm{Bild}(f)$ so definieren wir $g(n) := m_0$. Andernfalls existiert wegen der Injektivität von f ein eindeutiges $m \in M$ mit $f(m) = n$ und wir setzen $g(n) := m$. Dies definiert dann eine Funktion $g : N \to M$, und für alle $m \in M$ mit $f(m) = n$ gilt

$$(g \circ f)(m) = g(f(m)) = g(n) = m = \mathrm{Id}_M(m).$$

Daher gilt $g \circ f = \mathrm{Id}_M$.

„$\Longleftarrow$“: Nun gibt es nach Voraussetzung ein g mit $g \circ f = \mathrm{Id}_M$. Sind nun $m_1, m_2 \in M$ mit $f(m_1) = f(m_2)$, so folgt

$$m_1 = \mathrm{Id}_M(m_1) = (g \circ f)(m_1) = g(f(m_1)) = g(f(m_2)) = (g \circ f)(m_2) = \mathrm{Id}_M(m_2) = m_2,$$

also ist f injektiv.

(ii) „$\Longrightarrow$“: Hier ist f zunächst als surjektiv vorausgesetzt. Wir wählen[20] für jedes $n \in N$ ein $m \in M$ mit $f(m) = n$ und nennen dieses gewählte m geschickter Weise $h(n)$. Damit ist eine Abbildung $h : N \longrightarrow M$ ausgewählt, und für alle $n \in N$ gilt

$$(f \circ h)(n) = f(h(n)) = n = \mathrm{Id}_N(n),$$

also $f \circ h = \mathrm{Id}_N$.

„$\Longleftarrow$“: Nun nehmen wir an, wir hätten eine Abbildung h von N nach M mit $f \circ h = \mathrm{Id}_N$. Für jedes $n \in N$ gilt dann

$$n = \mathrm{Id}_N(n) = (f \circ h)(n) = f(h(n)),$$

und daher $h(n) \in f^{-1}[n]$, insbesondere $f^{-1}[n] \neq \emptyset$, und damit ist f surjektiv.

(iii) Die erste Aussage folgt direkt aus (i) und (ii), und es bleibt noch $g = h = f^{-1}$ zu zeigen. Zunächst gilt

$$g = g \circ \mathrm{Id}_N = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{Id}_M \circ h = h.$$

Für $n \in N$ ist $m := f^{-1}(n)$ das eindeutige Element von M mit $f(m) = n$. Nun gilt aber $f(h(n)) = (f \circ h)(n) = n$, also muss $m = h(n)$ gelten. Wir haben also gezeigt, dass $f^{-1}(n) = h(n)$ für jedes $n \in N$ gilt, und dies impliziert $f^{-1} = h$. □

[20] Wegen Surjektivität existieren Elemente von M mit der gewünschten Eigenschaft. Dass man unter allen diesen Elementen eines auswählen kann, scheint intuitiv klar. Es gibt aber Modelle der Mengenlehre, in denen man das nicht erlaubt. Wir arbeiten hier implizit mit einem Modell der Mengenlehre, in dem das sogenannte *Auswahlaxiom* als wahr angenommen ist.

Bemerkung 1.3.20. Eine Abbildung g wie in (i) (bzw. h wie in (ii)) heißt eine *Linksinverse* (bzw. *Rechtsinverse*) zu f. Ist f bijektiv, so ist die Umkehrfunktion also die eindeutige Linksinverse (und die eindeutige Rechtsinverse); im Allgemeinen kann eine injektive (bzw. surjektive) Funktion viele verschiedene Linksinverse (bzw. Rechtsinverse) haben.

Mittels Funktionen können wir nun auch kartesische Produkte mit mehr als zwei Faktoren definieren:

Definition 1.3.21. Sei I eine Menge und für jedes $i \in I$ sei X_i eine Menge. Dann heißt

$$\prod_{i\in I} X_i := \{f : I \to \bigcup_{i\in I} X_i \mid \forall\, i \in I : f(i) \in X_i\}$$

das *kartesische Produkt* der X_i über der *Indexmenge* I.

Bemerkung 1.3.22. Ist $I = \{1,2\}$, so erhalten wir eine Bijektion

$$\prod_{i\in\{1,2\}} X_i \to X_1 \times X_2, \quad f \mapsto (f(1), f(2)).$$

Wir können uns ein geordnetes Paar also als eine Abbildung auf der Menge $\{1,2\}$ vorstellen. In diesem Sinne ist Definition 1.3.21 eine Verallgemeinerung von Notation 1.3.1. Ist allgemeiner $I = \{1,\dots,n\}$, so können wir ein Element von $\prod_{i\in I} X_i$ mit dem geordneten n-Tupel $(f(1),\dots,f(n))$ identifizieren.

Zusammenfassung von Abschnitt 1.3

(1) Relationen und Funktionen erlauben es, Elemente verschiedener Mengen miteinander in Beziehung zu setzen.

(2) Funktionen mit passenden Definitions- und Wertebereichen können miteinander verkettet werden. Diese Verkettung (Komposition) ist assoziativ.

(3) Injektive/surjektive Funktionen haben ein Links-/Rechtsinverses bzgl. Komposition und bijektive Funktionen haben als eindeutiges beidseitiges Inverses die Umkehrfunktion.

1.4 Partitionen und Äquivalenzrelationen

In diesem Abschnitt seien M und N Mengen.

Definition 1.4.1. Sei $\mathscr{P} \subseteq \mathscr{P}(M)$ ein Mengensystem über M.

(i) $\mathscr{P}$ heißt *paarweise disjunkt*, falls für alle $A,B \in \mathscr{P}$ entweder $A = B$ oder $A \cap B = \emptyset$ gilt. In diesem Fall schreibt man auch

$$\bigsqcup \mathscr{P} := \bigcup \mathscr{P}$$

und nennt diese Menge die *disjunkte Vereinigung* von $\mathscr{P}$.

(ii) $\mathscr{P}$ heißt *Partition* von M, falls $\emptyset \notin \mathscr{P}$ gilt und $\mathscr{P}$ paarweise disjunkt ist mit $\bigsqcup \mathscr{P} = M$.

Im Folgenden sei $\mathscr{P}$ eine Partition von M.

Lemma 1.4.2. *Für jedes $x \in M$ existiert genau ein Element $A \in \mathscr{P}$ mit $x \in A$.*

Beweis. Die Existenz einer solchen Menge folgt aus $M = \bigcup \mathscr{P}$. Es seien nun $A, B \in \mathscr{P}$ mit $x \in A$ und $x \in B$. Dann ist $x \in A \cap B$, also $A \cap B \neq \emptyset$. Da $\mathscr{P}$ paarweise disjunkt ist, folgt $A = B$, also ist die Menge eindeutig. □

Notation 1.4.3. Ist $x \in M$, so bezeichne $[x]_{\mathscr{P}}$ das eindeutige Element von $\mathscr{P}$ mit $x \in [x]_{\mathscr{P}}$. Die Abbildung $\pi : M \to \mathscr{P}$, $x \mapsto [x]_{\mathscr{P}}$ heißt die *kanonische Projektion* zu $\mathscr{P}$. Wir sagen, $x, y \in M$ seien *$\mathscr{P}$-äquivalent*, falls $[x]_{\mathscr{P}} = [y]_{\mathscr{P}}$. Dies definiert eine Relation $R_{\mathscr{P}}$ auf M, genannt die *Äquivalenzrelation zu $\mathscr{P}$*.

Bemerkung 1.4.4 (Faserpartition)**.** Ist $p : M \to N$ eine beliebige surjektive Abbildung, so bilden die Fasern von N eine Partition $\mathscr{P}_p = \{p^{-1}[n] \mid n \in N\}$, genannt die *Faserpartition* zu p (Übung!). Die zugehörige Äquivalenzrelation R_p ist die sogenannte *Faserrelation*

$$x R_p y :\Leftrightarrow p(x) = p(y).$$

Es sei nun speziell $\pi : M \to \mathscr{P}$ die kanonische Projektion zu $\mathscr{P}$. Ist $A \in \mathscr{P}$, so ist $A \neq \emptyset$, also existiert ein $x \in A$. Es gilt dann $\pi(x) = A$, also $A \in \mathrm{Bild}(\pi)$, und daher ist π surjektiv. Nach Definition gilt weiter $\pi^{-1}[A] = \{x \in M \mid x \in A\} = A$, also ist $\mathscr{P}_\pi = \mathscr{P}$. Jede Partition ist also eine Faserpartition (nämlich zu ihrer kanonischen Projektion).

Bemerkung 1.4.5 (Repräsentantensystem)**.** Da die kanonische Projektion $\pi : M \to \mathscr{P}$ surjektiv ist, existiert eine Rechtsinverse $\sigma : \mathscr{P} \to M$. Das bedeutet gerade, dass $\sigma(A) \in A$ für alle $A \in \mathscr{P}$ gilt. Setzen wir $R := \mathrm{Bild}(\sigma)$, so gilt $A \cap R = \{\sigma(A)\}$ und daher $|A \cap R| = 1$ für alle $A \in \mathscr{P}$. Man nennt dann R ein *Repräsentantensystem* für $\mathscr{P}$ und $\sigma(A)$ den *Repräsentanten* von A in R. Ist $p := \pi|_R : R \to \mathscr{P}$ und $A \in \mathscr{P}$, so gilt $p^{-1}[A] = \pi^{-1}[A] \cap R = A \cap R = \{\sigma(A)\}$, insbesondere ist p bijektiv.

Wir illustrieren diese Begriffe anhand eines Beispiels aus der Geometrie:

Beispiel 1.4.6 (Parallelenschar)**.** Sei $\mathbf{E}$ die Anschauungsebene und $\ell \subseteq \mathbf{E}$ eine beliebige, aber fest gewählte Gerade. Die *Parallelenschar* zu ℓ ist definiert als das Mengensystem

$$\mathscr{P}_\ell := \{\ell' \in \mathscr{P}(\mathbf{E}) \mid \ell' \text{ ist parallele Gerade zu } \ell\}.$$

Das berühmte *Parallelenaxiom* der euklidischen[21] Geometrie besagt, dass es zu jeder Geraden $\ell \subseteq \mathbf{E}$ und jedem Punkt $p \in \mathbf{E}$ genau eine Gerade durch p gibt, die parallel zu ℓ liegt. Dies bedeutet gerade, dass das Mengensystem $\mathscr{P}_\ell$ für eine beliebige Gerade ℓ stets eine Partition von $\mathbf{E}$ ist. Die kanonische Projektion ordnet jedem $p \in \mathbf{E}$ die eindeutige Parallele ℓ_p zu ℓ durch p zu.

Wählen wir auf jeder Parallele zu ℓ einen beliebigen Punkt, so erhalten wir ein Repräsentantensystem. Dazu gibt es sehr viele Möglichkeiten. Ist z.B. $\ell' \subseteq \mathbf{E}$ eine beliebige nicht zu ℓ parallele[22] Gerade, so ist ℓ' ein Repräsentatensystem für $\mathscr{P}_\ell$.

[21] Euklid von Alexandria war ein griechischer Mathematiker (oder das Pseudonym einer Gruppe von Mathematikern), der (oder die) im 3. Jahrhundert v. Chr. in Alexandria in der 13-bändigen „Stoichea“ (dt. „Elemente“) das antike Wissen über Geometrie und Zahlentheorie zusammentrug(en). Das Buch wurde über 2000 Jahre lang bis ins frühe 20. Jahrhundert im Geometrieunterricht verwendet, und ist damit eines der einflussreichsten Lehrbücher der Menschheitsgeschichte.

[22] Nach unserer Konvention ist jede Gerade parallel zu sich selbst.

Um weitere Beispiele diskutieren zu können, brauchen wir eine effiziente Art um Partitionen zu definieren. Dazu verwenden wir die folgende Proposition[23].

Proposition 1.4.7. *Sei $\mathscr{P}$ eine Partition mit Äquivalenzrelation $R = R_{\mathscr{P}}$.*

(i) Für alle $x \in M$ gilt $[x]_{\mathscr{P}} = \{y \in M \mid xRy\}$.

(ii) Es gilt $\mathscr{P} = \{[x]_R \mid x \in M\}$.

Insbesondere ist $\mathscr{P}$ durch R eindeutig bestimmt.

Beweis. (i) „$\subseteq$“: Ist $y \in [x]_{\mathscr{P}}$, so gilt

$$y \in [x]_{\mathscr{P}} \cap [y]_{\mathscr{P}} \implies [x]_{\mathscr{P}} \cap [y]_{\mathscr{P}} \neq \emptyset \implies [x]_{\mathscr{P}} = [y]_{\mathscr{P}} \implies xRy.$$

„$\supseteq$“: Ist xRy, so gilt $[x]_{\mathscr{P}} = [y]_{\mathscr{P}}$. Wegen $y \in [y]_{\mathscr{P}}$ folgt $y \in [x]_{\mathscr{P}}$. (ii) Wegen $[x]_R = \pi(x)$ ist dies gerade die Surjektivität der kanonischen Projektion. □

Notation 1.4.8. Ist R eine beliebige Relation auf M, so setzen wir $[x]_R := \{y \in M \mid xRy\}$ und $M/R := \{[x]_R \mid x \in M\}$. Ist R die Äquivalenzrelation zu einer Partition $\mathscr{P}$, so ist nach Proposition 1.4.7 gerade $\mathscr{P} = M/R$. In diesem Fall nennt man $[x]_R$ auch die *Äquivalenzklasse* von x bzgl. R und M/R auch den *Quotienten* von M *modulo* R.

Es fragt sich nun, wie man einer Relation R ansehen kann, dass sie die Äquivalenzrelation zu einer Partition (nämlich M/R) ist.

Satz 1.4.9 (Charakterisierung von Äquivalenzrelationen)**.** *Sei R eine Relation auf M. Dann ist M/R genau dann eine Partition, wenn R die folgenden drei Bedingungen erfüllt:*

(Ä1) $\forall x \in M: xRx$. (Reflexivität)

(Ä2) $\forall x, y \in M: xRy \implies yRx$. (Symmetrie)

(Ä3) $\forall x, y, z \in M: (xRy \wedge yRz) \implies (xRz)$. (Transitivität)

In diesem Fall ist R gerade die Äquivalenzrelation zur Partition M/R.

Beweis. Wir zeigen zunächst, dass „M/R Partition“ $\iff$ „(Ä1), (Ä2), (Ä3)“.

„$\implies$“: Ist $\pi : M \to M/R$ die kanonische Projektion, so gilt $xRy \Leftrightarrow \pi(x) = \pi(y)$. Die Eigenschaften (Ä1)–(Ä3) folgen dann aus den entsprechenden Eigenschaften der Gleichheitsrelation.

„$\impliedby$“: Aus (Ä1) folgt, dass $x \in [x]_R$ für alle $x \in M$. Daraus folgt insbesondere, dass $\emptyset \notin M/R$ und $\bigcup M/R = M$. Es bleibt zu zeigen, dass

$$\forall\, x, y \in M: \quad [x]_R = [y]_R \quad \text{oder} \quad [x]_R \cap [y]_R = \emptyset. \tag{1.4.1}$$

Seien also $x, y \in M$ mit $[x]_R \cap [y]_R \neq \emptyset$. Wir können dann $z \in [x]_R \cap [y]_R$ wählen. Für alle $w \in [x]_R$ gilt dann:

$$(xRw) \wedge (xRz) \wedge (yRz) \overset{(Ä2)}{\implies} (wRx) \wedge (xRz) \wedge (zRy) \overset{(Ä3)}{\implies} (wRz) \wedge (zRy) \overset{(Ä3)}{\implies} wRy \overset{(Ä2)}{\implies} yRw \implies w \in [y]_R.$$

Dies zeigt $[x]_R \subseteq [y]_R$, und analog zeigt man $[y]_R \subseteq [x]_R$. Damit ist (1.4.1) bewiesen.

Dass R die Äquivalenzrelation zu M/R ist, folgt unmittelbar aus den Definitionen. □

[23] Eine Proposition ist eine einfache Beobachtung.

Eine reflexive, symmetrische und transitive Relation nennt man wegen Satz 1.4.9 auch kurz eine *Äquivalenzrelation*. Partitionen sind nach diesem Satz also genau die Quotienten von Mengen modulo solcher Äquivalenzrelationen.

Beispiel 1.4.10 (Gerade und ungerade Zahlen)**.** Auf $\mathbb{Z}$ definiert man eine Relation $\equiv_2$ durch

$$a \equiv_2 b \quad :\Longleftrightarrow \quad a - b \text{ ist gerade.}$$

Man überzeugt sich leicht, dass dies eine Äquivalenzrelation ist (Übung!), und der zugehörige Quotient besteht aus zwei Äquivalenzklassen, gegeben durch die Klasse der geraden Zahlen und die Klasse der ungeraden Zahlen. Zwei Repräsentatensysteme für den Quotienten $\mathbb{Z}/R_2$ sind z.B. {0,1} oder {17,34}.

Beispiel 1.4.11 (Kongruenzrechnung)**.** Allgemeiner definiert man für eine beliebige natürliche Zahl $n \in \mathbb{N}$ eine Äquivalenzrelation $\equiv_n$ auf $\mathbb{Z}$, genannt *Kongruenz modulo n*, durch

$$a \equiv_n b \quad :\Longleftrightarrow \quad a - b \text{ ist durch } n \text{ teilbar.}$$

Wir bezeichnen mit $[a]_n$ die Äquivalenzklasse von a bzgl. $\equiv_n$, also gilt z.B.

$$[1]_5 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}.$$

Die Klassen in $\mathbb{Z}/\equiv_n$ werden als *Restklassen modulo n* oder *arithmetische Progressionen von Schrittweite n* bezeichnet. {0,1,2,3,4} und $\{5, 11, 27, 3, 24\}$ sind zwei Repräsentantensysteme für $\equiv_5$, also

$$\mathbb{Z}/\equiv_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\} = \{[5]_5, [11]_5, [27]_5, [3]_5, [24]_5\}.$$

In den Übungen werden Sie zeigen, dass auf $\mathbb{Z}/\equiv_n$ eine Addition $\oplus$ und Multiplikation $\otimes$ definiert werden können mit der Eigenschaft, dass für alle $a, b \in \mathbb{Z}$ gilt

$$[a]_n \oplus [b]_n = [a + b]_n \quad \text{und} \quad [a]_n \otimes [b]_n = [a \cdot b]_n.$$

Für $n = 12$ oder $n = 24$ sind Sie mit dieser Art von Addition wohl vertraut (je nachdem, ob Sie eine Analoguhr oder Digitaluhr tragen).

Als eine erste Anwendung der bisher entwickelten Theorie zeigen wir, dass sich jede Abbildung kanonisch in eine surjektive, bijektive und injektive Abbildung zerlegen lässt. Diese einfache Beobachtung[24] spielt in der gesamten Algebra eine zentrale Rolle.

Konstruktion 1.4.12 (Kanonische Zerlegung einer Abbildung)**.** Sei $f : M \to N$ eine beliebige Abbildung. Die Abbildung $f|^{\mathrm{Bild}(f)} : M \to \mathrm{Bild}(f)$ ist dann surjektiv, und es bezeichne $R := R_f$ die in Bemerkung 1.4.4 definierte Faserrelation von $f|^{\mathrm{Bild}(f)}$. Nach Definition gilt dann für beliebige $x, y \in M$, dass

$$[x]_R = [y]_R \iff xRy \iff f(x) = f(y).$$

Wir können daher eine Abbildung definieren durch

$$\overline{f} : M/R \to \mathrm{Bild}(f), \quad [x]_R \mapsto f(x).$$

[24] Die sogenannten „Homomorphiesätze“ für Gruppen, Ringe, Körper, Vektorräume und viele weitere Strukturen beruhen allesamt auf dieser Beobachtung.

Nach Konstruktion ist diese Abbildung surjektiv, und für $x, y \in M$ gilt

$$\overline{f}([x]_R) = \overline{f}([y]_R) \Longrightarrow f(x) = f(y) \Longrightarrow xRy \Longrightarrow [x]_R = [y]_R,$$

also ist $\overline{f}$ auch injektiv und daher bijektiv.

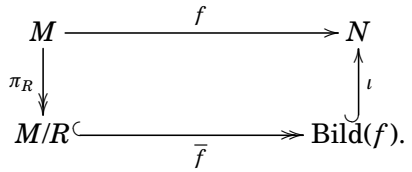
Sei nun weiter $\pi_R : M \to M/R$ die kanonische Projektion und $\iota : \mathrm{Bild}(f) \hookrightarrow N$ die Inklusion mit $\iota(n) = n$. Dann ist π_R surjektiv und ι injektiv, und für alle $x \in M$ gilt

$$\iota \circ \overline{f} \circ \pi_R(x) = \iota(\overline{f}([x]_R)) = \iota(f(x)) = f(x),$$

Dies zeigt, dass

$$f = \iota \circ \overline{f} \circ \pi_R, \tag{1.4.2}$$

d.h. das folgende Diagramm kommutiert:



Wir haben also eine beliebige Abbildung f in eine surjektive, eine bijektive und eine injektive Abbildung zerlegt.

Die Zerlegung in (1.4.2) heißt auch die *kanonische Zerlegung* der Abbildung f.

Beispiel 1.4.13. Wir betrachten die Abbildung $f : \{1,2,3,4,5,6,7\} \to \{1,2,3,4\}$ gegeben durch

$$f(1) := 2,\ f(2) := 3,\ f(3) := 1,\ f(4) := 3,\ f(5) := 2,\ f(6) := 1,\ f(7) := 3.$$

Es gilt dann $M/R = \{\{3,6\},\{1,5\},\{2,4,7\}\}$. Die Abbildung π_R ordnet jedem $x \in \{1,\dots 7\}$ diejenige dieser Mengen zu, die x enthät, und es gilt

$$\overline{f}(\{3,6\}) = 1, \quad \overline{f}(\{1,5\}) = 2 \quad \text{und} \quad \overline{f}(\{2,4,7\}) = 3.$$

Weiter ist ι die Inklusion $\{1,2,3\} \hookrightarrow \{1,2,3,4\}$.

Zusammenfassung von Abschnitt 1.4

(1) Partitionen sind Zerlegungen einer Menge in paarweise disjunkte nichtleere Teilmengen.

(2) Partitionen lassen sich durch zugehörige Äquivalenzrelationen beschreiben. Umgekehrt liefert jede Äquivalenzrelation auf einer Menge eine Partition, den sogenannten Quotienten nach dieser Relation.

(3) Jede Äquivalenzrelation induziert eine surjektive Abbildung, die zugehörige kanonische Projektion auf den Quotienten. Mittels solcher Projektionen lässt sich jede Abbildung kanonisch in je eine surjektive, bijektive und injektive Abbildung zerlegen.

1.5 Mengenvergleiche*

In diesem – rein optionalen[25], nicht klausurrelevanten – Abschnitt, wollen wir einen Ausblick auf einige fortgeschrittene Konzepte der Mengenlehre geben. Zur Motivation betrachten wir das folgende Beispiel:

Beispiel 1.5.1 (Was heißt eigentlich „gleich“ bzw. „vergleichen“?)**.** Wir betrachten die beiden in Abbildung 1.2 dargestellten Dreiecke in der Anschauungsebene: Als Teilmenge der Ebene sind diese beiden

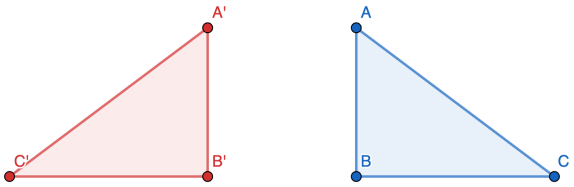


Abbildung 1.2: Zwei Dreiecke

Dreiecke sicher verschieden, und doch würde man sie für gewisse geometrische Probleme als äquivalent ansehen wollen. Das liegt daran, dass die beiden Dreiecke *kongruent* sind, dass es also eine bijektive euklidische Bewegung (in diesem Fall z.B. die Geradenspiegelung an der Mittelsenkrechten von A und A') gibt, die das eine Dreieck in das andere überführt.

Wie in diesem Beispiel interessiert es uns in vielen mathematischen Problemen eigentlich nicht, ob zwei gegebene mathematische Objekte *gleich* sind, sondern nur ob sie sich durch strukturerhaltende (im obigen Beispiel etwa längen- und winkeltreue) bijektive Abbildungen ineinander überführen lassen. Das führt auf den folgenden Begriff:

Definition 1.5.2. Eine *Kategorie* $\mathscr{C}$ besteht aus einer Klasse $\mathrm{Ob}(\mathscr{C})$ und für je zwei $X,Y \in \mathrm{Ob}(\mathscr{C})$ einer Menge $\mathrm{Mor}_{\mathscr{C}}(X,Y)$ von *Morphismen* sowie Abbildungen

$$\mathrm{Mor}_{\mathscr{C}}(Y,Z) \times \mathrm{Mor}_{\mathscr{C}}(X,Y) \to \mathrm{Mor}_{\mathscr{C}}(X,Z), \quad (f,g) \mapsto f \circ g$$

für alle $X,Y,Z \in \mathrm{Ob}(\mathscr{C})$, so dass die folgenden Axiome gelten:

(KAT 1) Für alle $W,X,Y,Z \in \mathrm{Ob}(\mathscr{C})$, $f \in \mathrm{Mor}_{\mathscr{C}}(Y,Z)$, $g \in \mathrm{Mor}_{\mathscr{C}}(X,Y)$ und $h \in \mathrm{Mor}_{\mathscr{C}}(W,X)$ gilt

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

(KAT 2) Für jedes $X \in \mathrm{Ob}(\mathscr{C})$ existiert ein $1_X \in \mathrm{Mor}_{\mathscr{C}}(X,X)$, so dass für alle $Y,Z \in \mathrm{Ob}(\mathscr{C})$ und $f \in \mathrm{Mor}_{\mathscr{C}}(X,Y)$ und $g \in \mathrm{Mor}_{\mathscr{C}}(Z,X)$ gilt

$$f \circ 1_X = f \quad \text{und} \quad 1_X \circ g = g.$$

Die Elemente von $\mathrm{Ob}(\mathscr{C})$ heißen die *Objekte* der Kategorie , und für $X,Y \in \mathrm{Ob}(\mathscr{C})$ heißen die Elemente von $\mathrm{Mor}_{\mathscr{C}}(X,Y)$ die *Morphismen* von X nach Y. Ein Morphismus $f \in \mathrm{Mor}_{\mathscr{C}}(X,Y)$ heißt ein *Isomorphismus*, falls ein $g \in \mathrm{Mor}_{\mathscr{C}}(Y,X)$ existiert mit $f \circ g = 1_Y$ und $g \circ f = 1_X$. Falls ein solcher existiert, sagen wir, dass X und Y in $\mathscr{C}$ *isomorph* (oder äquivalent) sind.

[25] Optionale Abschnitte sind hier und im Folgenden mit einem Stern gekennzeichnet.

Im obigen Beispiel könnten wir z.B. als Objekte die Dreiecke in der Ebene betrachten und als Morphismen von X nach Y die euklidischen Bewegungen (längen- und winkeltreue Abbildungen) zwischen X und Y. Zwei Dreiecke sind dann genau dann isomorph in dieser Kategorie, wenn sie kongruent sind.

Beispiel 1.5.3 (Kategorie der Mengen)**.** In diesem Kapitel haben wir gesehen, dass wir eine Kategorie[26] $\mathscr{S}$ erhalten, indem wir als Objektklasse die Klasse aller Mengen und als Morphismen zwischen zwei Mengen M und N die Menge $\mathrm{Abb}(M,N)$ der Abbildungen von M nach N betrachten, wobei 1_M die identische Abbildung auf M bezeichnet.

Nach Definition sind zwei Mengen M und N genau dann isomorph in dieser Kategorie (also als „äquivalent“ anzusehen), wenn es eine bijektive Abbildung $f : M \to N$ gibt. Man führt für diesen Äquivalenzbegriff, weil er so fundamental wichtig ist, eine eigene Sprechweise ein.

Definition 1.5.4. Zwei Mengen M und N heißen *gleichmächtig*, geschrieben $M \approx N$, falls eine bijektive Abbildung $f : M \to N$ existiert. Wir sagen, M ist *schmächtiger* als N (bzw. M ist *mächtiger* als N) falls eine injektive (bzw. surjektive) Abbildung $f : M \to N$ existiert. In diesem Fall schreiben wir $M \preceq N$ (bzw. $M \succeq N$).

Wir überlegen uns nun, was diese Sprechweise inhaltlich bedeutet.

Beispiel 1.5.5. Die Menge $\{1,2\}$ ist schmächtiger als $\{1,2,3\}$ aber mächtiger als $\{1\}$, wie man anhand der Inklusion $\{1,2\} \hookrightarrow \{1,2,3\}$ und der eindeutigen Surjektion $\{1,2\} \twoheadrightarrow \{1\}$ erkennt. Sie ist gleichmächtig zu $\{0,1\}$ wie man anhand von $f : \{1,2\} \to \{0,1\}$, $x \mapsto x-1$ erkennt.

Beispiel 1.5.6 (Endliche Menge)**.** Für endliche Mengen M und N gilt allgemein:

$$M \approx N \Leftrightarrow |M| = |N|, \quad M \preceq N \Leftrightarrow |M| \leq |N| \quad \text{und} \quad M \succeq N \Leftrightarrow |M| \geq |N|.$$

Diese Aussagen sollten sie nicht überraschen; um sie formal zu beweisen, müsste man zunächst einmal formal definieren, wann eine Menge endlich heißen soll, und was genau mit der „Anzahl der Elemente“ gemeint ist. Das wollen wir an dieser Stelle lieber nicht tun.

Beispiel 1.5.7 (Hilberts Hotel)**.** Es sei $M := \mathbb{N} \cup \{0\}$ und $N := \mathbb{N}$. Da die Abbildung $M \to N$, $x \mapsto x+1$ bijektiv ist, sind M und N gleichmächtig – und das, obwohl N eine echte Teilmeng von M ist (also $N \subsetneq M$ gilt). Es gibt also eine Menge M die „genauso groß“ ist, wie eine ihrer echten Teilmenge. In der modernen Mathematik nennt man eine Menge mit dieser Eigenschaft *unendlich*, und sagt, dass eine Menge *endlich* ist, wenn sie nicht unendlich ist.

Die Vorstellung unendlicher Mengen scheint paradox; DAVID HILBERT hat dieses scheinbare Paradoxon wie folgt veranschaulicht: In einem Hotel gibt es für jedes $n \in \mathbb{N} \cup \{0\}$ ein Bett, und alle Betten sind voll belegt. Um Mitternacht kommt noch ein weiterer Gast im Hotel an. Wenn nun alle Gäste ein Bett aufrücken, ist für den Neuankömmling noch ein Bett frei.

Übung 1.5.8. In welchem Sinne gibt es „genau so viele“ ungerade natürliche Zahlen wie natürliche Zahlen?

Aus Beispiel 1.5.6 sowie den entsprechenden Eigenschaften der natürlichen Zahlen und der 0 ergibt sich, dass für alle endlichen Mengen die folgenden Beziehungen gelten:

(M1) $M \preceq N \preceq O \implies M \preceq O$ und $M \succeq N \succeq O \implies M \succeq O$.

(M2) $M \preceq N \iff N \succeq M$.

(M3) $M \approx N \iff ((M \preceq N) \wedge (N \preceq M))$.

[26] $\mathscr{S}$ erinnert an das englische Wort „set“ für Menge

Gelten solche Eigenschaften auch noch für unendliche Mengen? Für Eigenschaft (M1) ist das noch relativ leicht zu sehen: Sind $f : M \to N$ und $g : N \to O$ injektive (bzw. surjektive Funktionen), so ist $g \circ f : M \to O$ injektiv (bzw. surjektiv). Am einfachsten sieht man das mit Satz 1.3.19: Sind f' und g' Linksinverse von f und g, so ist $f' \circ g'$ wegen

$$(f' \circ g') \circ (g \circ f) = f' \circ (g' \circ g) \circ f = f' \circ f = \mathrm{Id}_M$$

eine Linksinverse zu $g \circ f$, und analog für Rechtsinverse. Aussage (M2) folgt ebenfalls aus diesem Satz: Ist $M \preceq N$, so existiert eine injektive Abbildung $f : M \to N$, und diese besitzt eine Linksinverse $f' : N \to M$. Dann hat f' aber eine Rechtinverse, nämlich f, und ist daher surjektiv, und folglich $N \succeq M$. Die Gültigkeit der Aussage (M3) ist für unendliche Menge allerdings alles andere als klar; sie wurde erst 1897 von Cantors Student FELIX BERNSTEIN[27] bewiesen:

Satz 1.5.9 („Satz von Cantor-Schröder-Bernstein“)**.** *Für beliebige Mengen M und N gilt*

$$M \approx N \Longleftrightarrow ((M \preceq N) \wedge (N \preceq M)).$$

Übung 1.5.10. Folgern Sie aus Satz 1.5.9, dass (mit der aus der Analysis gewohnten Notation) $[0,1] \approx (0,1)$ gilt. Können Sie eine explizite Bijektion angeben?

Zum Beweis kann man den folgenden Satz verwenden:

Satz 1.5.11 (Fixpunktsatz von Tarski und Knaster)**.** *Ist $F : \mathscr{P}(M) \to \mathscr{P}(M)$ eine Funktion, sodass die Implikation $X \subseteq Y \Longrightarrow F(X) \subseteq F(Y)$ für alle $X, Y \in \mathscr{P}(M)$ gilt, so existiert ein $X_0 \in \mathscr{P}(M)$ mit $F(X_0) = X_0$.*

Beweis. Wir definieren $\mathscr{M} := \{X \in \mathscr{P}(M) \mid X \subseteq F(X)\}$ und definieren $X_0 := \bigcup \mathscr{M}$. Wir behaupten, dass dann $X_0 = F(X_0)$ gilt.

„$\subseteq$“: Ist $X \in \mathscr{M}$, so gilt $X \subseteq F(X)$ und wegen $X \subseteq X_0$ auch $F(X) \subseteq F(X_0)$. Daraus folgt

$$X_0 = \bigcup \{X \mid X \in \mathscr{M}\} \subseteq \bigcup \{F(X) \mid X \in \mathscr{M}\} \subseteq F(X_0).$$

„$\supseteq$“: Sei $X_1 := F(X_0)$; wir haben gezeigt, dass $X_0 \subseteq X_1$; daraus folgt nun $X_1 = F(X_0) \subseteq F(F(X_0)) = F(X_1)$. Dies zeigt aber, dass $X_1 \in \mathscr{M}$ und daher $X_1 \subseteq X_0$, also $F(X_0) \subseteq X_0$. □

Beweis von Satz 1.5.9. Es seien $f : M \to N$ und $g : N \to M$ injektive Abbildungen. Wir definieren

$$F : \mathscr{P}(M) \to \mathscr{P}(M), \quad F(X) := M \setminus g[N \setminus f[X]].$$

Sind nun $X_1 \subseteq X_2$ Teilmengen von M, so gilt $f[X_1] \subseteq f[X_2]$, also $N \setminus f[X_2] \subseteq N \setminus f[X_1]$ und daher $g[N \setminus f[X_2]] \subseteq g[N \setminus f[X_1]]$. Dies impliziert $F(X_1) \subseteq F(X_2)$. Es existiert also eine Teilmenge $M_1 \subseteq M$ mit $F(M_1) = M_1$, mit anderen Worten

$$M_1 = M \setminus g[N \setminus f[M_1]], \quad \text{und daher} \quad M \setminus M_1 = g[N \setminus f[M_1]]. \tag{1.5.1}$$

Setzen wir $M_2 := M \setminus M_1$, $N_1 := f[M_1]$ und $N_2 := N \setminus N_1$, so gilt $M = M_1 \sqcup M_2$ und $N = N_1 \sqcup N_2$, sowie

$$f[M_1] = N_1 \quad \text{und} \quad M_2 = g[N_2].$$

Da $h := g|_{N_2}^{M_2} : N_2 \to M_2$ surjektiv ist, besitzt h eine Rechtsinverse $f' : M_2 \to N_2$, die dann h als Linksinverse hat, und daher injektiv ist. Definieren wir nun

$$f'' : M \to N, \quad f''(m) := \begin{cases} f(m), & \text{falls } m \in M_1, \\ f'(m), & \text{falls } m \in M_2, \end{cases}$$

so ist f'' injektiv (da f und f' injektiv sind und $M_1 \cap M_2 . = \emptyset$ gilt) und surjektiv (da das Bild sowohl N_1 als auch N_2 enthält), also bijektiv. □

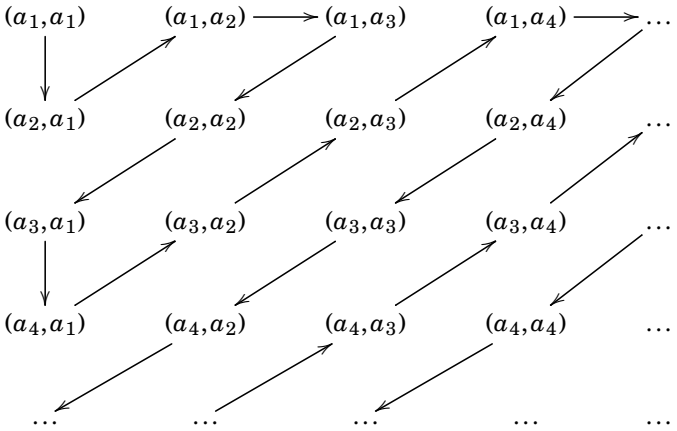
[27] Zur interessanten Geschichte und zum Namen dieses Satzes vgl. `https://www.youtube.com/watch?v=C1Zej87qvdg&t=1s&ab_channel=Weitz%2FHAWHamburg`

Definition 1.5.12. Eine Menge M heißt *abzählbar*, wenn sie schmächtiger als $\mathbb{N}$ ist. Sie heißt *abzählbar unendlich*, wenn sie gleichmächtig mit $\mathbb{N}$ ist.

Die folgenden Sätze werden (in leicht abgewandelter Form) in der ANALYSIS I bewiesen:

Satz 1.5.13 (1. Cantorsches Diagonalargument)**.** *Ist M abzählbar unendlich, so ist auch $M \times M$ abzählbar unendlich.*

Beweis. Es sei $f : \mathbb{N} \to M$ eine Bijektion und $a_n := f(n)$. Wir können dann die Paare (a_n, a_m) wie folgt durchnummerieren:



Wir senden also 1 auf (a_1, a_1), 2 auf (a_1, a_2), 3 auf (a_2, a_1) usw. □

Korollar 1.5.14. *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar unendlich.*

Satz 1.5.15 (2. Cantorsches Diagonalargument)**.** *Für jede Menge M gilt $M \not\approx \mathcal{P}(M)$. Speziell ist $\mathcal{P}(\mathbb{N})$ nicht abzählbar.*

Beweis. Wir führen einen Widerspruchsbeweis und nehmen dazu an, es gäbe eine surjektive Abbildung $f : M \to \mathcal{P}(M)$. Wir definieren dann eine Menge $N \in \mathcal{P}(M)$ durch[28] $N := \{x \in M \mid x \notin f(x)\}$. Da f surjektiv ist, müsste es dann ein $x_0 \in M$ geben mit $f(x_0) = N$. Nun gibt es zwei Möglichkeiten:

Ist $x_0 \in N$, so gilt $x_0 \in f(x_0)$, und daher $x_0 \notin N$, ein Widerspruch.

Ist dagegen $x_0 \notin N$, so ist $x_0 \notin f(x_0)$ und daher $x_0 \in N$, was ebenfalls ein Widerspruch ist. □

Korollar 1.5.16. *Die Menge $\mathbb{R}$ der reellen Zahlen ist nicht abzählbar.*

Übung 1.5.17. Zeigen Sie, dass es eine reelle Zahl x gibt, die nicht die Nullstelle einer Polynomfunktion mit rationalen Koeffizienten ist. Man nennt eine solche Zahl *transzendent*. [Anleitung: Zeigen Sie, dass es nur abzählbar viele solche Nullstellen gibt.]

[28] Die Parallele zur Russelschen Antinomie ist unverkennbar!

2 Von linearen Gleichungssystemen zu abstrakten Vektorräumen

[8.11.23]

2.1 Motivation: Lineare Gleichungssysteme in zwei Veränderlichen

In der Vorlesung ANALYSIS I haben Sie den vollständig-angeordneten Körper $\mathbb{R}$ der reellen Zahlen kennen gelernt. Wir setzen im Folgenden die grundlegenden Rechnenregeln für reelle Zahlen als bekannt voraus. Genauer benötigen wir hier nur die algebraischen Rechenregeln, also weder die Anordnungseigenschaften noch die Vollständigkeit von $\mathbb{R}$.

Definition 2.1.1. Es seien $a,b,c,d,e,f \in \mathbb{R}$. Das zugehörige *lineare Gleichungssystem (LGS)* in den zwei reellen Veränderlichen x_1 und x_2 ist die Aussageform

$$\mathscr{A}(x_1,x_2) \quad :\Longleftrightarrow \quad \left\{ \begin{array}{rcl} ax_1+bx_2 & = & e \\ cx_1+dx_2 & = & f \end{array} \right\}. \tag{2.1.1}$$

Aufhänger dieses Abschnitts ist das folgende Problem:

Problem 2.1.2. Man bestimme die *Lösungsmenge*

$$\mathscr{L}(a,b,c,d,e,f) := \{(x_1,x_2) \in \mathbb{R}\times\mathbb{R} \mid \mathscr{A}(x_1,x_2) \text{ ist wahr}\}$$

des LGS (2.1.1) für gegebene Parameter $a,b,c,d,e,f \in \mathbb{R}$.

Vermutlich haben Sie in der Schule bereits Verfahren kennengelernt, mit denen man Problem 2.1.2 für konkrete Wahlen der Parameter $a,b,c,d,e,f \in \mathbb{R}$ lösen kann. Einen echten Mathematiker können Sie damit aber nicht beeindrucken; es ist eben nur ein Spielzeugproblem, an dem sich allerdings einige wichtige Dinge lernen lassen. Aus mathematischer Sicht ist es vor allem interessant, ein allgemeines Verständnis und eine geometrische Anschauung für die dem Problem zugrundeliegenden abstrakten Strukturen zu erhalten, denn ein solches Verständnis erlaubt es, mit ähnlichen Methoden auch sehr viel kompliziertere Probleme zu lösen. Wenn man diese Strukturen einmal verstanden hat, ist es übrigens leicht, eine allgemeine Formel für die Lösungsmenge $\mathscr{L}(a,b,c,d,e,f)$ anzugeben; wir werden dies in Satz 2.1.47 tun.

Bemerkung 2.1.3 (Zahlenpaare als Vektoren)**.** Wir werden im Folgenden eine geometrische Reformulierung von Problem 2.1.2 ansteuern. Ausgangspunkt ist die Beobachtung, dass man jedem geordneten Paar $(x_1,x_2) \in \mathbb{R}\times\mathbb{R}$ eine Verschiebung der Anschauungsebene $\mathbb{E}^2$ zuordnen. Das Paar (x_1,x_2) korrespondiert dabei zu der Abbildung

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} : \mathbb{E}^2 \to \mathbb{E}^2,$$

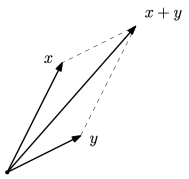
die jeden Punkt um x_1 nach rechts und x_2 nach oben verschiebt (bei negativem Vorzeichen in die entgegengesetzte Richtung). Eine solche Verschiebungsabbildung bezeichnet man als *Vektor*, und wir schreiben $\mathbb{R}^2$ für die Menge aller solcher Vektoren. Wir können einen Vektor durch einen[1] Pfeil in der Ebene visualisieren, der einen beliebigen Startpunkt in $\mathbb{E}^2$ mit seinem Bildpunkt verbindet. Die Verkettung von Vektoren ist wieder ein Vektor: Für $x_1, x_2, y_1, y_2 \in \mathbb{R}$ gilt

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \circ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix} =: \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Wir nennen die Abbildung

$$\mathrm{add} : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \mapsto x + y$$

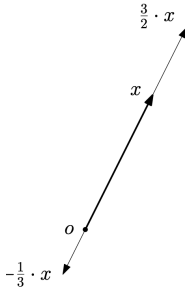
die *Vektoraddition*; die Kommutativität dieser Addition lässt sich durch das folgende Parallelogramm veranschaulichen.



Wir können Vektoren *skalieren*, indem wir die Verschiebungsrichtung beibehalten, aber die Verschiebungslänge mit einer nicht-negativen reellen Zahl λ (dem *Skalierungsfaktor* oder kurz *Skalar*) multiplizieren; in Formeln ist diese Skalierung durch

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

gegeben. Diese Formel ergibt auch für negative Werte von λ Sinn; in diesem Fall wird die Verschiebungsrichtung umgekehrt und um $|\lambda|$ skaliert.



Wir erhalten also eine *Skalarmultiplikation*

$$\mathrm{mult} : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2, \quad (\lambda, x) \mapsto \lambda \cdot x.$$

Den Punkt für die Skalarmultiplikation lässt man häufig weg und schreibt einfach λx statt $\lambda \cdot x$. Weitere häufige Abkürzungen sind

$$-y := (-1) \cdot y \quad \text{und} \quad x - y := x + (-y).$$

[1] Indem wir unterschiedliche Startpunkte wählen, erhalten wir unendlich viele Pfeile, die aber alle dieselbe Information tragen. In diesem Sinne können wir einen Vektor mit einer Äquivalenzklasse von Pfeilen identifizieren.

Wählen wir einen Punkt $P \in \mathbb{E}^2$, so erhalten wir eine Bijektion

$$\tau_P : \mathbb{R}^2 \to \mathbb{E}^2, \quad v \mapsto v(P);$$

wir können also Vektoren nach Wahl eines *Koordinatenursprungs* O via τ_O mit Punkten der Ebene identifizieren. Die Umkehrabbildung τ_O^{-1} ordnet jedem Punkt P die eindeutige Verschiebung zu, die O auf P abbildet, den sogenannten *Ortsvektor* zu P bzgl. O.

Im Folgenden werden wir meist[2] einen festen Koordinatenursprung O wählen und dann nicht zwischen dem Zahlenpaar (x_1, x_2), den Vektor $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ und dem Punkt $\tau_O(x)$ unterscheiden.

Bemerkung 2.1.4 (Historische Bemerkung)**.** Die für uns heute selbstverständliche Idee, Punkte der Ebene durch Paare reeller Zahlen zu beschreiben, war der antiken Mathematik vollkommen fremd und steht am Beginn der Renaissance. Sie wird häufig RENÉ DESCARTES zugeschrieben, weswegen man auch von *kartesischen Koordinaten* eines Punktes spricht.

Wir kehren nun zu unserem LGS zurück. Definieren wir eine Abbildung

$$\Phi : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}, \tag{2.1.2}$$

so gilt (unter der obigen Identifikation von $\mathbb{R} \times \mathbb{R}$ mit $\mathbb{R}^2$)

$$\mathscr{L}(a,b,c,d,e,f) = \Phi^{-1}\left[\begin{pmatrix} e \\ f \end{pmatrix}\right].$$

Wir können Problem 2.1.2 daher wie folgt umformulieren:

Problem 2.1.5. Man bestimme die Fasern der Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ aus (2.1.2).

Wir werden sehen, dass die Fasern von Φ entweder leer, ein Punkt, eine Gerade oder die ganze Ebene (aber z.B. kein Kreis und keine Parabel) sind. Der tiefere Grund dafür ist die folgende geometrische Eigenschaft von Φ:

Proposition 2.1.6 (Linearität)**.** *Die Abbildung* Φ *aus* (2.1.2) *hat die folgenden Eigenschaften:*

(L1) Für alle $\lambda \in \mathbb{R}$ *und* $x \in \mathbb{R}^2$ *gilt* $\Phi(\lambda x) = \lambda \Phi(x)$.

(L2) Für alle $x, y \in \mathbb{R}^2$ *gilt* $\Phi(x + y) = \Phi(x) + \Phi(y)$.

Beweis. Im Folgenden seien $\lambda \in \mathbb{R}$ und $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in \mathbb{R}^2$. Wir rechnen die Eigenschaften (L1) und (L2) nach:

$$\text{(L1)} \qquad \Phi(\lambda x) = \Phi\left(\begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix}\right) = \begin{pmatrix} a\lambda x_1 + b\lambda x_2 \\ c\lambda x_1 + d\lambda x_2 \end{pmatrix} = \begin{pmatrix} \lambda(ax_1 + bx_2) \\ \lambda(cx_1 + dx_2) \end{pmatrix} = \lambda \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} = \lambda \Phi(x).$$

$$\text{(L2)} \qquad \Phi(x + y) = \Phi\left(\begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}\right) = \begin{pmatrix} a(x_1 + y_1) + b(x_2 + y_2) \\ c(x_1 + y_1) + d(x_2 + y_2) \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} + \begin{pmatrix} ay_1 + by_2 \\ cy_1 + dy_2 \end{pmatrix} = \Phi(x) + \Phi(y). \qquad \square$$

Definition 2.1.7. Eine Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ heißt *linear*, falls Sie den Bedingungen (L1) und (L2) aus Proposition 2.1.6 genügt.

[2] Es gibt einige wenige Situationen, in denen man zwischen Punkten und ihren Ortsvektoren unterscheiden sollte, z.B. wenn man untersuchen will, wie sich Formeln unter Änderung des Koordinatenursprungs transformieren.

Übung 2.1.8 (Geometrie linearer Abbildungen)**.** Zeigen Sie, dass eine Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ genau dann linear ist, wenn für alle $\lambda, \mu \in \mathbb{R}$ und $x, y \in \mathbb{R}^2$ gilt:

$$\Phi(\lambda x + \mu y) = \lambda\Phi(x) + \mu\Phi(y).$$

Folgern Sie, dass eine lineare Abbildung Geraden auf Geraden oder Punkte und Parallelogramme auf Parallelogramme, Strecken oder Punkte abbildet.

Notation 2.1.9. Die lineare Abbildung Φ aus (2.1.2) ist festgelegt durch die vier Zahlen $a, b, c, d \in \mathbb{R}$. Es ist üblich, diese vier Zahlen in einem Quadrat

$$Q := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2.1.3}$$

anzuordnen. (Der Vorteil dieser Notation wird sich noch erweisen.) Dieses Quadrat heißt die *Matrix* der linearen Abbildung Φ; wir nennen eine solche Matrix eine „reelle (2×2)-Matrix“. Φ heißt dann auch die lineare Abbildung zur Matrix Q, und wir schreiben $\Phi_Q := \Phi$. Wir schreiben auch kurz

$$Qx := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x := \Phi_Q(x).$$

Im Folgenden bezeichnen wir mit $\mathbb{R}^{2\times 2}$ die Menge der reellen (2×2)-Matrizen, und mit $\mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$ die Menge der linearen Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$.

Unser nächstes Ziel ist der Beweis des folgenden Satzes:

Satz 2.1.10 (Klassifikation der linearen Abbildungen)**.** *Die Abbildung $\iota : \mathbb{R}^{2\times 2} \to \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$, $Q \mapsto \Phi_Q$ ist bijektiv, d.h. jede lineare Abbildung Φ ist von der Form $\Phi = \Phi_Q$ für eine eindeutig bestimmte Matrix Q.*

Zum Beweis benötigen wir die folgende Vorüberlegung:

Bemerkung 2.1.11 (Lineare Abbildungen und Standardbasis)**.** Es seien

$$e_1 := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{und} \quad e_2 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Das Paar (e_1, e_2) heißt die *Standardbasis* von $\mathbb{R}^2$. Ist $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ ein beliebiger Vektor in $\mathbb{R}^2$, so gilt

$$x = \begin{pmatrix} x_1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \end{pmatrix} = x_1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = x_1 e_1 + x_2 e_2.$$

Man sagt auch[3], x ist eine *Linearkombination* von e_1 und e_2 mit den *Koeffizienten* x_1 und x_2. Ist nun $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ eine beliebige lineare Abbildung, so gilt:

$$\Phi(x) = \Phi(x_1 e_1 + x_2 e_2) \overset{(L2)}{=} \Phi(x_1 e_1) + \Phi(x_2 e_2) \overset{(L1)}{=} x_1\Phi(e_1) + x_2\Phi(e_2).$$

Die lineare Abbildung Φ ist also durch die beiden Vektoren $\Phi(e_1)$ und $\Phi(e_2)$ bereits eindeutig bestimmt. Ist speziell $\Phi = \Phi_Q$ mit $Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, so gilt

$$\Phi_Q(e_1) = \begin{pmatrix} a \\ c \end{pmatrix} \quad \text{und} \quad \Phi_Q(e_2) = \begin{pmatrix} b \\ d \end{pmatrix}.$$

[3] Wir werden diese Begriffe später noch genauer diskutieren, für den Moment ist es nur eine Sprechweise.

Die Spalten von Q sind also genau die Bilder der Standardbasisvektoren, insbesondere ist Φ_Q durch Q eindeutig bestimmt.

Beweis von Satz 2.1.10. Injektivität folgt sofort aus Bemerkung 2.1.11. Für die Surjektivität sei Φ eine beliebige lineare Abbildung und es seien $a,b,c,d \in \mathbb{R}$ mit

$$\Phi(e_1) = \begin{pmatrix} a \\ c \end{pmatrix} \quad \text{und} \quad \Phi(e_2) = \begin{pmatrix} b \\ d \end{pmatrix}.$$

Wenn der Satz wahr sein soll[4], dann muss nach Bemerkung 2.1.11 schon $\Phi = \Phi_Q$ für Q wie in (2.1.3) gelten, und in der Tat rechnet man nach, dass wegen der Linearität von Φ für alle $x \in \mathbb{R}^2$ schon die folgende Gleichheit gilt:

$$\Phi(x) = \Phi(x_1 e_2 + x_2 e_2) = x_1\Phi(e_1) + x_2\Phi(e_2) = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} = \Phi_Q(x). \qquad \square$$

Definition 2.1.12. Die Matrix $D(\Phi) := \iota^{-1}(\Phi)$ aus Satz 2.1.10 heißt die *darstellende Matrix* von Φ bzgl. der Standardbasis.

Nach Bemerkung 2.1.11 gilt, $D(\Phi) = (\Phi(e_1)\ \Phi(e_2))$ und wegen Satz 2.1.10 können wir Problem (2.1.5) äquivalent wie folgt formulieren:

Problem 2.1.13. Man bestimme die Fasern einer beliebigen linearen Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$.

Wir betrachten zunächst einen Spezialfall:

Notation 2.1.14. Das LGS (2.1.1) heißt *homogen*, falls $e = f = 0$ gilt. Setzen wir $\mathbf{0} := \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und definieren Q wie in (2.1.3), so ist die Lösungsmenge des homogenen Systems gerade die Faser

$$\ker(\Phi_Q) := \Phi_Q^{-1}[\mathbf{0}],$$

genann der *Kern*[5] von Φ_Q.

Proposition 2.1.15 (Eigenschaften des Kerns)**.** *Es sei $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ eine lineare Abbildung und $W := \ker(\Phi)$. Dann gilt:*

(U1) $\mathbf{0} \in W$.

(U2) $\forall\, x, y \in W$*:* $x + y \in W$.

(U3) $\forall\, x \in W\ \forall\, \lambda \in \mathbb{R}$*:* $\lambda x \in W$.

Beweis. (U1) Es gilt $\Phi(\mathbf{0})+\Phi(\mathbf{0}) = \Phi(\mathbf{0}+\mathbf{0}) = \Phi(\mathbf{0})$, und die Subtraktion von $\Phi(\mathbf{0})$ auf beiden Seiten liefert $\Phi(\mathbf{0}) = \mathbf{0}$, also $\mathbf{0} \in W$.
(U2) Für $x, y \in W$ gilt $\Phi(x + y) = \Phi(x) + \Phi(y) = \mathbf{0} + \mathbf{0} = \mathbf{0}$, also $x + y \in W$.
(U3) Für $x \in W$ und $\lambda \in \mathbb{R}$ gilt $\Phi(\lambda x) = \lambda\Phi(x) = \lambda\mathbf{0} = \mathbf{0}$, also $\lambda x \in W$. $\square$

Definition 2.1.16. Eine Teilmenge $W \subseteq \mathbb{R}^2$ heißt ein *Untervektorraum* (geschrieben $W \leq \mathbb{R}^2$), wenn sie (U1)–(U3) erfüllt.

[4] Ein solches Gedankenspiel, bei dem man zunächst die Wahrheit des zu zeigenden annimmt und sich überlegt, was dann gelten muss, bezeichnet man als *Heuristik*.

[5] Ist $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ eine beliebige lineare Abbildung, so nennt man analog $\ker(\Phi) := \Phi^{-1}[\mathbf{0}]$ den *Kern* von Φ.

Übung 2.1.17. Zeigen Sie: $W \subseteq \mathbb{R}^2$ ist genau dann ein Untervektorraum, wenn $W \neq \emptyset$ und $\lambda x + \mu y \in W$ für alle $\lambda, \mu \in \mathbb{R}$ und $x, y \in W$ gilt.

Beispiel 2.1.18 (Ursprungsgeraden)**.** Ist $x \in \mathbb{R}^2$, so ist $\mathbb{R}x := \{\lambda x \mid \lambda \in \mathbb{R}\}$ ein Untervektorraum, genannt die *Ursprungsgerade* durch x.

Welche weiteren offensichtlichen Beispiele für Untervektorräume gibt es? Offensichtlich sind auch $\{\mathbf{0}\}$ und $\mathbb{R}^2$ Untervektorräume sind; das sind dann aber auch schon alle Beispiele:

Satz 2.1.19 (Klassifikation der Untervektorräume)**.** *Die Untervektorräume des $\mathbb{R}^2$ sind genau die folgenden Teilmengen:*

(0) Der Nullvektorraum $\{\mathbf{0}\}$*, der nur aus einem Punkt besteht. („0-dimensional“)*

(1) Die Ursprungsgeraden $\mathbb{R}x$ mit $x \in \mathbb{R}^2$. („1-dimensional“)

(2) Die Ebene $\mathbb{R}^2$ selbst. („2-dimensional“)

Insbesondere ist die Lösungsmenge jedes homogenen LGS von dieser Form.

Beweis. Es sei W ein Untervektorraum des $\mathbb{R}^2$, der weder der Nullvektorraum noch eine Ursprungsgerade ist. Wir zeigen, dass $W = \mathbb{R}^2$ gilt.

Nach Annahme existieren zwei Vektoren $x, y \in W$ mit $x \neq \lambda y$ für alle $\lambda \in \mathbb{R}$. Insbesondere gilt $x \neq \mathbf{0}$, also entweder $x_1 \neq 0$ oder $x_2 \neq 0$. Wir nehmen an, dass $x_1 \neq 0$ gilt; den analogen Fall $x_2 \neq 0$ überlassen wir Ihnen zur Übung. Es gilt dann $y_1 = \lambda x_1$ für ein $\lambda \in \mathbb{R}$, und wir definieren

$$z := x - \lambda y = \begin{pmatrix} 0 \\ z_2 \end{pmatrix}.$$

Wegen $x \neq \lambda y$ ist $z_2 \neq 0$, und daher ist $e_2 = z_2^{-1} \cdot z \in W$. Dann ist aber auch

$$e_1 = x_1^{-1} \begin{pmatrix} x_1 \\ 0 \end{pmatrix} = x_1^{-1}(x - x_2 \cdot e_2) \in W.$$

Da jeder Vektor $w \in \mathbb{R}^2$ als $w = w_1 e_1 + w_2 e_2$ geschrieben werden kann, ist dann schon $W = \mathbb{R}^2$. □

Damit ist die „Struktur“ und „Geometrie“ der Lösungsmengen homogener LGSe vollständig beschrieben. Wir wollen nun in ähnlicher Weise auch Lösungsmengen nicht-homogener Systeme beschreiben.

Bemerkung 2.1.20 (Affine Unterräume)**.** Wir haben Vektoren als Verschiebungen der Anschauungsebene $\mathbb{E}^2$ definiert. Ist $W \subseteq \mathbb{R}^2$ ein Untervektorraum und $P \in \mathbb{E}^2$, so nennen wir die Teilmenge $W_P := \{w(P) \mid w \in W\} \subseteq \mathbb{E}^2$ einen *affinen Unterraum* von $\mathbb{E}^2$. Ist z.B. W eine Ursprungsgerade, so ist W_P die zu W parallele Gerade durch P. Für $v \in \mathbb{R}^2$ gilt dann (Übung!)

$$v \in W \iff v(P) \in W_P \iff \forall\, Q \in W_P : v(Q) \in W_P \iff \exists\, Q \in W_P : v(Q) \in W_P. \tag{2.1.4}$$

Wir nennen daher W den *Verschiebungsvektorraum* von W_P; dieser ist wegen (2.1.4) durch W_P eindeutig bestimmt. Wir nennen zwei affine Unterräume *parallel* wenn sie denselben Verschiebungsvektorraum haben. Die zu W parallelen affinen Unterräume von $\mathbb{E}^2$ bilden eine Partition, genannt die *Parallelenschar* zu W.

Wenn wir wie üblich $\mathbb{E}^2$ durch Wahl eines Koordinatenursprungs O mit $\mathbb{R}^2$ identifizieren, dann entspricht der affine Unterraum W_P genau der Teilmenge

$$x + W := \{x + w \mid w \in W\} \subseteq \mathbb{R}^2,$$

wobei x der Ortsvektor von P ist. Wir nennen dann auch $x + W$ einen *affinen Unterraum* von $\mathbb{R}^2$, und wir können W aus $x + W$ als die Menge der Differenzenvektoren zurückgewinnen. Die Partition

$$\mathbb{R}^2/W := \{x + W \mid x \in \mathbb{R}^2\}$$

von $\mathbb{R}^2$ heißt dann ebenfalls die *Parallelenschar* zu W. Ist W eine Ursprungsgerade, so erhalten wir eine Partition der „Lasagne-Platte“ $\mathbb{R}^2$ in parallele „Spaghetti“. Ein Repräsentantensystem ist durch eine beliebige zu W nicht-parallele Gerade gegeben.

Wegen Fakt 2.1.19 sind die affinen Unterräume von $\mathbb{R}^2$ gerade die einelementigen Mengen (Parallelen zu $\{\mathbf{0}\}$), die Geraden (Parallelen von Ursprungsgeraden) und die Ebene.

Satz 2.1.21 (Fasern linear Abbildungen)**.** *Es sei* $\Phi \in \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$ *und* $y \in \mathbb{R}^2$*. Dann gilt:*

(i) Ist $y \notin \mathrm{Bild}(\Phi)$*, so ist* $\Phi^{-1}[y] = \emptyset$*.*

(ii) Ist $y \in \mathrm{Bild}(\Phi)$*, so existiert* $x_0 \in \Phi^{-1}[y]$*, und für jedes solche* x_0 *ist*

$$\Phi^{-1}[y] = x_0 + \ker(\Phi)$$

ein affiner Unterraum parallel zu $\ker(\Phi)$*.*

Insbesondere sind die nicht-leeren Fasern einer linearen Abbildung zueinander parallele affine Unterräume.

Beweis. (i) gilt nach Definition. (ii) Nach Definition existiert ein $x_0 \in \Phi^{-1}[y]$, und für $x \in \mathbb{R}^2$ gilt

$$\begin{aligned} x \in \Phi^{-1}[y] &\iff \Phi(x) = y \iff \Phi(x) = \Phi(x_0) \iff \Phi(x) + (-1)\Phi(x_0) = 0 \\ &\overset{\text{(L1)}}{\iff} \Phi(x) + \Phi((-1)x_0) = 0 \overset{\text{(L2)}}{\iff} \Phi(x + (-1)x_0) = 0 \\ &\iff x - x_0 \in \ker(\Phi) \iff x \in x_0 + \ker(\Phi). \quad \square \end{aligned}$$

Korollar 2.1.22. *Die kanonische Zerlegung einer linearen Abbildung* $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ *ist von der Form*

$$\begin{array}{ccc} \mathbb{R}^2 & \xrightarrow{\Phi} & \mathbb{R}^2 \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ \mathbb{R}^2/\ker(\Phi) & \xrightarrow{\overline{\Phi}} & \mathrm{Bild}(\Phi). \end{array}$$

In die Sprache der LGSe zurückübersetzt besagt dies:

Korollar 2.1.23 (Lösungsmengen linearer Gleichungssyteme)**.** *Die Lösungsmenge eines LGS ist entweder leer oder ein affiner Unterraum parallel zur Lösung der zugehörigen homogenen LGS.*

Um die Lösungsmenge eines LGS zu bestimmen, muss man also eine spezielle Lösung finden und zu dieser dann alle möglichen Lösungen des zugehörigen homogenen LGS addieren. Dies klärt die Frage nach der Struktur und Geometrie der Lösungsmenge eines LGS, und wir wenden uns nun der Frage zu, wie man diese praktisch bestimmen kann. Im Hinblick auf spätere Verallgemeinerungen nehmen wir wieder eine abstrakte Sichtweise ein. In der Schule haben Sie vielleicht gelernt, dass man ein LGS durch „elementare Umformungen“ lösen kann. Abstrakt gesehen sind solche Umformungen Anwendungen bijektiver linearer Abbildungen.

Bemerkung 2.1.24. Für alle $\Phi, \Psi \in \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$ und $x, y \in \mathbb{R}^2$ gilt

$$\Phi(x) = y \quad \Longrightarrow \quad \Psi \circ \Phi(x) = \Psi(y).$$

Ist Ψ *bijektiv*, so gilt auch die Umkehrung, d.h.

$$\Phi(x) = y \quad \Longleftrightarrow \quad \Psi \circ \Phi(x) = \Psi(y). \tag{2.1.5}$$

Wir können nämlich in diesem Fall die Umkehrabbildung Ψ^{-1} auf die rechte Gleichung anwenden und erhalten (wegen Lemma 1.3.17)

$$y = \Psi^{-1}(\Psi(y)) = (\Psi^{-1} \circ (\Psi \circ \Phi))(x) = ((\Psi^{-1} \circ \Psi) \circ \Phi)(x) = \Phi(x).$$

Lemma 2.1.25 (Verkettung linearer Abbildungen)**.** *Seien* $\Phi, \Psi \in \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$.

(i) $\Psi \circ \Phi$ *ist linear.*

(ii) Ist Ψ *bijektiv, so ist auch* Ψ^{-1} *linear.*

Beweis. (i) Für alle $x, y \in \mathbb{R}^2$ und $\lambda \in \mathbb{R}$ gilt

$$\begin{aligned}(\Psi \circ \Phi)(\lambda x) &= \Psi(\Phi(\lambda x)) = \Psi(\lambda \Phi(x)) = \lambda \Psi(\Phi(x)) = \lambda(\Psi \circ \Phi)(x),\\ (\Psi \circ \Phi)(x + y) &= \Psi(\Phi(x) + \Phi(y)) = \Psi(\Phi(x)) + \Psi(\Phi(y)) = (\Psi \circ \Phi)(x) + (\Psi \circ \Phi)(y),\end{aligned}$$

also ist $\Psi \circ \Phi$ linear.

(ii) Es seien x, y, λ wie in (i) und $x' := \Psi^{-1}(x)$ und $y' := \Psi^{-1}(y)$; dann gilt

$$\begin{aligned}\Psi(\lambda x') = \lambda \Psi(x') = \lambda x \quad &\Longrightarrow \quad \Psi^{-1}(\lambda x) = \lambda x' = \lambda \Psi^{-1}(x),\\ \Psi(x' + y') = \Psi(x') + \Psi(y') = x + y \quad &\Longrightarrow \quad \Psi^{-1}(x + y) = x' + y' = \Psi^{-1}(x) + \Psi^{-1}(y),\end{aligned}$$

also ist Ψ^{-1} linear. □

Mit (2.1.5) folgt, dass das Anwendungen bijektiver lineare Abbildungen eine Äquivalenzumformung im folgenden Sinne ist:

Korollar 2.1.26 (Äquivalente LGSe)**.** *Ist* $\Psi \in \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$ *bijektiv, so ist das LGS* $\mathscr{A}_{\Phi, y}(x)$ *äquivalent zum LGS* $\mathscr{A}_{\Psi \circ \Phi, \Psi(y)}(x)$.

Bemerkung 2.1.27 (Matrizenmultiplikation)**.** Seien $\Phi, \Psi \in \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$. Nach Lemma 2.1.25 ist dann auch $\Psi \circ \Phi$ linear und korrespondiert nach Bemerkung 2.1.11 zu einer Matrix $D(\Psi \circ \Phi)$. Da die Abbildung $D : \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2) \to \mathbb{R}^{2\times 2}$ bijektiv ist, können wir eine Abbildung definieren durch

$$\mu : \mathbb{R}^{2\times 2} \times \mathbb{R}^{2\times 2} \to \mathbb{R}^{2\times 2}, \quad (A, B) \mapsto AB := D(\Phi_A \circ \Phi_B).$$

Diese ist gerade so gemacht, dass

$$D(\Psi \circ \Phi) = D(\Psi)D(\Phi) \tag{2.1.6}$$

gilt und heißt *Matrizenmultiplikation*. Da die Verkettung von Abbildungen assoziativ ist (Lemma 1.3.17), ist auch die Matrizenmultiplikation assoziativ, d.h. $(AB)C = A(BC)$ für alle $A, B, C \in \mathbb{R}^{2\times 2}$. Um eine explizite Formel für die Matrizenmultiplikation zu finden, seien $\Phi, \Psi \in \mathrm{Lin}(\mathbb{R}^2, \mathbb{R}^2)$ mit darstellenden Matrizen

$$D(\Psi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{und} \quad D(\Phi) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Es gilt

$$(\Psi \circ \Phi)(e_1) = \Psi(\Phi(e_1)) = \Psi\left(\begin{pmatrix} a' \\ c' \end{pmatrix}\right) = \begin{pmatrix} aa' + bc' \\ ca' + dc' \end{pmatrix},$$
$$(\Psi \circ \Phi)(e_2) = \Psi(\Phi(e_2)) = \Psi\left(\begin{pmatrix} b' \\ d' \end{pmatrix}\right) = \begin{pmatrix} ab' + bd' \\ cb' + dd' \end{pmatrix},$$

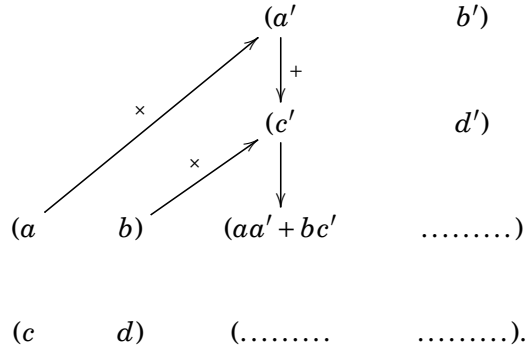
und wegen Bemerkung 2.1.11 folglich

$$D(\Psi \circ \Phi) = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Wir haben also gezeigt, dass Matrizenmultiplikation durch die Formel

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

gegeben ist. Man kann sich die Formel wie folgt veranschaulichen:



Caveat 2.1.28. Die Matrizenmultiplikation ist (assoziativ aber) **nicht** kommutativ, d.h. es gibt Matrizen $A, B \in \mathbb{R}^{2\times 2}$ mit $AB \neq BA$, z.B. gilt

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

[10.11.23]

Bemerkung 2.1.29 (Invertierbarkeit)**.** Eine Matrix $A \in \mathbb{R}^{2\times 2}$ heißt *invertierbar*, falls $\Phi := \Phi_A$ bijektiv ist. In diesem Fall heißt $A^{-1} := D(\Phi^{-1})$ die zu A *inverse Matrix*. Bezeichnet

$$\mathbf{1} := D(\mathrm{Id}_{\mathbb{R}^2}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.1.7}$$

die *Einheitsmatrix*, so ist A nach Satz 1.3.19 genau dann invertierbar, falls es Matrizen $B, C \in \mathbb{R}^{2\times 2}$ gibt mit $AB = \mathbf{1} = CA$, und in diesem Fall gilt $B = C = A^{-1}$.

Übung 2.1.30 (Produkte invertierbarer Matrizen)**.** Zeigen Sie: Sind $A, B \in \mathbb{R}^{2\times 2}$ zwei invertierbare Matrizen, so ist auch AB invertierbar mit $(AB)^{-1} = B^{-1}A^{-1}$.

Bemerkung 2.1.31. Wir betrachten nun eine Reihe wichtiger Beispiele von Matrizen A; wir fragen uns jeweils:

- Wie sieht die zugehörige lineare Abbildung Φ_A aus? Was macht diese Abbildung geometrisch?
- Was passiert mit einer Matrix Q, wenn man sie von links oder von rechts mit A multipliziert?
- Ist die Matrix A invertierbar? Wie sieht ggf. die Inverse aus? (Hierzu verwenden wir das Kriterium aus Bemerkung 2.1.29.)

Im Folgenden sei Q stets wie in (2.1.3) gegeben.

Beispiel 2.1.32 (Einheitsmatrix)**.** Die Einheitsmatrix $\mathbf{1}$ aus (2.1.7) entspricht der identischen Abbildung, insbesondere gilt $\mathbf{1}Q = Q\mathbf{1}$. Sie ist *selbst-invers*, also invertierbar mit $\mathbf{1}^{-1} = \mathbf{1}$.

Beispiel 2.1.33 (Permutationsmatrix)**.** Die Matrix $P_{12} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ erfüllt die Rechenregeln

$$P_{12}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} P_{12} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

Links- bzw. Rechtsmultiplikation mit P_{12} entspricht also Zeilen- bzw. Spaltenvertauschung, weswegen P_{12} auch eine *Permutationsmatrix*[6] heißt. Speziell gilt $P_{12}P_{12} = \mathbf{1}$, also ist P_{12} selbstinvers. Weiter gilt

$$\Phi_{P_{12}}(x) = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix},$$

was geometrisch einer Spiegelung an der Ursprungsgeraden $\mathbb{R}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ entspricht.

Beispiel 2.1.34 (Diagonalmatrix)**.** Für $\lambda, \mu \in \mathbb{R}$ heißt die Matrix

$$\mathrm{diag}(\lambda, \mu) := \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

[6] lat. permutare = vertauschen

eine *Diagonalmatrix*. Es gilt

$$\operatorname{diag}(\lambda,\mu)\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}\lambda a & \lambda b\\ \mu c & \mu d\end{pmatrix} \quad \text{und} \quad \begin{pmatrix}a & b\\ c & d\end{pmatrix}\operatorname{diag}(\lambda,\mu) = \begin{pmatrix}\lambda a & \mu b\\ \lambda c & \mu d\end{pmatrix}.$$

Links- und Rechtsmultiplikation multipliziert also die Zeilen bzw. Spalten mit den entsprechenden Skalaren. Speziell gilt

$$\operatorname{diag}(\lambda,\mu)\operatorname{diag}(\lambda',\mu') = \operatorname{diag}(\lambda\lambda',\mu\mu'),$$

also ist $\operatorname{diag}(\lambda,\mu)$ genau dann invertierbar, wenn $\lambda \neq 0 \neq \mu$, und in diesem Fall ist

$$\operatorname{diag}(\lambda,\mu)^{-1} = \operatorname{diag}(\lambda^{-1},\mu^{-1}).$$

Weiter gilt

$$\Phi_{\operatorname{diag}(\lambda,\mu)}(x) = \begin{pmatrix}\lambda x_1\\ \mu x_2\end{pmatrix}$$

Für $\lambda,\mu > 0$ ist die zugehörige lineare Abbildung eine Streckung oder Stauchung um den Faktor λ bzw. μ in die beiden Koordinatenrichtungen. Die Abbildungen $\operatorname{diag}(1,-1)$ bzw. $\operatorname{diag}(-1,1)$ entsprechen Spiegelungen an den Koordinatenachsen; allgemeine Diagonalmatrizen entsprechen daher Kombinationen von Streckungen/Stauchungen und Spiegelungen.

Beispiel 2.1.35 (Unipotente Elementarmatrix)**.** Für $t \in \mathbb{R}$ betrachten wir nun die sogenannten *unipotenten Elementarmatrizen*

$$U_{12}(t) := \begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} \quad \text{und} \quad U_{21}(t) := \begin{pmatrix}1 & 0\\ t & 1\end{pmatrix}.$$

Es gilt dann

$$U_{12}(t)Q = \begin{pmatrix}a+tc & b+td\\ c & d\end{pmatrix} \quad \text{und} \quad QU_{12}(t) = \begin{pmatrix}a & b+ta\\ c & d+tc\end{pmatrix}$$

Man beachte: Bei Multiplikation von $U_{12}(t)$ von links wird die ein Vielfaches der *zweiten* Zeile zur *ersten* addiert, bei Multiplikation von rechts aber ein Vielfaches der *ersten* Spalte zur *zweiten* Spalte! Analog gilt

$$U_{21}(t)Q = \begin{pmatrix}a & b\\ c+ta & d+tb\end{pmatrix} \quad \text{und} \quad QU_{21}(t) = \begin{pmatrix}a+tb & b\\ c+td & d\end{pmatrix}.$$

Für $(i,j) \in \{(1,2),(2,1)\}$ gilt insbesondere

$$U_{ij}(s)U_{ij}(t) = U_{ij}(s+t), \quad \text{und daher} \quad U_{ij}(t)^{-1} = U_{ij}(-t).$$

Unipotente Elementarmatrizen sind also stets invertierbar. Die linearen Abbildungen

$$\Phi_{U_{12}(t)}(x) = \begin{pmatrix}x_1+tx_2\\ x_2\end{pmatrix} \quad \text{und} \quad \Phi_{U_{21}(t)}(x) = \begin{pmatrix}x_1\\ x_2+tx_1\end{pmatrix}$$

sind sogenannte *Scherungen*, vgl. die nachfolgende Übung.

Übung 2.1.36 (Elementarmatrizen und Rechtecke)**.** Die folgende Übung soll Ihnen eine bessere geometrische Vorstellung für unipotente Elementarmatrizen geben.

(a) Beschreiben Sie den Effekt der linearen Abbildungen $\Phi_{U_{12}(t)}$ und $\Phi_{U_{21}(t)}$ auf ein achsenparalleles Rechteck. Wie ändert sich der Flächeninhalt?

(b) Beschreiben Sie analog das Bild eines achsenparallelen Rechtecks unter einer linearen Abbildung der Form $\Phi_{\mathrm{diag}(\lambda,\mu)}$ mit $\lambda,\mu \in \mathbb{R}$. Wie ändert sich der Flächeninhalt in diesem Fall?

Definition 2.1.37. Eine Matrix $A \in \mathbb{R}^{2\times 2}$ heißt *Elementarmatrix*, wenn sie die Einheitsmatrix, die Permutationsmatrix, eine Diagonalmatrix oder eine unipotente Elementarmatrix ist.

Wir betrachten nun noch zwei weitere Arten von Matrizen, die geometrisch bedeutsam, aber für lineare Gleichungssysteme nicht unmittelbar relevant sind.

Übung 2.1.38 (Drehungen)**.** In dieser Übung werden Sie zeigen, dass Drehungen um den Koordinatenursprung lineare Abbildungen sind.

(a) Zeigen Sie: Jeder Vektor $x \in \mathbb{R}^2$ kann geschrieben werden als

$$x = r\begin{pmatrix}\cos(\theta)\\ \sin(\theta)\end{pmatrix}$$

für ein eindeutiges $r \in [0,\infty)$ und ein $\theta \in [0,2\pi)$. Ist $r \neq 0$, so ist θ eindeutig. Was ist die geometrische Bedeutung von r und θ?

(b) Für $t \in \mathbb{R}$ heißt die Abbildung

$$\rho_t : \mathbb{R}^2 \to \mathbb{R}^2, \quad r\begin{pmatrix}\cos(\theta)\\ \sin(\theta)\end{pmatrix} \mapsto r\begin{pmatrix}\cos(\theta+t)\\ \sin(\theta+t)\end{pmatrix}$$

die *Drehung* um den Winkel t. Zeigen Sie, dass ρ_t wohldefiniert und linear ist mit darstellender Matrix

$$R_t := \begin{pmatrix}\cos(t) & -\sin(t)\\ \sin(t) & \cos(t)\end{pmatrix}. \tag{2.1.8}$$

Beispiel 2.1.39 (Drehmatrizen)**.** Ist R_t die Drehmatrix aus (2.1.8), so gilt (nach den Additionstheoremen für Sinus und Kosinus), dass $R_s R_t = R_{st}$, wie geometrisch zu erwarten ist. Insbesondere sind Drehmatrizen invertierbar mit $R_t^{-1} = R_{-t}$.

Übung 2.1.40 (Spiegelungen)**.** Wir erinnern daran, dass die Matrix $S := \mathrm{diag}(1,-1)$ einer Spiegelung an der x_1-Achse entspricht. Weiter sei R_t die Drehmatrix aus Übung 2.1.38.

(i) Machen Sie sich klar, dass die lineare Abbildung mit darstellender Matrix $A_t := R_t S R_{-t}$ ebenfalls eine Spiegelung ist. Wie lautet die Spiegelungsachse?

(ii) Rechnen Sie nach, dass

$$S_t = \begin{pmatrix}\cos(2t) & \sin(2t)\\ \sin(2t) & -\cos(2t)\end{pmatrix}. \tag{2.1.9}$$

Beispiel 2.1.41 (Spiegelungsmatrix)**.** Die Spiegelungsmatrix A_t aus (2.1.9) ist selbstinvers; dies ist geometrisch offensichtlich und folgt rechnerisch aus der Gleichung $\cos^2(x) + \sin^2(x) = 1$.

Wir fassen die bisherigen Beispiele noch einmal in der folgenden Tabelle zusammen; hierbei ist Q wie in (2.1.3).

Elementarmatrizen

Name	Notation	Matrix	$\Phi_A(x)$	Bedeutung	AQ	QA	invertierbar	Inverse
Einheitsmatrix	$\mathbf{1}$	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	x	Identität	Q	Q	ja	$\mathbf{1}$
Permutationsmatrix	P_{12}	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}x_2\\ x_1\end{pmatrix}$	Spiegelung	$\begin{pmatrix}c & d\\ a & b\end{pmatrix}$	$\begin{pmatrix}b & a\\ d & c\end{pmatrix}$	ja	P_{12}
Diagonalmatrix	$\mathrm{diag}(\lambda,\mu)$	$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$	$\begin{pmatrix}\lambda x_1\\ \mu x_2\end{pmatrix}$	Skalierung/ Spiegelung	$\begin{pmatrix}\lambda a & \lambda b\\ \mu c & \mu d\end{pmatrix}$	$\begin{pmatrix}\lambda a & \mu b\\ \lambda c & \mu d\end{pmatrix}$	$\lambda\neq 0\neq\mu$	$\mathrm{diag}(\lambda^{-1},\mu^{-1})$
unipotente Elementarmatrix	$U_{12}(t)$	$\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}x_1+tx_2\\ x_2\end{pmatrix}$	Scherung	$\begin{pmatrix}a+tc & b+td\\ c & d\end{pmatrix}$	$\begin{pmatrix}a & b+ta\\ c & d+tc\end{pmatrix}$	ja	$U_{12}(-t)$
unipotente Elementarmatrix	$U_{21}(t)$	$\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix}$	$\begin{pmatrix}x_1\\ x_2+tx_1\end{pmatrix}$	Scherung	$\begin{pmatrix}a & b\\ c+ta & d+tb\end{pmatrix}$	$\begin{pmatrix}a+tb & b\\ c+td & d\end{pmatrix}$	ja	$U_{21}(-t)$

Weitere wichtige Matrizen

Name	Notation	Matrix	$\Phi_A(x)$	Bedeutung	invertierbar	Inverse
Drehmatrix	R_t	$\begin{pmatrix}\cos(t) & -\sin(t)\\ \sin(t) & \cos(t)\end{pmatrix}$	$\begin{pmatrix}\cos(t)x_1-\sin(t)x_2\\ \sin(t)x_1+\cos(t)x_2\end{pmatrix}$	Drehung	ja	R_{-t}
Spiegelungsmatrix	S_t	$\begin{pmatrix}\cos(2t) & \sin(2t)\\ \sin(2t) & -\cos(2t)\end{pmatrix}$	$\begin{pmatrix}\cos(2t)x_1+\sin(2t)x_2\\ \sin(2t)x_1-\cos(2t)x_2\end{pmatrix}$	Spiegelung	ja	S_t

Wichtige Identitäten

$$\begin{aligned}\mathrm{diag}(\lambda,\mu)\mathrm{diag}(\lambda',\mu') &= \mathrm{diag}(\lambda\lambda',\mu\mu')\\ U_{12}(t)U_{12}(s) &= U_{12}(t+s)\\ U_{21}(t)U_{21}(s) &= U_{21}(t+s)\\ R_tR_s &= R_{t+s}.\end{aligned}$$

Bemerkung 2.1.42 (Elementarumformungen)**.** Wir können das LGS (2.1.1) in *Matrix-Vektor-Form* schreiben als

$$Qx = y \quad \text{mit} \quad Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ y = \begin{pmatrix} e \\ f \end{pmatrix}. \tag{2.1.10}$$

Ist E eine invertierbare Elementarmatrix, so ist dieses LGS nach Korollar 2.1.26 äquivalent zum LGS

$$Q'x = y' \quad \text{mit} \quad Q' = EQ,\ y' = Ey. \tag{2.1.11}$$

Wir nennen den Übergang von (2.1.10) zu (2.1.11) eine *Elementarumformung*. Die möglichen Elementarumformungen sind also:

- Vertauschen von Zeilen ($E = P_{12}$);
- Addieren des Vielfachen einer Zeile zu einer anderen Zeile ($E = U_{12}(t)$ oder $E = U_{21}(t)$);
- Skalieren der Zeilen ($E = \operatorname{diag}(\lambda, \mu)$ mit $\lambda \neq 0 \neq \mu$).

Wir werden sehen, dass man durch solche Umformungen jedes LGS in eine Form überführen kann, in der man die Lösungsmenge sofort ablesen kann. Wir führen dies zunächst anhand einiger Beispiele vor.

Beispiel 2.1.43 (Unser erstes LGS)**.** Betrachte das LGS

$$\begin{aligned} x_1 + 2x_2 &= 5 \\ 3x_1 + 4x_2 &= 6. \end{aligned}$$

In Matrix-Vektorschreibweise liest sich dieses LGS als

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} x = \begin{pmatrix} 5 \\ 6 \end{pmatrix}.$$

Linksmultiplikation beider Seiten mit $U_{21}(-3)$ (also abziehen des 3-fachens der ersten Zeile von der zweiten) liefert das folgende äquivalente LGS:

$$\begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix} x = \begin{pmatrix} 5 \\ -9 \end{pmatrix}.$$

Eine weitere Linksmultipliation mit $U_{12}(1)$ liefert

$$\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} x = \begin{pmatrix} -4 \\ -9 \end{pmatrix}.$$

Eine letzte Linksmultiplikation mit $\operatorname{diag}(1, -0{,}5)$ liefert

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x = \begin{pmatrix} -4 \\ 4{,}5 \end{pmatrix}.$$

Das LGS hat also die eindeutige Lösung $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -4 \\ 4{,}5 \end{pmatrix}$.

Vermutlich wussten Sie schon aus der Schule, wie man das LGS aus Beispiel 2.1.43 löst. Wozu also der ganze Aufwand? Es wird sich noch Herausstellen, dass unsere Sichtweise auf LGS und die Einsicht, dass das systematische Lösen von Gleichungssystemen auf dem Anwenden linearer Abbildungen beruht, zu einer ganzen Reihe tieferer Einsichten führt. Als kleinen Vorgeschmack geben wir zwei kleine Anwendungen:

Bemerkung 2.1.44 (Invertieren einer Matrix)**.** Wenn wir in Beispiel 2.1.43 nur die jeweils linken Seiten der äquivalenten LGS betrachten, so haben wir gezeigt, dass

$$\begin{aligned} U_{21}(-3)\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} &= \begin{pmatrix}1 & 2\\ 0 & -2\end{pmatrix}\\ U_{12}(1)\left((U_{21}(-3)\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\right) &= \begin{pmatrix}1 & 0\\ 0 & -2\end{pmatrix}\\ \operatorname{diag}(1,-0{,}5)\left(U_{12}(1)\left((U_{21}(-3)\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\right)\right)\right) &= \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{aligned}$$

gilt. Setzen wir

$$B := \operatorname{diag}(1,-0{,}5)U_{12}(1)U_{21}(-3)$$

so haben wir gezeigt, dass B ein Links-Inverses der Matrix $A := \begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$ ist, dass also gilt

$$BA = \mathbf{1}.$$

Um B konkret auszurechnen, kann man verwenden, dass $B = \operatorname{diag}(1,-0{,}5)U_{12}(1)U_{21}(-3)\mathbf{1}$, d.h. B entsteht aus der Einheitsmatrix durch Anwenden derselben Zeilenumformungen, die A in die Einheitsmatrix verwandeln. Konkret gilt

$$B = \begin{pmatrix}-2 & 1\\ 1{,}5 & -0{,}5\end{pmatrix},$$

und damit rechnet man nach, dass zufällig[7] auch $AB = \mathbf{1}$ gilt. Wir haben also gezeigt, dass A invertierbar ist mit $A^{-1} = B$. Daraus folgt insbesondere, dass das LGS $Ax = y$ für *jede* Inhomogenität $y \in \mathbb{R}^2$ eine eindeutige Lösung hat, nämlich

$$x = A^{-1}y = By = \begin{pmatrix}-2y_1 + y_2\\ 1{,}5y_1 - 0{,}5y_2\end{pmatrix}.$$

Bemerkung 2.1.45 (Zerlegung invertierbarer Matrizen)**.** Aufgrund der letzten Bemerkung haben wir

$$\begin{aligned} A &= B^{-1} = (\operatorname{diag}(1,-0{,}5)U_{12}(1)U_{21}(-3))^{-1} = U_{21}(-3)^{-1}U_{12}(1)^{-1}\operatorname{diag}(1,-0{,}5)^{-1}\\ &= U_{21}(3)U_{12}(-1)\operatorname{diag}(1,-2).\end{aligned}$$

Wir haben also die invertierbare Matrix A als ein Produkt aus unipotenten Elementarmatrizen und einer Diagonalmatrix geschrieben.

Beispiel 2.1.46 (Ein LGS mit nicht-invertierbarer Matrix)**.** Die Matrix A in Beispiel 2.1.43 war invertierbar, und folglich hat das LGS $Ax = y$ für jede Inhomogenität $y \in \mathbb{R}^2$ eine eindeutige Lösung – nämlich $A^{-1}y$. Wir betrachten nun noch ein Beispiel, in dem die Matrix A nicht invertierbar ist, nämlich

$$A := \begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}$$

[7] Wir werden noch sehen, dass jede Linksinverse einer Matrix auch automatisch eine Rechtsinverse ist, aber solange uns die Theorie fehlt, müssen wir das von Hand nachrechnen.

Wir betrachten die beiden LGSe gegeben durch

$$\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}x = \begin{pmatrix}5\\ 10\end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}x = \begin{pmatrix}5\\ 11\end{pmatrix}$$

Multiplizieren von links mit $U_{21}(-2)$ liefert

$$\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}x = \begin{pmatrix}5\\ 0\end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}x = \begin{pmatrix}5\\ 1\end{pmatrix},$$

oder ausgeschrieben,

$$\left\{\begin{array}{rcl} x_1 + 2x_2 & = & 5 \\ 0 & = & 0 \end{array}\right\} \quad \text{bzw.} \quad \left\{\begin{array}{rcl} x_1 + 2x_2 & = & 5 \\ 0 & = & 1 \end{array}\right\}$$

Das zweite LGS hat keine Lösung, da die Aussage $0 = 1$ falsch ist, während die Lösungsmenge des ersten LGS durch die Gerade

$$\mathscr{L} := \left\{\begin{pmatrix}x_1\\ x_2\end{pmatrix} \in \mathbb{R}^2 \mid x_1 + 2x_2 = 5\right\}$$

gegeben ist. Da die Lösung (in beiden Fällen) nicht eindeutig ist, ist A in der Tat nicht invertierbar.

Durch ähnliches Vorgehen wie in Beispiel 2.1.43 und Beispiel 2.1.46 kann man für beliebige Matrizen $A \in \mathbb{R}^{2\times 2}$ und Inhomogenitäten $y \in \mathbb{R}^2$ die Lösungsmenge des LGS $Ax = y$ bestimmen und entscheiden, ob A invertierbar ist und ggf. auch die inverse Matrix bestimmen. Das Ergebnis ist wie folgt:

Satz 2.1.47 (Allgemeine Lösung von LGSen in zwei Unbestimmten)**.** *Seien* $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathbb{R}^{2\times 2}$ *und* $y \in \mathbb{R}^2$*, und es sei* $\mathscr{L} := \Phi_A^{-1}[y]$ *die Lösungsmenge des LGS* $Ax = y$*.*

(i) Ist $ad - bc \neq 0$*, so ist* A *invertierbar mit* $A^{-1} = \frac{1}{ad-bc}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$ *und* $\mathscr{L} = \{A^{-1}y\}$*.*

In diesem Fall ist A *ein Produkt von unipotenten Elementarmatrizen, Permutationsmatrizen und invertierbaren Diagonalmatrizen.*

(ii) Ist $ad - bc = 0$*, so ist* A *nicht invertierbar und einer der folgenden Fälle tritt ein:*

(a) Ist $a \neq 0$*, so gilt*

$$\mathscr{L} = \left\{\begin{array}{ll} \{x \in \mathbb{R}^2 \mid ax_1 + bx_2 = y_1\}, & \text{falls } y_2 = ca^{-1}y_1, \\ \emptyset, & \text{sonst.} \end{array}\right.$$

(b) Ist $a = 0$ *und* $c \neq 0$*, so gilt*

$$\mathscr{L} = \left\{\begin{array}{ll} \{x \in \mathbb{R}^2 \mid cx_1 + dx_2 = y_2\}, & \text{falls } y_1 = ac^{-1}y_2, \\ \emptyset, & \text{sonst.} \end{array}\right.$$

(c) Ist $a = c = 0$ *und* $b \neq 0$*, so gilt*

$$\mathscr{L} = \left\{\begin{array}{ll} \{x \in \mathbb{R}^2 \mid bx_2 = y_1\}, & \text{falls } y_2 = db^{-1}y_1, \\ \emptyset, & \text{sonst.} \end{array}\right.$$

(d) Ist $a = b = c = 0$ und $d \neq 0$, so gilt

$$\mathscr{L} = \begin{cases} \{x \in \mathbb{R}^2 \mid dx_2 = y_2\}, & \text{falls } y_1 = 0, \\ \emptyset, & \text{sonst.} \end{cases}$$

(e) Ist $a = b = c = d = 0$, so gilt

$$\mathscr{L} = \begin{cases} \mathbb{R}^2, & \text{falls } y = o, \\ \emptyset, & \text{sonst.} \end{cases}$$

Beweis. Übungen 2.1.48, 2.1.49 und 2.1.50. □

Übung 2.1.48. Seien $a, b, c, d \in \mathbb{R}$ mit $a \neq 0$ und $ad - bc \neq 0$. Zeigen Sie, dass $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertierbar ist und bestimmen Sie die Inverse, indem Sie genau wie in Bemerkung 2.1.44 vorgehen. Schreiben Sie außerdem die Matrix als ein Produkt von unipotenten Elementarmatrizen und Diagonalmatrizen.

Übung 2.1.49. Seien $a, b, c, d \in \mathbb{R}$ mit $a = 0$ und $-bc = ad - bc \neq 0$. Zeigen Sie, dass $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertierbar ist und bestimmen Sie die Inverse, indem Sie zunächst die Permutationsmatrix S anwenden, und dann wie in Bemerkung 2.1.44 vorgehen. Schreiben Sie außerdem die Matrix als ein Produkt von unipotenten Elementarmatrizen, Permutationsmatrizen und Diagonalmatrizen.

Übung 2.1.50. Seien $a, b, c, d \in \mathbb{R}$ mit $ad = bc$ und $y \in \mathbb{R}^2$. Bestimmen Sie die Lösungsmenge des LGS $\begin{pmatrix} a & b \\ c & d \end{pmatrix} x = y$, indem Sie dieselbe Fallunterscheidung wie in Satz 2.1.47.(ii) verwenden und in jedem der Fälle wie in Beispiel 2.1.46 vorgehen (und im Fall (b) zusätzlich eine Zeilenvertauschung vornehmen).

Bemerkung 2.1.51 (Invertierbarkeit vs. Flächeninhalt)**.** Da die Zahl $ad - bc$ determiniert, ob die Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2}$ invertierbar ist oder nicht, heißt sie auch die *Determinante* der Matrix, geschrieben $\det(A)$. Ihr Absolutbetrag hat eine einfache geometrische Bedeutung: Betrachte das Einheitsquadrat

$$Q := \{x \in \mathbb{R}^2 \mid x_1 \in [0,1], x_2 \in [0,1]\}.$$

Nach Übung 2.1.8 ist $\Phi_A(Q)$, das Bild von Q unter der linearen Abbildung Φ_A, entweder ein Parallelogramm oder eine Strecke oder ein Punkt. Jedes nicht-ausgeartete Parallelogramm hat einen positiven Flächeninhalt, während ausgeartete Parallelogramme (d.h. Strecken oder Punkte) nach Definition den Flächeninhalt 0 haben.

Mittels einer Skizze und etwas elementarer Flächenrechnung überlegt man sich leicht, dass der Flächeninhalt von $\Phi_A(Q)$ gerade durch die Formel $|ad - bc|$ gegeben ist (Übung!). Folglich ist A genau dann invertierbar, wenn Φ_A das Einheitsquadrat nicht auf eine Menge von Flächeninhalt 0 zusammenquetscht, wenn also das Bild des Einheitsquadrats unter Φ_A nicht zu einer Strecke oder einem Punkt ausartet.

Aus Satz 2.1.47 folgt unmittelbar das folgende Phänomen, dessen tieferen Grund wir erst später verstehen werden:

Korollar 2.1.52 (Eindeutige Lösbarkeit linearer Gleichungssysteme)**.** *Für* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2}$ *sind die folgenden Aussagen äquivalent:*

(i) *Es gibt ein* $y \in \mathbb{R}^2$*, so dass das LGS* $Ax = y$ *eine eindeutige Lösung hat.*

(ii) *Für jedes* $y \in \mathbb{R}^2$ *hat das LGS* $Ax = y$ *eine eindeutige Lösung.*

(iii) *Für jedes* $y \in \mathbb{R}^2$ *hat das LGS* $Ax = y$ *mindestens eine Lösung.*

(iv) *Für jedes* $y \in \mathbb{R}^2$ *hat das LGS* $Ax = y$ *höchstens eine Lösung.*

(v) A *ist invertierbar.*

(vi) A *ist ein Produkt von unipotenten Elementarmatrizen, Permutationsmatrizen und invertierbaren Diagonalmatrizen.*

(vii) $\det(A) := ad - bc \neq 0$.

(viii) Fläche$(A) := |ad - bc| \neq 0$. □

Zusammenfassung von Abschnitt 2.1

(1) Lineare Gleichungssysteme in zwei Veränderlichen können geschrieben werden als $\Phi(x) = y$ für eine lineare Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ und eine Inhomogenität $y \in \mathbb{R}^2$.

(2) Die zugehörige Lösungsmenge $\Phi^{-1}[y]$ ist entweder ein affiner Unterraum von $\mathbb{R}^2$ (Punkt, Gerade, Ebene) oder leer.

(3) Zum praktischen Rechnen stellt man lineare Abbildungen durch Matrizen dar. Jede Aussage über lineare Abbildungen lässt sich äquivalent in Matrizensprache formulieren.

(4) Zum Lösen linearer Gleichungssysteme wendet man (spezielle) invertierbare lineare Abbildungen an. Diese überführen das LGS in ein äquivalentes LGS, dessen zugehörige Matrix einfacher ist.

(5) Eine lineare Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ ist bijektiv genau dann, wenn das LGS $\Phi(x) = y$ für jede Inhomogenität $y \in \mathbb{R}^2$ eine eindeutige Lösung hat. Durch Anwenden invertierbarer linearer Abbildungen zeigt man, dass dies genau dann der Fall ist, wenn Φ das Einheitsquadrat nicht auf eine Strecke oder einen Punkt zusammenquetscht.

(6) Invertierbare Matrizen lassen sich als Produkte von unipotenten Elementarmatrizen, Permutationsmatrizen und invertierbaren Diagonalmatrizen schreiben.

[15.11.23]

2.2 Abstrakte Vektorräume

Wir wollen im Folgenden die im Abschnitt 2.1 gewonnenen Erkenntnisse verallgemeinern. Diese Verallgemeinerung wird einen Großteil dieses und des nächsten Kapitels einnehmen. Wenn wir lineare Gleichungssysteme in mehr als zwei Unbestimmten studieren wollen, so stoßen wir zwangsläufig auf die folgenden naheliegenden Verallgemeinerungen des $\mathbb{R}^2$:

Beispiel 2.2.1 (Die Räume $\mathbb{R}^n$ und $\mathbb{R}^{p\times q}$)**.** In Analogie zum $\mathbb{R}^2$ können wir für alle $n \geq 1$ Mengen $\mathbb{R}^n$ definieren durch

$$\mathbb{R}^n := \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \dots x_n \in \mathbb{R} \right\}.$$

Elemente von $\mathbb{R}^n$ nennen wir *Spaltenvektoren* der *Länge* n. Nach Definition sind zwei Spaltenvektoren gleich, wenn sie in allen n Einträgen übereinstimmen. Wie im Fall des $\mathbb{R}^2$ können wir jeweils eine Vektoraddition $\mathrm{add} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, $(x, y) \mapsto x + y$ und eine Skalarmultiplikation $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$, $(\lambda, x) \mapsto \lambda \cdot x$ komponentenweise definieren durch

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \quad \text{und} \quad \lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

Etwas allgemeiner können wir für beliebige $p, q \in \mathbb{N}$ die Menge $\mathbb{R}^{p\times q}$ der $p \times q$-*Matrizen*[8] definieren durch

$$\mathbb{R}^{p\times q} := \left\{ x = \begin{pmatrix} x_{11} & \dots & x_{1q} \\ \vdots & & \vdots \\ x_{p1} & \dots & x_{pq} \end{pmatrix} \mid x_{11}, \dots, x_{pq} \in \mathbb{R} \right\},$$

wobei wiederum zwei Matrizen als gleich angesehen werden, wenn sie in allen ihre Einträgen übereinstimmen. Auch hier lassen sich wieder eine Addition $\mathrm{add} : \mathbb{R}^{p\times q} \times \mathbb{R}^{p\times q} \to \mathbb{R}^{p\times q}$ und eine Skalarmultiplikation $\mathrm{mult} : \mathbb{R} \times \mathbb{R}^{p\times q} \to \mathbb{R}^{p\times q}$ komponentenweise[9] definieren.

Bemerkung 2.2.2 (Abstrakte Eigenschaften der Räume $\mathbb{R}^{p\times q}$)**.** In Abschnitt 2.1 haben wir zwei Zugänge zu linearen Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$ kennengelernt: Einerseits können wir solche lineare Abbildungen konkret durch Matrizen in $\mathbb{R}^{2\times 2}$ beschreiben, andererseits abstrakt durch zwei einfache Eigenschaften. Beispiel 2.2.1 liefert einige *konkrete* Verallgemeinerungen des $\mathbb{R}^2$, wir wollen diese aber nun ebenfalls möglichst prägnant durch einige wenige *abstrakte Eigenschaften* beschreiben. Alle Beispiele haben gemeinsam, dass auf der zugrundeliegenden Menge V jeweils eine Addition und Skalarmultiplikation definiert sind. Wir fragen uns daher nun, welche Eigenschaften diese beiden Operationen besitzen. Aus den üblichen Rechenregeln für reelle Zahlen, ergeben sich leicht die folgenden Eigenschaften der Vektoraddition:

[8] Zur Reihenfolge der Indizes gilt: **Z**uerst **Z**eile, **s**päter **S**palte

[9] Wir werden später noch eine dritte Operation, die Matrizenmultiplikation, kennenlernen, diese lassen wir an dieser Stelle aber vorerst bewusst außen vor.

(V1) $\forall\, u,v,w \in V\colon (u+v)+w = u+(v+w)$. *(Assoziativgesetz)*

(V2) $\exists!\, \mathbf{0} \in V\ \forall\, v \in V\colon \mathbf{0}+v = v+\mathbf{0} = v$. *(Existenz eines neutralen Elements)*.

(V3) $\forall\, v \in V\ \exists!\, (-v) \in V : v+(-v) = (-v)+v = \mathbf{0}$. *(Existenz eines inversen Elements)*.
(Hierbei ist $\mathbf{0}$ das durch (V2) eindeutig bestimmte Element von V.)

(V4) $\forall\, v,w \in V\colon v+w = w+v$. *(Kommutativgesetz)*

In unseren Beispielen war dabei $\mathbf{0}$ jeweils der Vektor bzw. die Matrix, für die alle Einträge gleich 0 sind (sogenannter *Nullvektor* bzw. *Nullmatrix*), und es war jeweils $-v = (-1)\cdot v$. Die Skalarmultiplikation hat unter anderem die folgenden Eigenschaften:

(S1) $\forall\, \lambda,\mu \in \mathbb{R}\ \forall\, v \in V\colon \lambda(\mu v) = (\lambda\mu)(v)$. *(Wirkungsgesetz)*

(S2) $\forall\, v \in V\colon 1\cdot v = v$. *(Wirkung des neutralen Elements)*

Weiter sind die Vektoraddition und die Skalarmultiplikation miteinander kompatibel im folgenden Sinn:

(D1) $\forall\, \lambda \in \mathbb{R}\ \forall\, v,w \in V\colon \lambda(v+w) = (\lambda v)+(\lambda w)$. *(1. Distributivgesetz)*

(D2) $\forall\, \lambda,\mu \in \mathbb{R}\ \forall\, v \in V\colon (\lambda+\mu)v = (\lambda v)+(\mu v)$. *(2. Distributivgesetz)*

Das sind natürlich nur einige wenige und sehr spezielle Eigenschaften der Vektoraddition und Skalarmultiplikation. In unseren Beispielen gilt z.B. auch stets $\mathbf{0}\cdot v = \mathbf{0}$ und $-1\cdot v = -v$.

Wir kommen nun zu einer der zentralen Definition dieser Vorlesung:

Definition 2.2.3. Ist V eine Menge und sind

$$\mathrm{add}\colon V\times V \to V,\quad (x,y)\mapsto x+y \quad \text{und} \quad \mathrm{mult}\colon \mathbb{R}\times V \to V,\quad (\lambda,x)\mapsto \lambda x$$

zwei Abbildungen, die den Eigenschaften (V1)-(V4), (S1)-(S2) und (D1)-(D2) genügen, so heißt das Tripel $(V,\mathrm{add},\mathrm{mult})$ ein $\mathbb{R}$-Vektorraum. Die Abbildungen add bzw. mult heißen dann die *Vektoraddition* bzw. *Skalarmultiplikation* dieses Vektorraums.

Ein $\mathbb{R}$-Vektorraum ist also eine Menge mit einer Vektoraddition und einer Skalarmultiplikation, die den üblichen Rechengesetzen für Vektoren aus $\mathbb{R}^n$ genügen.

Notation 2.2.4. Ist V ein $\mathbb{R}$-Vektorraum, so nennen wir wie im Fall von $\mathbb{R}^2$ die Elemente von V *Vektoren* und die Elemente von $\mathbb{R}$ *Skalare*. Im Fall von $\mathbb{R}^{2\times 2}$ sind unsere „Vektoren“ also eigentlich Matrizen, aber das soll uns nicht stören. Für uns ist im Folgenden jedes Element eines abstrakten $\mathbb{R}$-Vektorraums ein Vektor.

Wir führen noch die folgenden Notationen und Sprechweisen ein: Das eindeutige Element $\mathbf{0}$ aus Axiom (V2) heißt der *Nullvektor* von V (auch wenn es sich u.U. um eine Nullmatrix handelt...), und wie schon im Fall von $\mathbb{R}^2$ definieren wir die *Differenz* zweier Vektoren $v,w \in V$ durch

$$v-w := v+(-w).$$

Beim Rechnen mit Skalaren und Vektoren können wir wegen der Assoziativgesetze in vielen Ausdrücken auf Klammern verzichten. Für $u, v, w \in V$ schreiben wir z.B. einfach $u+v+w$ statt $(u+v)+w$ oder $u+(v+w)$. Darüber hinaus machen wir die übliche „Punkt- vor Strichrechnung"-Konvention, d.h. für $\lambda \in \mathbb{K}$ und $u, v \in V$ schreiben wir $\lambda u + v$ statt $(\lambda u) + v$.

Bemerkung 2.2.5 (Zur Wahl der Axiome)**.** Eine Frage sollte Ihnen an dieser Stelle auf dem Herzen brennen: Warum haben die Mathematiker gerade die obigen Eigenschaften des $\mathbb{R}^n$ als Axiome für den abstrakten Vektorraumbegriff gewählt? Historisch gesehen war dies ein langer Prozess, und es hat sich erst sehr allmählich gezeigt, welche Axiome man annehmen muss, um eine reichhaltige Theorie zu erhalten. Die obigen Axiome haben sich historisch bewährt, aber es gibt durchaus auch andere mögliche Axiomensysteme für $\mathbb{R}$-Vektorräume. Beispielsweise kann man die Axiome (V2) und (V3) noch wie folgt[10] abschwächen:

In (V2) muss die Eindeutigkeit des Nullvektors nicht extra gefordert werden. Sind nämlich $\mathbf{0}$ und $\mathbf{0}'$ zwei Elemente von V, die die definierende Eigenschaft des Nullvektors erfüllen, so gilt

$$\mathbf{0} = \mathbf{0} + \mathbf{0}' = \mathbf{0}'.$$

Analog muss in (V3) die Eindeutigkeit des Inversen nicht extra gefordert werden, denn ist w ein weiteres Element von V mit $v + w = w + v = \mathbf{0}$, so folgt

$$-v = \mathbf{0} + (-v) = (w+v) + (-v) = w + (v + (-v)) = w + \mathbf{0} = w.$$

Einige der weiter oben erwähnten Eigenschaften der Addition im $\mathbb{R}^n$ wurden nur deshalb nicht in die Axiomenliste aufgenommen, weil sie sich bereits aus den obigen Axiomen ableiten lassen:

Lemma 2.2.6 (Direkte Folgerungen aus den Axiomen)**.** *Sei $\lambda \in \mathbb{R}$, V ein $\mathbb{R}$-Vektorraum und $v \in V$.*

(i) $\lambda v = \mathbf{0} \iff (\lambda = 0) \vee (v = \mathbf{0})$.

(ii) $(-1)v = -v$.

Beweis. (i) „$\Longleftarrow$": Für $v \in V$ gilt

$$0v = (0+0)v = 0v + 0v \Longrightarrow \mathbf{0} = 0v - 0v = (0v + 0v) - 0v = 0v.$$

Analog gilt für $\lambda \in \mathbb{R}$, dass

$$\lambda\mathbf{0} = \lambda(\mathbf{0}+\mathbf{0}) = \lambda\mathbf{0} + \lambda\mathbf{0} \Longrightarrow \mathbf{0} = \lambda\mathbf{0} - \lambda\mathbf{0} = (\lambda\mathbf{0} + \lambda\mathbf{0}) - \lambda\mathbf{0} = \lambda\mathbf{0}.$$

„$\Longrightarrow$": Sei $\lambda v = \mathbf{0}$, aber $\lambda \neq 0$. Dann hat λ ein multiplikatives Inverses λ^{-1} und wegen „$\Longleftarrow$" gilt

$$\mathbf{0} = \lambda^{-1}\mathbf{0} = \lambda^{-1}(\lambda v) = (\lambda^{-1}\lambda)v = 1v = v.$$

(ii) Mit (i) erhalten wir

$$(v + (-1)v) = 1v + (-1)v = (1 + (-1))v = 0v = \mathbf{0}. \qquad \square$$

Es sieht also so aus, als ob unsere Axiome ziemlich gut die Eigenschaften der Vektorräume $\mathbb{R}^n$ widerspiegeln. Es gibt allerdings auch exotische Beispiele für Vektorräume, die – zumindest auf den ersten Blick – sehr anders aussehen als die Räume $\mathbb{R}^n$.

[10] Man vergleich den Beweis von Satz 1.3.19.(iii)!

Beispiel 2.2.7 (Ein exotischer $\mathbb{R}$-Vektorraum)**.** Ist M eine beliebige Menge, so können wir auf der Menge $\mathrm{Abb}(M,\mathbb{R})$ der Abbildungen von M nach $\mathbb{R}$ eine Vektoraddition und Skalarmultiplikation „punktweise“ definieren durch

$$(f+g)(x) := f(x)+g(x) \quad \text{bzw.} \quad (\lambda f)(x) := \lambda f(x) \quad \text{für alle } x \in M.$$

Aus den Rechenregeln für reelle Zahlen folgt dann leicht, dass $\mathrm{Abb}(M,\mathbb{R})$ mit diesen Operationen ein $\mathbb{R}$-Vektorraum ist, wobei $\mathbf{0}$ die Nullabbildung (mit $\mathbf{0}(x) = 0$ für alle $x \in M$) ist und $(-f)(x) = -f(x)$ für alle $x \in M$ gilt.

Auf den zweiten Blick ist dieses Beispiel übrigens doch mit den vorigen Beispielen verwandt: Ist speziell $M = \{1,\dots,n\}$, so erhalten wir eine Bijektion

$$\mathrm{Abb}(M,\mathbb{R}) \to \mathbb{R}^n, \quad f \mapsto \begin{pmatrix} f(1) \\ \vdots \\ f(n) \end{pmatrix},$$

und diese erhält die Vektorraumstruktur[11].

Man kann dieses Beispiel noch etwas verallgemeinern: Ist V ein beliebiger $\mathbb{R}$-Vektorraum, so auch $\mathrm{Abb}(M,V)$ mit punktweiser Vektoraddition und Skalarmultiplikation.

Beispiel 2.2.8 (Nullvektorräume)**.** Ist V eine einelementige Menge (z.B. $V = \mathrm{Abb}(\emptyset,\mathbb{R})$), so gibt es jeweils genau eine Abbildung $V \times V \to V$ und $\mathbb{R} \times V \to V$. Mit diesen Abbildungen ist dann V ein Vektorraum (z.B. nach Beispiel 2.2.7, angewandt auf $M = \emptyset$), und das einzige Element von V ist dann automatisch das Nullelement; es gilt also $V = \{\mathbf{0}\}$. Man nennt einen Vektorraum mit genau einem Element daher auch einen *Nullvektorraum*. Gelegentlich schreiben wir auch $\mathbb{R}^0 := \mathrm{Abb}(\emptyset,\mathbb{R})$ für den kanonischen Nullvektorraum.

Die einfachste Art, neue Beispiele für Vektorräume zu konstruieren, ist als Unterräume der oben genannten. Es sei also im Folgenden V stets ein $\mathbb{R}$-Vektorraum.

Definition 2.2.9. Eine Teilmenge $W \subseteq V$ heißt $\mathbb{R}$-*Untervektorraum* (kurz: *Unterraum*), falls gilt:

(U1) $\mathbf{0} \in W$.

(U2) $\forall\, x,y \in W\colon x+y \in W$.

(U3) $\forall\, x \in W\ \forall\, \lambda \in \mathbb{R}\colon \lambda x \in W$.

Im Folgenden schreiben wir kurz „$W \leq V$“ für „W ist ein Unterraum von V.“ Jeder Vektorraum V enthält mindestens den Nullvektorraum $\{\mathbf{0}\}$ und sich selbst als Unterräume; diese heißen auch die *trivialen Unterräume*.

Bemerkung 2.2.10 (Untervektorräume als Vektorräume)**.** Ist $W \leq V$, so können wir wegen (U2) und (U3) Abbildungen

$$W \times W \to W,\ (x,y) \mapsto x+y \quad \text{und} \quad \mathbb{R} \times W \to W,\ (\lambda,x) \mapsto \lambda x$$

definieren. Wir behaupten, dass W mit diesen Operationen dann selbst wieder ein Vektorraum ist. Die Axiome (V1), (V4), (S1)-(S2) und (D1)-(D2) folgen direkt aus denen von V. Wegen (U1) ist das neutrale Element o von V ein neutrales Element für W, und nach Bemerkung 2.2.5 ist es das eindeutige neutrale Element von W. Dies zeigt (V2), und die Existenz des Inversen in (V3) folgt aus (U3) und Lemma 2.2.6.(ii). Die Eindeutigkeit des Inversen folgt wieder aus Bemerkung 2.2.5.

[11] d.h. sie ist ein Vektorraumisomorphismus im Sinne von Notation 2.2.16

Beispiel 2.2.11 (Mehr exotische Vektorräume)**.** In der Analysis untersucht man systematisch Unterräume des Raumes $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ der reellwertigen Funktionen, z.B. die Unterräume der stetigen Funktionen, differenzierbaren Funktionen, Riemann-intergrierbaren Funktionen etc. Analog untersucht man auch Unterräume des Raumes $\mathrm{Abb}(\mathbb{N},\mathbb{R})$ der Folgen, z.B. die Unterräume der konvergenten Folgen, Cauchy-Folgen, Nullfolgen etc.

Wir können nun die zentrale Definition aus Abschnitt 2.1 verallgemeinern:

Definition 2.2.12. Seien V und W zwei $\mathbb{R}$-Vektorräume. Eine Abbildung $\Phi : V \to W$ heißt *linear*, falls für alle $\lambda \in \mathbb{R}$ und $x, y \in V$ gilt:

(L1) $\Phi(\lambda x) = \lambda\Phi(x)$;

(L2) $\Phi(x + y) = \Phi(x) + \Phi(y)$.

Übung 2.2.13. Zeigen Sie: Sind V und W zwei $\mathbb{K}$-Vektorräume, so ist eine Abbildung $\Phi : V \to W$ genau dann linear, wenn für alle $\lambda, \mu \in \mathbb{K}$ und $x, y \in V$ gilt, dass

$$\Phi(\lambda x + \mu y) = \lambda\Phi(x) + \mu\Phi(y).$$

Beispiel 2.2.14. Ist $A \in \mathbb{R}^{p\times q}$ eine Matrix, so definiert A eine lineare Abbildung $\Phi_A : \mathbb{R}^q \to \mathbb{R}^p$ (man beachte die Reihenfolge!) durch Matrix-Vektor-Multiplikation; für $p = q = 2$ haben wir dies im Abschnitt 2.1 ausführlich diskutiert, dem allgemeinen Fall werden wir im Folgenden noch ein ganzes Kapitel (Kapitel 3) widmen.

Beispiel 2.2.15 (Eine exotische lineare Abbildung)**.** Ist $V \subseteq \mathrm{Abb}(\mathbb{R},\mathbb{R})$ der Unterraum der differenzierbaren Funktionen, so definiert die Ableitung eine lineare Abbildung $V \to \mathrm{Abb}(\mathbb{R},\mathbb{R})$.

Notation 2.2.16. Man nennt eine lineare Abbildung im Sinne von Definition 2.2.12 auch einen $\mathbb{R}$-*Vektorraum-Homomorphismus*[12] oder kurz einen *Homomorphismus*. Daher wird die Menge aller linearen Abbildungen von V nach W meist mit $\mathrm{Hom}_{\mathbb{R}}(V,W)$ bezeichnet. Die Notation $\mathrm{Lin}_{\mathbb{R}}(V,W)$ ist ebenfalls gebräuchlich, aber seltener.

Proposition 2.2.17. *Die Teilmenge* $\mathrm{Hom}_{\mathbb{R}}(V,W) \subseteq \mathrm{Abb}(V,W)$ *ist ein Unterraum.*

Beweis. Es seien $\lambda, \mu \in \mathbb{R}$ und $v, v' \in V$.

(U1) Die Nullabbildung $\mathbf{0}$ ist linear, denn es gilt

$$\mathbf{0}(\lambda v + \mu v') = 0 = \lambda \cdot 0 + \mu \cdot 0 = \lambda \cdot \mathbf{0}(v) + \mu \cdot \mathbf{0}(w).$$

(U2) Sind $f, g \in \mathrm{Hom}_{\mathbb{R}}(V,W)$, so ist auch $f + g$ linear, denn es gilt

$$\begin{aligned}(f+g)(\lambda v + \mu v') &= f(\lambda v + \mu v') + g(\lambda v + \mu v')\\ &= \lambda f(v) + \mu f(v') + \lambda g(v) + \mu g(v')\\ &= \lambda(f+g)(v) + \mu(f+g)(v').\end{aligned}$$

[12] Diese Terminologie folgt einer gewissen Systematik in der abstrakten Algebra: Sind X und Y Mengen mit einer zusätzlichen „Struktur“ z.B. der einer Gruppe oder eines Rings, so heißen Abbildunge $X \to Y$ die diese Struktur erhalten entsprechend Gruppenhomomorphismen, Ringhomomorphismen etc. Die Silbe „homos“ ist griechisch für „ähnlich“ die Silbe „morphe“ bedeutet „Form“. Ein Homomorphismus bildet also Dinge auf ander Dinge von „ähnlicher Form“ ab.

(U3) Ist $f \in \mathrm{Hom}_{\mathbb{R}}(V,W)$ und $\kappa \in \mathbb{R}$, so gilt

$$\begin{aligned}(\kappa \cdot f)(\lambda v + \mu v') &= \kappa f(\lambda v + \mu v') \\ &= \kappa(\lambda f(v) + \mu f(v')) \\ &= \lambda(\kappa f)(v) + \mu(\kappa f)(v'). \quad \square\end{aligned}$$

Bemerkung 2.2.18. An dieser Stelle sehen wir zum ersten Mal einen Vorteil unserer abstrakten Methode: Nicht nur der $\mathbb{R}^n$ ist ein Vektorraum, sondern auch der Raum $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^m,\mathbb{R}^n)$ der linearen Abbildungen von $\mathbb{R}^m$ nach $\mathbb{R}^n$ für beliebige $m,n \in \mathbb{N}$. Alle Aussagen, die wir über den $\mathbb{R}^n$ mittels der Vektorraumaxiome bewiesen haben, geben uns nun gratis auch Aussagen über den Raum $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^m,\mathbb{R}^n)$!

Beispiel 2.2.19 (Dualraum)**.** Ist V ein $\mathbb{R}$-Vektorraum, so ist $V^* := \mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R})$ ein Unterraum von $\mathrm{Abb}(V,\mathbb{R})$. Dieser Vektorraum heißt der *Dualraum* von V, und wird später eine entscheidende Rolle spielen

Definition 2.2.20. Ist Φ ein injektiver/surjektiver/bijektiver Homomorphismus, so bezeichnet man Φ als *Monomorphismus*/*Epimorphismus*/*Isomorphismus*. Zwei $\mathbb{R}$-Vektorräume V und W heißen *isomorph*[13], geschrieben $V \cong W$, wenn es einen Isomorphismus $\Phi : V \to W$ gibt.

Isomorphe Vektorräume haben die „gleiche Struktur“[14]: Nimmt man sich irgendwelche Elemente von V her und benennt diese mittels Φ in Elemente in W um, so erfüllen die ursprünglichen Elemente genau dieselben Gleichungen wie die umbenannten Elemente.

Beispiel 2.2.21. Ist $n = pq$, so erhalten wir einen Isomorphismus $\mathbb{R}^{p\times q} \to \mathbb{R}^n$, indem wir die Einträge der Matrizen auf beliebige (aber fest gewählte!) Art und Weise durchnummerieren.

Die folgende Übung liefert ein Beispiel für einen nicht-offensichtlichen Isomorphismus:

Übung 2.2.22. Nach Proposition 2.2.17 ist $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2,\mathbb{R}^2) \subseteq \mathrm{Abb}(\mathbb{R}^2,\mathbb{R}^2)$ ein Unterraum. Zeigen Sie (unter Verwendung von Abschnitt 2.1) dass dieser Unterraum isomorph zu $\mathbb{R}^{2\times 2}$ (und daher zu $\mathbb{R}^4$) ist. Können Sie allgemeiner zeigen, dass für alle $p,q \in \mathbb{N}$ ein Isomorphismus $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^q,\mathbb{R}^p) \to \mathbb{R}^{p\times q}$ existiert?

Nach Übung 2.2.22 ist insbesondere der Dualraum von $\mathbb{R}^n$ isomorph zum Raum $\mathbb{R}^{1\times n}$ der „Zeilenvektoren“ der Länge n (also Matrizen mit nur einer Zeile).

Übung 2.2.23 (Bilder und Urbilder)**.** Seien V und W $\mathbb{R}$-Vektorräume und $\Phi \in \mathrm{Hom}_{\mathbb{R}}(V,W)$. Zeigen Sie:

(a) Für jeden Unterraum $U \leq V$ ist $\Phi[U] \leq W$.

(b) Für jeden Unterraum $U' \leq W$ ist $\Phi^{-1}[U'] \leq V$.

Als Spezialfall halten wir die folgende Beobachtung fest, die die entsprechenden Aussagen aus Abschnitt 2.1 verallgemeinert.

Lemma 2.2.24. *Seien V und W $\mathbb{R}$-Vektorräume und $\Phi \in \mathrm{Hom}_{\mathbb{R}}(V,W)$.*

(i) $\ker(\Phi) := \Phi^{-1}[0]$ *ist ein Unterraum von V.*

[13] Dies ist ein Spezialfall von Definition 1.5.2, da Vektorräume und lineare Abbildungen eine Kategorie bilden.
[14] Die griechische Silbe „isos“ bedeute gleich, isomorphe Vektorräume haben also die „gleiche Form“.

(ii) Bild(Φ) *ist ein Unterraum von* W.

Wie in Abschnitt 2.1 nennen wir $\ker(\Phi)$ den *Kern* von Φ. Hier ist eine weitere wichtige Konstruktion von Vektorräumen:

Beispiel 2.2.25 (Produktvektorräume)**.** Sind V und W zwei $\mathbb{R}$-Vektorräume, so ist $V \times W$ wieder ein $\mathbb{R}$-Vektorraum bgzl. der komponentenweise Vektoraddition und Skalarmultiplikation gegeben durch

$$(v,w)+(v',w') = (v+v',w+w') \quad \text{und} \quad \lambda(v,w) = (\lambda v, \lambda w).$$

Die Vektorraumaxiome für $V \times W$ folgen sofort aus denen von V und W. Sind allgemeiner $V_1,\dots,V_n$ Vektorräume, so definieren wir das Produkt

$$\prod_{i=1}^{n} V_i := V_1 \times \cdots \times V_n := \{(v_1,\dots,v_n) \mid \forall i \in \{1,\dots,n\} : v_i \in V_i\}.$$

Dieses Produkt ist dann wieder ein Vektorraum bzgl. komponentenweiser Vektoraddition und Skalarmultiplikation. Implizit haben wir diese Konstruktion bereits gesehen, es gilt nämlich

$$\mathbb{R}^n \cong \mathbb{R}^{1\times n} = \prod_{i=1}^{n} \mathbb{R} = \mathbb{R} \times \cdots \times \mathbb{R}.$$

Übung 2.2.26. Es seien V und W zwei $\mathbb{R}$-Vektorräume und $\Phi : V \to W$ eine Abbildung Zeigen Sie, dass Φ genau dann linear ist, wenn der Graph von Φ ein Unterraum von $V \times W$ ist.

Am Ende dieses abstrakten Abschnitts wollen wir nun noch einmal reflektieren, was wir eigentlich getan haben.

Bemerkung 2.2.27 (Warum eigentlich „Axiomatisieren“?)**.** Ausgangspunkt dieser Abschnitts war die Frage, wie sich die Lösungstheorie linearer Gleichungssysteme in zwei Veränderlichen auf Systeme von mehr als zwei Veränderliche verallgemeinern lässt. Im Hinblick auf die Beantwortung dieser Frage wäre es vermutlich das Effizienteste, lediglich die Vektorräume $\mathbb{R}^n$ einzuführen und dann lineare Abbildungen zwischen diesen Vektorräumen zu studieren. Das ist nun aber gerade *nicht* das Vorgehen, das wir hier gewählt haben. Stattdessen haben wir einen sehr abstrakten Vektorraumbegriff eingeführt, dessen Verbindung zu linearen Gleichungssystemen doch sehr unklar ist. Warum haben wir das getan?

Ein Grund für unser Vorgehen ist sicherlich, dass wir in dieser Vorlesung einen Eindruck davon vermitteln wollen, wie Mathematiker denken. Eine gute Mathematikerin wird sich in der Regel nicht damit zufrieden geben, eine in einem Fall gewonnene Erkenntnis möglichst Eins-zu-Eins auf einen anderen Fall zu übertragen. Stattdessen wird sie sich (hoffentlich) die folgenden Fragen stellen:

- Kann ich die für den Beweis eines Satzes relevanten Eigenschaften der Objekte, die ich betrachtet habe, mit möglichst wenigen prägnanten Axiomen formulieren?
- Bleibt ein Satz gültig, wenn ich einige der gemachten Annahmen abschwäche?
- Kann ich eine stärkere Version des Satzes beweisen, wenn ich stärkere Annahmen hinzufüge?
- Kann ich neue Situationen finden, in denen der Satz anwendbar ist?

Aus diesen Fragen spricht eine gewisse Weltsicht (man könnte auch sagen: Ideologie), die wir Ihnen im Folgenden näherbringen wollen. Mathematik ist – so die Sicht der Mathematiker – nicht nur ein Werkzeug, um Probleme zu lösen, sondern auch eine sehr spezielle Art, über die Welt nachzudenken.

Was das Lösen konkreter Probleme angeht, so ist der mathematische Zugang in der Regel mühsamer und langsamer als der Zugang eines Physikers oder Ingenieurs. Der axiomatische Zugang der Mathematiker erfordert in vielen Fällen einen sehr langen Atem – vor allem natürlich beim Entwickeln einer mathematischen Theorie, aber auch schon beim bloßen Nachvollziehen. Zum Beispiel war Ihnen, als wir die Theorie linearer Abbildungen entwickelt haben, vielleicht zunächst nicht klar, welche Rolle diese im Zusammenhang mit linearen Gleichungssystemen spielen werden.

Was sind nun die Vorteile des mathematischen Zugangs? Der große Vorteil des Zugangs liegt wohl in der sehr breiten Anwendbarkeit. Man löst sicher manche Probleme langsamer, aber dafür findet man auf dem Weg dahin häufig Antworten auf andere Fragen, die man sich vielleicht sonst gar nicht gestellt hätte. Manchmal hat man auch unerwartet Glück und kann dieselben Argumente mehrmals verwenden. Ein Beispiel für einen solchen Zufall haben wir bereits gesehen: Wenn wir über Gleichungssysteme in n Unbestimmten nachdenken, dann taucht in diesem Zusammenhang nicht nur der Vektorraum $\mathbb{R}^n$, sondern auch die Menge der linearen Selbstabbildungen von $\mathbb{R}^n$ auf, und diese ist nun zufällig selbst wieder ein Vektorraum!

Ein wichtiger Aspekt der mathematischen Methode ist auch, dass man dank ihr immer wieder unerwartete Querverbindungen entdeckt, weil z.B. ein Satz, der ursprünglich aus der Geometrie motiviert war, plötzlich in der Arithmetik anwendbar wird oder umgekehrt. Die Geschichte der Mathematik ist voller solcher überraschender Querverbindungen, und das bestärkt die Mathematiker, an ihrer Methode festzuhalten. Nichtsdestotrotz soll hier nicht verschwiegen werden, dass die mathematische Art des Verallgemeinerns viel Geduld und Durchhaltevermögen erfordert, die manchmal erst spät (dann aber häufig umso mehr) belohnt werden.

Falls Sie an dieser Stelle nun aber ungeduldig werden und sich fragen, worauf das hier alles hinausläuft: Wir versprechen, dass wir bis zum Ende von Kapitel 3 die allgemeine Lösungstheorie linearer Gleichungssysteme entwickelt haben werden, aber wir nehmen jetzt nicht den kürzesten Weg dorthin, sondern einen landschaftlich schöneren Umweg.

Bemerkung 2.2.28 (Welche Objekte haben wir da jetzt eigentlich axiomatisiert?)**.** Wir werden später noch sehen, dass jeder abstrakte $\mathbb{R}$-Vektorraum isomorph zu einem Unterraum eines Vektorraums der Form $\mathrm{Abb}(M,\mathbb{R})$ für eine geeignete Menge M ist. Es ist allerdings häufig praktisch unmöglich einen solchen Isomorphismus auf einen Unterraum explizit anzugeben.

Bemerkung 2.2.29 (Noch nicht allgemein genug?)**.** Bisher haben wir uns nur (auf abstrakte Weise) mit *reellen* Lösungen linearer Gleichungssysteme. Insbesondere bei LGSen mit rationalen oder ganzzahligen Koeffizienten ist es aber mindestens genauso natürlich, nach rationalen oder ganzzahligen Lösungen zu fragen. Es stellt sich heraus, dass die Theorie der LGS über den rationalen Zahlen $\mathbb{Q}$ vollständig analog zur Theorie der reellen LGS verläuft, während die Frage nach ganzzahligen Lösungen viel komplizierter ist.

Im Sinne der oben erklärten Ideologie sollte man daher jetzt eigentlich fragen: Welche Eigenschaften der reellen oder rationalen Zahlen (die die ganzen Zahlen nicht haben) sind für die Vektorraumtheorie maßgeblich? Wir werden das im Detail im Kapitel 4 diskutieren, und es wird sich herausstellen, dass man in allem bisher Gesagten die reellen Zahlen $\mathbb{R}$ durch einen beliebigen sogenannten *Körper* ersetzten kann, also eine Menge $\mathbb{K}$ mit zwei Operationen (Addition und Multiplikation), die geeignete Axiome erfüllen. Ersetzt man in der Definition eines

$\mathbb{R}$-Vektorraums überall „$\mathbb{R}$“durch „$\mathbb{K}$“, so erhält man die Definition eines $\mathbb{K}$-*Vektorraums*.

Die folgenden Abschnitte funktionieren allesamt in dieser Allgemeinheit. Beim ersten Lesen sollten Sie sich allerdings auf den Fall $\mathbb{K} = \mathbb{R}$ und (wenn Sie mögen) $\mathbb{K} = \mathbb{Q}$ konzentrieren, alles andere diskutieren wir später.

Zusammenfassung von Abschnitt 2.2

(1) Abstrakte $\mathbb{R}$-Vektorräume sind durch eine Reihe von Axiomen definiert, die wesentliche Eigenschaften der Vektoraddition und Skalarmultiplikation der Anschauungsebene $\mathbb{R}^2$ abstrahieren.

(2) Typische Beispiele für $\mathbb{R}$-Vektorräume sind die Räume $\mathbb{R}^n$ von Spaltenvektoren, $\mathbb{R}^{p\times q}$ von Matrizen und $\mathrm{Abb}(M,\mathbb{R}^n)$ von Abbildungen.

(3) Die Definitionen eines Unterraums und einer linearen Abbildung lassen sich auf abstrakte Vektorräume übertragen. Unterräume eines $\mathbb{R}$-Vektorraums sind selbst wieder $\mathbb{R}$-Vektorräume.

(4) Die linearen Abbildungen zwischen zwei gegebenen Vektorräumen bilden selbst wieder einen Vektorraum.

(5) Vektorräume können nicht nur über $\mathbb{R}$, sondern auch über einem beliebigen Körper $\mathbb{K}$ definiert werden. (Ignorieren Sie diesen Punkt beim ersten Lesen.)

2.3 Erzeugendensysteme und lineare Hüllen

Falls Sie diesen Abschnitt zum ersten Mal lesen (oder in der Vorlesung hören), dann sei $\mathbb{K}$ entweder der Körper $\mathbb{R}$ der reellen Zahlen oder der Körper $\mathbb{Q}$ der rationalen Zahlen. Wenn Sie schon über mehr mathematische Erfahrung verfügen (z.B. weil Sie gerade die Vorlesung für die Klausur wiederholen), dann dürfen Sie sich $\mathbb{K}$ als einen beliebigen Körper denken - auf eigene Gefahr. In jedem Fall seien im Folgenden U, V, W stets $\mathbb{K}$-Vektorräume (wobei $\mathbb{K}$ fest gewählt ist). Wir stellen uns nun die Frage, wie man Unterräume von V möglichst effizient beschreiben kann. Wir beginnen mit einer sehr allgemeinen Konstruktion:

Lemma 2.3.1 (Schnitte von Unterräumen)**.** *Ist $\mathfrak{U} \subseteq \mathscr{P}(V)$ eine nichtleere Menge von Unterräumen, so gilt $\bigcap \mathfrak{U} \leq V$. (Mit anderen Worten, Schnitte von Unterräumen sind wieder Unterräume.)*

Beweis. Wir rechnen die Axiome (U1)–(U3) nach:

(U1) Für alle $U \in \mathfrak{U}$ gilt $\mathbf{0} \in U$ (da $U \leq V$), also ist $\mathbf{0} \in \bigcap \mathfrak{U}$.

(U2) Für $x, y \in V$ gelten die Implikationen

$$\begin{aligned} x, y \in \bigcap \mathfrak{U} &\implies \forall\, U \in \mathfrak{U} \colon x, y \in U \implies \forall\, U \in \mathfrak{U} \colon x + y \in U \\ &\implies x + y \in \bigcap \mathfrak{U}. \end{aligned}$$

(U3) Für $\lambda \in \mathbb{K}$ und $x \in V$ gelten die Implikationen

$$x \in \bigcap \mathfrak{U} \implies \forall\, U \in \mathfrak{U} \colon x \in U \implies \forall\, U \in \mathfrak{U} \colon \lambda x \in U \implies \lambda x \in \bigcap \mathfrak{U}. \qquad \square$$

Konstruktion 2.3.2 (Lineare Hülle)**.** Sei $S \subseteq V$ eine beliebige Teilmenge. Wir definieren

$$\mathfrak{U}_S := \{U \in \mathscr{P}(V) \mid (U \leq V) \wedge (S \subseteq U)\}.$$

Nach Definition sind die Elemente von $\mathfrak{U}_S$ Unterräume. Weiter gilt stets $V \in \mathfrak{U}_S$, also ist $\mathfrak{U}_S$ nicht leer. Wegen Lemma 2.3.1 ist daher

$$\langle S \rangle := \bigcap \mathfrak{U}_S$$

ein Unterraum von V. Dieser Unterraum hat die folgenden Eigenschaften:

(i) $S \subseteq \langle S \rangle$. Dies folgt aus der Tatsache, dass $S \subseteq U$ für alle $U \in \mathfrak{U}_S$.

(ii) Sei W ein beliebiger Unterraum von V mit $S \subseteq W$. Dann gilt $W \in \mathfrak{U}_S$, also

$$\langle S \rangle = \bigcap \mathfrak{U}_S \subseteq W.$$

Es folgt, dass $\langle S \rangle$ der eindeutige Unterraum von V ist, der S enthält und in jedem Unterraum, der S enthält, enthalten ist. Es ist also der eindeutige *kleinste* Unterraum, der S enthält.

Definition 2.3.3. Ist $S \subseteq V$, so heißt $\langle S \rangle$ die *lineare Hülle* der Menge S. Ist $S = \{v_1, \ldots, v_n\}$ endlich, so schreiben wir auch $\langle v_1, \ldots, v_n \rangle := \langle S \rangle$.

Der Vorteil dieser Definition liegt darin, dass sofort klar ist, dass $\langle S \rangle$ der kleinste Unterraum von V ist, er S enthält. Der große Nachteil der Definition ist allerdings, dass man zunächst keine Ahnung hat, wie die Elemente von $\langle S \rangle$ aussehen. Das wollen wir nun beheben.

Notation 2.3.4 (Linearkombinationen)**.** Sind $v_1, \ldots, v_n \in V$ und $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$, so heißt

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

die *Linearkombination* von $v_1, \ldots, v_n$ mit *Koeffizienten* $\lambda_1, \ldots, \lambda_n$. Die Menge aller soclcher Linearkombinationen bezeichnet man auch als den *Spann* von $v_1, \ldots, v_n$. Ist allgemeiner $S \subseteq V$ eine Teilmenge, so definieren wir den *Spann* von V als die Menge

$$\mathrm{Spann}(S) := \{\lambda_1 v_1 + \cdots + \lambda_n v_n \mid n \in \mathbb{N}, \lambda_1, \ldots, \lambda_n \in \mathbb{K}, v_1, \ldots, v_n \in S\}.$$

Für $S = \emptyset$ ist dies so zu verstehen, dass $\mathrm{Spann}(\emptyset) = \{o\}$.

Wir werden im folgenden viel mit Linearkombinationen herumrechnen müssen. Um Schreibarbeit zu verringern führen wir für $n \in \mathbb{N}$ die abkürzende *Summennotation*

$$\sum_{i=1}^{n} \lambda_i v_i := \lambda_1 v_1 + \cdots + \lambda_n v_n$$

ein. Das griechische Σ steht hierbei als Abkürzung für „Summe“. Um Fallunterscheidungen zu vermeiden, definieren wir auch noch die *leere Summe* durch

$$\sum_{i=1}^{0} \lambda_i v_i := \mathbf{0}.$$

Mit dieser Konvention gilt dann

$$\mathrm{Spann}(S) = \{\sum_{i=1}^{n} \lambda_i v_i \mid n \in \mathbb{N} \cup \{0\}, \lambda_1, \ldots, \lambda_n \in \mathbb{K}, v_1, \ldots, v_n \in S\} \cup \{o\}.$$

[17.11.23]

Satz 2.3.5 (Charakterisierung der linearen Hülle)**.** *Für alle $S \subseteq V$ gilt*

$$\langle S \rangle = \operatorname{Spann}(S).$$

Beweis. „$\supseteq$“: Seien $v_1, \dots, v_n \in S$ und $\lambda_1, \dots, \lambda_n \in \mathbb{K}$. Dann gilt:

$$\begin{aligned} \forall U \in \mathfrak{U}_S : v_1, \dots, v_n \in U &\implies \forall U \in \mathfrak{U}_S : \lambda_1 v_1, \dots, \lambda_n v_n \in U \\ &\implies \forall U \in \mathfrak{U}_S : (\lambda_1 v_1 + \cdots + \lambda_n v_n \in U) \wedge (\mathbf{0} \in U) \\ &\implies (\lambda_1 v_1 + \cdots + \lambda_n v_n \in \bigcap \mathfrak{U}_S) \wedge (\mathbf{0} \in \bigcap \mathfrak{U}_S). \end{aligned}$$

Dies zeigt, dass jedes Element von $\operatorname{Spann}(S)$ im Schnitt erhalten ist.

„$\subseteq$“: Wir zeigen zunächst, dass $W := \operatorname{Spann}(S)$ ein Unterraum von V ist: Axiom (U1) gilt nach Definition. Ist $v \in W$ und $\lambda \in \mathbb{K}$, so ist entweder $v = \mathbf{0}$ und daher $\lambda v = \mathbf{0} \in W$ nach Lemma 2.2.6, oder es gilt $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ für gewisse $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ und $v_1, \dots, v_n \in S$, und daher

$$\lambda v = \lambda(\lambda_1 v_1 + \cdots + \lambda_n v_n) = (\lambda\lambda_1)v_1 + \cdots + (\lambda\lambda_n)v_n \in W.$$

Dies zeigt (U2), und (U3) zeigt man analog wie folgt: Sind $v, w \in W \setminus \{\mathbf{0}\}$, so finden wir Elemente $v_1, \dots, v_n \in S$ und $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \mathbb{K}$ mit

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \quad \text{und} \quad w = \mu_1 v_1 + \cdots + \mu_n v_n,$$

denn kommen in der Linearkombination für v und w unterschiedliche Vektoren aus S vor, so können wir die jeweils fehlenden mit einem Koeffizienten 0 ergänzen. Dann ist aber

$$v + w = (\lambda_1 v_1 + \cdots + \lambda_n v_n) + (\mu_1 v_1 + \cdots + \mu_n v_n) = (\lambda_1 + \mu_1)v_1 + \cdots + (\lambda_n + \mu_n)v_n \in W,$$

und den Fall $v = \mathbf{0}$ oder $w = \mathbf{0}$ behandelt man analog. Dies zeigt (U3), also ist W ein Unterraum, der offensichtlich S enthält, also $W \in \mathfrak{U}_S$ und folglich $\bigcap \mathfrak{U}_S \subseteq W$. □

Beispiel 2.3.6 (Ursprungsgeraden und Ebenen)**.** Es seien $v, w \in V$. Nach Satz 2.3.5 gilt

$$\langle v \rangle = \mathbb{K}v := \{\lambda v \mid \lambda \in \mathbb{K}\}.$$

Für $v = \mathbf{0}$ gilt $\langle v \rangle = \{\mathbf{0}\}$. Ist $v \in V \setminus \{\mathbf{0}\}$, so heißt der Untervektorraum $\langle v \rangle$ die *Ursprungsgerade* durch v. Analog gilt

$$\langle v, w \rangle = \{\lambda v + \mu w \mid \lambda, \mu \in \mathbb{K}\}.$$

Je nachdem, wie v und w gewählt sind, kann es sich bei dieser Menge um den Nullraum, eine Ursprungsgerade oder eine *Ursprungsebene* handeln.

Definition 2.3.7. $S \subseteq V$ heißt ein *Erzeugendensystem* von V, falls $\langle S \rangle = V$. Der Vektorraum V heißt *endlichdimensional*, wenn er ein endliches Erzeugendensystem besitzt.

Beispiel 2.3.8. In Bemerkung 2.1.11 haben wir gesehen, dass jedes $x \in \mathbb{R}^2$ geschrieben werden kann als

$$x = x_1 e_1 + x_2 e_2, \tag{2.3.1}$$

also als eine Linearkombination der Vektoren e_1 und e_2. Daher ist $\{e_1, e_2\}$ ein Erzeugendensystem von $\mathbb{R}^2$.

Andererseits ist aber auch $\mathbb{R}^2$ ein Erzeugendensystem von $\mathbb{R}^2$ und jede Menge S mit $\{e_1, e_2\} \subseteq S \subseteq \mathbb{R}^2$ ist ebenfalls ein Erzeugendensystem. Das sind aber noch nicht alle Erzeugendensysteme von $\mathbb{R}^2$: Wir behaupten, dass auch $S := \{e_1, e_1 + e_2\}$ ein Erzeugendensystem von $\mathbb{R}^2$ ist. Für jeden Vektor $x \in \mathbb{R}^2$ gilt nämlich

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 \\ 0 \end{pmatrix} + \begin{pmatrix} x_2 \\ x_2 \end{pmatrix} = (x_1 - x_2)e_1 + x_2(e_1 + e_2). \tag{2.3.2}$$

Allgemeiner gilt übrigens das Folgende:

Übung 2.3.9. Zeigen Sie: Sind $v, w \in \mathbb{R}^2$, so ist $\{v, w\}$ ein Erzeugendensystem genau dann, wenn die Matrix mit erster Spalte v und zweiter Spalte w invertierbar ist.

Wir halten fest: Es gibt sehr viele verschieden Erzeugendensysteme von $\mathbb{R}^2$ von sehr unterschiedlicher Größe - mit 2 Elementen, 3 Elementen, sogar mit unendlich vielen Elementen.

Es ist aber nicht möglich, den $\mathbb{R}^2$ mit nur einem Element zu erzeugen:

Übung 2.3.10. Sei $v \in \mathbb{R}^2$. Zeigen Sie, dass $\langle v \rangle \subsetneq \mathbb{R}^2$.

Wir sehen also insbesondere, dass jedes zwei-elementige Erzeugendensystem von $\mathbb{R}^2$ minimal in dem Sinne ist, dass man kein Erzeugendensystem mehr erhält, wenn man einen der beiden Vektoren streicht. Solche minimalen Erzeugendensysteme werden wir im nächsten Abschnitt systematisch untersuchen.

Bemerkung 2.3.11 (Schnitt vs. Vereinigung)**.** Während der Schnitt von Unterräumen stets wieder ein Unterraum ist, ist die *Vereinigung* von Unterräumen im Allgemeinen kein Unterraum. Z.B. ist die Vereinigung K der Geraden $\langle e_1 \rangle$ und $\langle e_2 \rangle$ in $\mathbb{R}^2$ (das Koordinatenkreuz) kein Untervektorraum, da $e_1 \in K$ und $e_2 \in K$, aber $e_1 + e_2 \notin K$. Es gibt nun eine offensichtliche (wenn auch etwas plumpe) Art, diese Defekt zu beheben:

Definition 2.3.12. Sind $U_1, \ldots, U_n$ Unterräume von V, so ist ihre *Summe* definiert als

$$\sum_{i=1}^{n} U_i := U_1 + \cdots + U_n := \langle U_1 \cup \cdots \cup U_n \rangle .$$

Der Grund für die Summennotation ist die folgende Übung:

Übung 2.3.13. Seien $U_1, \ldots, U_n$ Unterräume von V. Folgern Sie aus Satz 2.3.5, dass

$$\sum_{i=1}^{n} U_i = \{u_1 + u_2 + \cdots + u_n \mid \forall\, i \in \{1, \ldots, n\} : u_i \in U_i\}. \tag{2.3.3}$$

Bemerkung 2.3.14 (Lineare Hülle vs. Summe)**.** Sind $v_1, \ldots, v_n \in V$, so besagt Satz 2.3.5 gerade, dass

$$\langle v_1, \ldots, v_n \rangle = \mathbb{K}v_1 + \cdots + \mathbb{K}v_n$$

die Summe der durch $v_1, \ldots, v_n$ gegebenen Ursprungsgeraden ist. Ein endlichdimensionaler Vektorraum kann also als Summe von endlich vielen Geraden geschrieben werden.

Beispiel 2.3.15. Da $\{e_1, e_2\}$ und $\{e_1, e_2, e_1 + e_2\}$ Erzeugendensysteme von $\mathbb{R}^2$ sind, gilt

$$\mathbb{R}^2 = \mathbb{R}e_1 + \mathbb{R}e_2 \quad \text{und} \quad \mathbb{R}^2 = \mathbb{R}e_1 + \mathbb{R}e_2 + \mathbb{R}(e_1 + e_2),$$

d.h. wir können $\mathbb{R}^2$ als Summe von zwei oder als Summe von drei Geraden schreiben. Es gibt hier aber einen entscheidenden Unterschied: Im ersten Fall, lässt sich jeder Vektor $v \in \mathbb{R}^2$ eindeutig als Summe von Elementen der beiden Geraden schreiben, während die Darstellung im zweiten Fall nicht eindeutig ist. Diesen Unterschied wollen wir nun formalisieren.

Notation 2.3.16. Sind $U_1,\dots,U_n$ Unterräume von V, so definieren wir eine Abbildung

$$S : U_1 \times \cdots \times U_n \to U_1 + \cdots + U_n, \quad (u_1,\dots,u_n) \mapsto u_1 + \cdots + u_n.$$

Man rechnet leicht nach, dass diese Abbildung linear ist, und nach (2.3.3) ist sie surjektiv. Wir nennen die Summe $U_1 + \cdots + U_n$ eine *direkte Summe* und schreiben $U_1 \oplus \cdots \oplus U_n := U_1 + \cdots + U_n$, falls S auch injektiv ist.

Die Summe $\mathbb{R}e_1 + \mathbb{R}e_2 + \mathbb{R}(e_1+e_2)$ ist nicht direkt, denn es gilt $S(e_1, e_2, -(e_1+e_2)) = \mathbf{0} = S(\mathbf{0},\mathbf{0},\mathbf{0})$. Die Summe $\mathbb{R}e_1 \oplus \mathbb{R}e_2$ ist hingegen direkt; dies folgt sofort aus der folgenden Anwendung von Satz 2.3.5:

Korollar 2.3.17 (Direkte Summe)**.** *Sei $n \in \mathbb{N}$ und seien $U_1,\dots,U_n$ Unterräume von V. Dann gilt:*

(i) Die Summe $U_1 + \cdots + U_n$ ist direkt genau dann, wenn gilt

$$\forall\, u_1 \in U_1,\dots,u_n \in U_n : u_1 + \cdots + u_n = \mathbf{0} \Longrightarrow u_1 = \cdots = u_n = \mathbf{0}. \tag{2.3.4}$$

(ii) Die Summe $U_1 + U_2$ ist direkt genau dann, wenn $U_1 \cap U_2 = \{\mathbf{0}\}$.

(iii) Die Summe $U_1 + \cdots + U_n$ ist direkt genau dann, wenn die Summe $U_1 + \cdots + U_{n-1}$ direkt ist und $(U_1 \oplus \cdots \oplus U_{n-1}) \cap U_n = \{\mathbf{0}\}$ gilt.

Beweis. (i) Ist die Summe direkt, so hat der Nullvektor die eindeutige Zerlegung $\mathbf{0} = \mathbf{0} + \cdots + \mathbf{0}$, also folgt (2.3.4). Ist die Summe nicht direkt, so gibt es ein $v \in \sum_{i=1}^n U_i$, das sich auf zweierlei Arten als Summe von Elementen der U_i schreiben lässt, also

$$v = u_1 + \cdots + u_n = u_1' + \cdots + u_n' \quad (u_i, u_i' \in U_i, (u_1,\dots,u_n) \neq (u_1',\dots,u_n')).$$

Dann sind die Vektoren $u_i - u_i' \in U_i$ nicht alle gleich $\mathbf{0}$, und wegen

$$(u_1 - u_1') + \cdots + (u_n - u_n') = \mathbf{0},$$

gilt (2.3.4) nicht. Daraus folgt die Behauptung durch Kontraposition.

(ii) Bedingung (2.3.4) besagt in diesem Fall, dass

$$\forall\, u_1 \in U_1, u_2 \in U_n : (u_1 + u_2 = \mathbf{0}) \Longrightarrow (u_1 = u_2 = \mathbf{0})). \tag{2.3.5}$$

Ist dies der Fall und ist $u \in U_1 \cap U_2$, so gilt $u \in U_1$ und $-u \in U_2$. Wegen $u + (-u) = \mathbf{0}$ folgt daher $u = -u = \mathbf{0}$. Dies zeigt, dass (2.3.5) impliziert, dass $U_1 \cap U_2 \subseteq \{\mathbf{0}\}$, und daher $U_1 \cap U_2 = \{\mathbf{0}\}$.

Ist umgekehrt $U_1 \cap U_2 = \{\mathbf{0}\}$ und sind $u_1 \in U_1$ und $u_2 \in U_2$ mit $u_1 + u_2 = \mathbf{0}$, so gilt $u_1 = -u_2 \in U_2$, also $u_1 \in U_1 \cap U_2 = \{\mathbf{0}\}$. Folglich gilt $u_1 = \mathbf{0}$ und daher auch $u_2 = -u_1 = \mathbf{0}$. Daher impliziert $U_1 \cap U_2 = \{\mathbf{0}\}$ schon (2.3.5).

(iii) Übung! □

Beispiel 2.3.18 (Direkte Zerlegungen von $\mathbb{R}^n$)**.** Es ist nun leicht, Beispiele für direkte Summen anzugeben:

(i) Ist $e_j \in \mathbb{R}^n$ der Vektor mit j-tem Eintrag 1 und anderen Einträgen 0, so gilt

$$v = v_1 e_1 + \cdots + v_n e_n$$

für alle $v \in \mathbb{R}^n$, und daher

$$\sum_{i=1}^{n} \langle e_i \rangle = \mathbb{R}^n.$$

Andererseits gilt

$$\sum_{i=1}^{j} \langle e_i \rangle = \{v \in \mathbb{R}^n \mid v_{j+1} = \cdots = v_n = 0\},$$

und daraus folgt durch wiederholte Anwendung von Korollar 2.3.17.(iii) nun leicht, dass

$$\mathbb{R}^n = \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle = \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_n.$$

Geometrisch besagt dies gerade, dass man jeden Vektor im n-dimensionalen Raum eindeutig in Anteile in Richtung der Koordinatenachsen zerlegen kann.

(ii) Die Zerlegung in (i) ist nicht die einzige mögliche Zerlegung von $\mathbb{R}^n$ als direkte Summe von Ursprungsgeraden. Sind ℓ_1, ℓ_2 zwei verschiedene Ursprungsgeraden in $\mathbb{R}^2$, so gilt $\ell_1 \cap \ell_2 = \{o\}$. Darüber hinaus lässt sich jeder Vektor im $\mathbb{R}^2$ in einen Anteil in Richtung ℓ_1 und einen Anteil in Richtung ℓ_2 zerlegen - dies ist anschaulich klar, aber man kann es auch aus den Definitionen nachrechnen (Übung!). Es gilt daher $\mathbb{R}^2 = \ell_1 \oplus \ell_2$.

Zusammenfassung von Abschnitt 2.3

(1) Jede Teilmenge S eines Vektorraums ist in einem eindeutigen kleinsten Untervektorraum, seiner linearen Hülle, enthalten. Dieser ist durch alle endlichen Linearkombinationen der Elemente von S gegeben.

(2) Eine Teilmenge eines Vektorraums heißt ein Erzeugendensystem, wenn ihre lineare Hülle der gesamte Raum ist. Falls ein endliches Erzeugendensystem existiert, heißt der Vektorraum endlichdimensional.

(3) Aus (endlichen) Mengen von Unterräumen kann man durch Bilden von Summen größere Unterräume konstruieren, deren Elemente sich in Elemente der gegebenen Unterräume zerlegen lassen. Ist diese Zerlegung eindeutig, so spricht man von einer direkten Summe.

2.4 Basen und Koordinaten

In diesem Abschnitt sei weiterhin $\mathbb{K}$ wie in Abschnitt 2.3, und es sei V ein $\mathbb{K}$-Vektorraum. Im letzten Abschnitt haben wir gesehen, dass der $\mathbb{R}^2$ Erzeugendensysteme mit 2,3,4,... oder unendlich vielen Elementen besitzt, aber kein Erzeugendensystem mit nur einem Element. In diesem Sinne sind Erzeugendensysteme mit 2 Elementen also minimal, und wir wollen uns nun überlegen, ob solche minimalen Erzeugendensysteme auch in allgemeinen Vektorräumen existieren. Es stellt sich heraus, dass sich minimale Erzeugendensysteme auf viele verschiedene Arten charakterisieren lassen.

Definition 2.4.1. Es sei $n \geq 1$ und $b_1, \ldots, b_n \in V$ und $B := \{b_1, \ldots, b_n\}$.

(i) $b_1, \ldots, b_n$ *erzeugen* V, wenn B ein Erzeugendensystem von V ist.

(ii) $b_1,\dots,b_n$ *erzeugen V minimal*, wenn zusätzlich keine Teilmenge $B' \subseteq B$ mit $|B'| \leq n-1$ ein Erzeugendensystem[15] ist.

(iii) b_j heißt *redundant* in $(b_1,\dots,b_n)$, falls $b_j \in \langle b_1,\dots,b_{j-1},b_{j+1},\dots,b_n\rangle$.

(iv) $b_1,\dots,b_n$ sind *linear unabhängig*, wenn für alle $\lambda_1,\dots,\lambda_n \in \mathbb{K}$ gilt:

$$\sum_{i=1}^{n} \lambda_i b_i = \mathbf{0} \implies \lambda_1 = \dots = \lambda_n = 0.$$

Andernfalls heißen $b_1,\dots,b_n$ linear abhängig.

(v) $b_1,\dots,b_n$ heißen *maximal linear unabhängig* falls sie linear unabhängig sind und $b_1,\dots,b_n,w$ für jedes $w \in V \setminus B$ linear abhängig sind.

Satz 2.4.2 (Charakterisierung endlicher Basen)**.** *Es seien $n \in \mathbb{N}$, $b_1,\dots,b_n \in V$ und $B := \{b_1,\dots,b_n\}$. Dann sind die folgenden Aussagen äquivalent:*

(i) $b_1,\dots,b_n$ *erzeugen V minimal.*

(ii) $b_1,\dots,b_n$ *erzeugen V und kein b_j ist redundant.*

(iii) $b_1,\dots,b_n$ *erzeugen V und sind linear unabhängig.*

(iv) Für alle $v \in V$ existieren eindeutige $\lambda_1,\dots,\lambda_n \in \mathbb{K}$, so dass

$$v = \sum_{i=1}^{n} \lambda_i b_i. \tag{2.4.1}$$

(v) $V = \mathbb{K}b_1 \oplus \dots \oplus \mathbb{K}b_n$.

(vi) $b_1,\dots,b_n$ *sind maximal linear unabhängig.*

Definition 2.4.3. Falls die äquivalenten Bedingungen von Satz 2.4.2 gelten, so nennen wir $B = \{b_1,\dots,b_n\}$ eine *endliche Basis* von V und $(b_1,\dots,b_n)$ eine *geordnete endliche Basis* von V.

Später werden wir auch noch unendliche Basen betrachten, daher die Terminologie. Um Fallunterscheidungen zu vermeiden, nennen wir die leere Menge eine endliche Basis des Nullvektorraums; hier kann man natürlich nichts anordnen, aber es handelt sich offensichtlich um eine in jeder Hinsicht minimale Erzeugendenmenge. Bevor wir Satz 2.4.2 beweisen, schauen wir uns zunächst an, was wir mit geordneten Basen anstellen können.

Notation 2.4.4. Ist $(b_1,\dots,b_n)$ eine geordnete Basis von V, so existieren nach Satz 2.4.2 eindeutige Funktionen $b_1^*,\dots,b_n^* : V \to \mathbb{K}$, so dass

$$v = b_1^*(v)b_1 + \dots + b_n^*(v)b_n.$$

Wir nennen diese Funktionen die *Koordinaten* bzgl. der geordneten Basis $(b_1,\dots,b_n)$ und den Vektor

$$[v]_{(b_1,\dots,b_n)} := \begin{pmatrix} b_1^*(v) \\ \vdots \\ b_n^*(v) \end{pmatrix}$$

den *Koordinatenvektor* von v bzgl. $(b_1,\dots,b_n)$.

[15] Dies impliziert insbesondere, dass die Vektoren $b_1,\dots,b_n$ alle paarweise verschieden sind.

Beispiel 2.4.5 (Standardbasis und Standardkoordinaten)**.** Sei $V := \mathbb{K}^n$, und für $i \in \{1,\dots,n\}$ sei e_i der Vektor mit $i$tem Eintrag = 1 und allen anderen Einträgen = 0. Für ein beliebiges $x \in \mathbb{K}^n$ gilt dann

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + \cdots + x_n e_n, \tag{2.4.2}$$

also erzeugen $e_1,\dots,e_n$ den $\mathbb{K}^n$, und nach Beispiel 2.3.18 bilden sie sogar eine geordnete Basis, genannt die *Standardbasis* von $\mathbb{K}^n$. Wegen (2.4.2) sind die zugehörigen Koordinaten durch $e_j^*(x) = x_j$ gegeben (die sogenannten *Standardkoordinaten*), und es gilt $[x]_{(e_1,\dots,e_n)} = x$.

Beispiel 2.4.6 (Nichtstandardkoordinaten)**.** Die Vektoren e_1 und $e_1 + e_2$ von $\mathbb{K}^2$ sind linear unabhängig, denn es gilt

$$\lambda_1 e_1 + \lambda_2(e_1 + e_2) = \mathbf{0} \Longrightarrow \begin{pmatrix} \lambda_1 + \lambda_2 \\ \lambda_2 \end{pmatrix} = \mathbf{0} \Longrightarrow \lambda_1 + \lambda_2 = \lambda_2 = 0 \Longrightarrow \lambda_1 = \lambda_2 = 0.$$

Andererseits gilt für beliebige $v \in \mathbb{K}^2$, dass

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} v_1 - v_2 \\ 0 \end{pmatrix} + \begin{pmatrix} v_2 \\ v_2 \end{pmatrix} = (v_1 - v_2)e_1 + v_2(e_1 + e_2), \tag{2.4.3}$$

also ist $(e_1, e_1 + e_2)$ geordnete Basis mit zugehörigen Koordinaten $e_1^*(v) = v_1 - v_2$ und $(e_1 + e_2)^*(v) = v_2$. Die Koordinatenvektoren zu dieser Basis sind also gegeben durch

$$[v]_{e_1, e_1+e_2} = \begin{pmatrix} v_1 - v_2 \\ v_2 \end{pmatrix}.$$

Beispiel 2.4.7 (Noch mehr Basen)**.** Wegen Satz 2.1.47 und Korollar 2.1.52 für alle $a,b,c,d \in \mathbb{R}$:

$$\begin{aligned}
\left\{\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}\right\} \text{ Basis von } \mathbb{R}^2 \quad &\Longleftrightarrow \quad \underbrace{\left(\forall\, y \in \mathbb{R}^2\, \exists\, \lambda,\mu \in \mathbb{R} :\ \lambda \begin{pmatrix} a \\ c \end{pmatrix} + \mu \begin{pmatrix} b \\ d \end{pmatrix} = y\right)}_{\text{Erzeugendensystem}} \wedge \underbrace{\left(\exists!\, \lambda,\mu \in \mathbb{R} :\ \lambda \begin{pmatrix} a \\ c \end{pmatrix} + \mu \begin{pmatrix} b \\ d \end{pmatrix} = \mathbf{0}\right)}_{\text{linear unabhängig}} \\
&\Longleftrightarrow \quad \left(\forall\, y \in \mathbb{R}^2\, \exists\, \lambda,\mu \in \mathbb{R} :\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = y\right) \wedge \left(\exists!\, \lambda,\mu \in \mathbb{R} :\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \mathbf{0}\right) \\
&\Longleftrightarrow \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ invertierbar} \quad \Longleftrightarrow \quad ad - bc \neq 0.
\end{aligned}$$

Wir sehen also, dass alle Paare von Vektoren, deren Einträge die Bedingung $ad - bc \neq 0$ erfüllen, eine Basis des $\mathbb{R}^2$ bilden.

Übung 2.4.8. Seien $a,b,c,d \in \mathbb{R}$ mit $ad - bc \neq 0$. Bestimmen Sie die Koordinaten zu der geordneten Basis

$$\left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}\right)$$

von $\mathbb{R}^2$ aus Beispiel 2.4.7.

Die Koordinaten zu einer geordneten Basis haben die folgende wichtige Eigenschaft:

Proposition 2.4.9. *Ist $(b_1,\dots,b_n)$ eine geordnete Basis von V, dann sind die zugehörigen Koordinatenfunktionen $b_1^*,\dots,b_n^* : V \to \mathbb{K}$ linear.*

Beweis. Sind $v, w \in V$ und $\lambda, \mu \in \mathbb{K}$, dann gilt

$$\begin{aligned} \lambda v + \mu w &= \lambda \sum_{i=1}^{n} b_i^*(v) b_i + \mu \sum_{i=1}^{n} b_i^*(w) b_i \\ &= \sum_{i=1}^{n} \left(\lambda b_i^*(v) + \mu b_i^*(w)\right) b_i. \end{aligned}$$

Dies bedeutet nach Definition der Koordinatenfunktionen aber gerade, dass $b_i^*(\lambda v + \mu w) = \lambda b_i^*(v) + \mu b_i^*(w)$. □

Korollar 2.4.10 (Koordinatenisomorphismus)**.** *Ist $(b_1, \ldots, b_n)$ eine geordnete Basis von V, so ist*

$$\iota_{(b_1,\ldots,b_n)} : V \to \mathbb{K}^n, \quad x \mapsto [x]_{(b_1,\ldots,b_n)}$$

ein Vektorraumisomorphismus. Insbesondere gilt $V \cong \mathbb{K}^n$.

Beweis. Die Abbildung ist linear wegen Proposition 2.4.9, und sie ist bijektiv, denn die Abbildung

$$\mathbb{K}^n \to V, \quad y \mapsto \sum_{i=1}^{n} y_i b_i$$

ist wegen Satz 2.4.2.(iv) eine Umkehrabbildung. □

Wir sehen also, dass jeder Vektorraum, der eine endliche Basis besitzt, isomorph zu einem der Räume $\mathbb{K}^n$ ist. Wir werden noch sehen, dass jeder endlichdimensionale Vektorraum eine solche Basis besitzt.

Bemerkung 2.4.11. Nach Korollar 2.4.10 liefert jede endliche geordnete Basis $\mathscr{B} \in V^n$ einen Isomorphismus $(-)_B : V \to \mathbb{K}^n$. Ist umgekehrt $\iota : V \to \mathbb{K}^n$ ein Isomorphismus, so überlegt man sich leicht, dass $(\iota^{-1}(e_1), \ldots, \iota^{-1}(e_n))$ eine Basis von V ist. Dies liefert eine Bijektion zwischen der Menge aller n-elementigen geordneten Basen von V und der Menge der Isomorphismen von V nach $\mathbb{K}^n$ (Übung!). Man sagt daher oft etwas ungenau: Die Wahl einer n-elementigen Basis ist "das Gleiche" wie die Wahl eines Isomorphismus zu $\mathbb{K}^n$. Da ein Vektorraum im Allgemeinen sehr viele verschieden Basen hat, gibt es im Allgemeinen sehr viele verschieden Isomorphismen zu $\mathbb{K}^n$. Diese Wahlmöglichkeit (also die Möglichkeit, Koordinaten zu wählen) wird sich später als ein entscheidender Vorteil herausstellen: Durch geschickte Koordinatenwahl lassen sich viele Probleme substantiell vereinfachen. Das gilt sogar für Probleme im $\mathbb{K}^n$ selbst - auch hier muss man nicht die Standardkoordinaten wählen!

Nach Proposition 2.4.9 sind die Koordinaten zu einer geordneten endlichen Basis Elemente des sogenannten *Dualraums* $V^* = \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K})$. Man bezeichnet Elemente dieses Raums auch als *lineare Funktionale* oder *Linearformen*.

Proposition 2.4.12 (Duale Basis)**.** *Ist $(b_1, \ldots, b_n)$ eine geordnete Basis von V, so ist $(b_1^*, \ldots, b_n^*)$ eine geordnete Basis des Dualraums V^*. Insbesondere gilt dann $V^* \cong \mathbb{K}^n$.*

Wir skizzieren den Beweis in der folgenden Übung.

Übung 2.4.13. Es sei $(b_1, \ldots, b_n)$ eine geordnete Basis von V.

(a) Zeigen Sie, dass für alle $i, j \in \{1, \ldots, n\}$ gilt:

$$b_i^*(b_j) = \delta_{ij} := \begin{cases} 1, & \text{falls } i = j \\ 0, & \text{sonst} \end{cases}$$

(b) Zeigen Sie, dass $b_1^*, \ldots, b_n^*$ linear unabhängig sind. [Hinweis: Seien $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ mit

$$\sum_{i=1}^{n} \lambda_i b_i^* = \mathbf{0}.$$

Setzen Sie die Vektoren $b_1, \ldots, b_n$ in diese Funktion ein, und verwenden Sie (a).]

(c) Es sei $\varphi \in V^*$. Zeigen Sie, dass

$$\varphi = \sum_{i=1}^{n} \varphi(b_i) b_i^*,$$

und folgern Sie, dass $b_1^*, \ldots, b_n^*$ den Dualraum V^* erzeugen. [Erinnerung: Um zu zeigen, dass zwei Funktionen mit gleicher Definitions- und Zielmenge gleich sind, muss man zeigen, dass sie ausgewertet an jedem Element der Definitionsmenge denselben Wert liefern.]

[22.11.23]

Wir wenden uns nun dem Beweis von Satz 2.4.2 zu und machen die folgende Vorüberlegung.

Lemma 2.4.14. *Seien $b_1,\dots,b_n \in V$. Dann sind $b_1,\dots,b_n$ genau dann linear abhängig wenn mindestens ein b_j redundant ist.*

Beweis. „$\Longrightarrow$“: Nach Annahme existieren $\lambda_1,\dots,\lambda_n \in \mathbb{K}$ mit $\sum_{i=1}^n \lambda_i b_i = \mathbf{0}$, wobei $\lambda_j \neq 0$ für mindestens ein j gilt. Es gilt dann

$$-\lambda_j b_j = \lambda_1 b_1 + \cdots + \lambda_{j-1} b_{j-1} + \lambda_{j+1} b_{j+1} + \cdots + \lambda_n b_n,$$

und indem wir beide Seiten durch $-\lambda_j$ teilen, sehen wir das b_j redundant ist.

„$\Longleftarrow$“: Existieren $\lambda_i \in \mathbb{K}$ mit $b_j = \lambda_1 b_1 + \cdots + \lambda_{j-1} b_{j-1} + \lambda_{j+1} b_{j+1} + \cdots + \lambda_n b_n$, so können wir $\lambda_j := -1$ setzen und erhalten $\sum_{i=1}^n \lambda_i b_i = 0$. □

Damit können wir nun den Satz beweisen:

Beweis von Satz 2.4.2. (i) $\Longrightarrow$ (ii): Wir führen einen Widerspruchsbeweis und nehmen an, b_j sei redundant. Wir setzen $B' := B \setminus \{b_j\}$. Da $b_1,\dots,b_n$ minimal erzeugen, sind diese Vektoren insbesondere paarweise verschieden, also gilt $|B'| = n-1$. Da b_j redundant ist, ist andererseits $b_j \in \langle B' \rangle$, und daher $B \subseteq \langle B' \rangle$. Dies impliziert

$$V = \langle B \rangle \subseteq \langle B' \rangle \subseteq V,$$

also ist B' Erzeugendensystem von V, im Widerspruch zur Minimalität von $b_1,\dots,b_n$.

(ii) $\Longrightarrow$ (iii): Dies folgt sofort aus Lemma 2.4.14.

(iii) $\Longrightarrow$ (iv) Da B Erzeugendensystem ist, existieren $\lambda_1,\dots,\lambda_n \in \mathbb{K}$, die (2.4.1) genügen. Genügen $\mu_1,\dots,\mu_n \in \mathbb{K}$ ebenfalls dieser Gleichung, so gilt

$$\mathbf{0} = v - v = \sum_{i=1}^n \lambda_i b_i - \sum_{i=1}^n \mu_i b_i = \sum_{i=1}^n (\lambda_i - \mu_i) b_i,$$

und mit der linearen Unabhängigkeit folgt daraus $\lambda_i - \mu_i = 0$ (also $\lambda_i = \mu_i$) für alle i.

(iv) $\Longrightarrow$ (i) Aus (2.4.1) folgt sofort, dass B ein Erzeugendensystem ist. Wir führen einen Widerspruchsbeweis und nehmen an, es gäbe ein $B' \subseteq B$ mit $|B| \leq n-1$, etwa $B' = \{b_{\sigma(1)},\dots,b_{\sigma(|B'|)}\}$ für eine Abbildung $\sigma : \{1,\dots,|B'|\} \to \{1,\dots,n\}$. Es sei $j \in \{1,\dots,n\} \setminus \mathrm{Bild}(\sigma)$. Wegen $b_j \in \langle B' \rangle$ finden wir $\lambda_1,\dots,\lambda_n \in \mathbb{K}$ mit $\lambda_k = 0$ für alle $k \in \{1,\dots,n\} \setminus \mathrm{Bild}(\sigma)$, so dass $b_j = \sum_{i=1}^n \lambda_i b_i$; insbesondere ist $\lambda_j = 0$. Andererseits ist aber

$$b_j = 0 \cdot b_1 + \cdots + 1 \cdot b_j + \cdots + 0 \cdot b_n,$$

im Widerspruch zur Eindeutigkeit der Darstellung.

An dieser Stelle haben wir gezeigt, dass (i) $\Longleftrightarrow$ (ii) $\Longleftrightarrow$ (iii) $\Longleftrightarrow$ (iv).

(iv) $\Longleftrightarrow$ (v): Dies gilt nach Definition der direkten Summe.

(iii) $\Longrightarrow$ (vi): Nach Annahme sind $b_1,\dots,b_n$ linear unabhängig, aber nicht maximal linear unahbhängig. Dann gäbe es ein $w \in V \setminus B$, so dass $b_1,\dots,b_n,w$ linear unabhängig sind. Wegen Lemma 2.4.14 wäre dann w nicht redundant in $B \cup \{w\}$, also $w \notin \langle B \rangle$, Widerspruch!

(vi) $\Longrightarrow$ (iii): Sei $b_1,\dots,b_n$ maximal linear unabhängig; wir zeigen, dass B ein Erzeugendensystem ist. Sei dazu $v \in V$. Sei dazu $v \in V$. Ist $v \in B$, so ist $v \in \langle B\rangle$; ist dagegen $v \notin B$, so ist $B \cup \{v\}$ nach Annahme linear abhängig, also existieren $\lambda_1,\dots,\lambda_{n+1}$ mit

$$\lambda_1 b_1 + \cdots + \lambda_n b_n + \lambda_{n+1} v = \mathbf{0} \quad \text{und} \quad \{\lambda_1,\dots,\lambda_{n+1}\} \neq \{0\}.$$

Wäre $\lambda_{n+1} = 0$, so wären $b_1,\dots,b_n$ linear abhängig, Widerspruch! Folglich ist $\lambda_{n+1} \neq 0$, und daher ist

$$v = -\frac{\lambda_1}{\lambda_{n+1}} b_1 - \cdots - \frac{\lambda_n}{\lambda_{n+1}} b_n \in \langle B\rangle.$$

Wir erhalten also in jedem Fall $v \in \langle B\rangle$, und da $v \in V$ beliebig war, folgt $V = \langle B\rangle$. □

Bemerkung 2.4.15 (Unendliche Basen)**.** Für die Zwecke der Vorlesungen LINEARE ALGEBRA I und LINEARE ALGEBRA II sind endliche Basen und ihre Koordinaten überwiegend ausreichend. In fortgeschrittenen Anwendungen, insbesondere in der höheren Analysis, ist es aber sehr wichtig, auch mit gewissen unendlichen Basismengen zu operieren. Es gibt in verschiedenen Gebieten der Mathematik verschiedene Verallgemeinerungen des Konzepts einer endlichen Basis auf unendliche Mengen. Wir erwähnen hier eine Verallgemeinerung, wie sie in der ALGEBRA häufig verwendet wird; in der FUNKTIONALANALYSIS werden sie eine andere Verallgemeinerung kennenlernen.

Definition 2.4.16. Eine Teilmenge B eines Vektorraums V heißt *endlich linear unabhängig*, wenn sie leer ist oder für alle $n \in \mathbb{N}$ alle paarweise verschiedenen $b_1,\dots,b_n \in B$ linear unabhängig sind. Ein endlich linear unabhängiges Erzeugendensystem heißt eine *(algebraische) Basis*.

Nach Definition ist eine endliche Teilmenge von V genau dann eine Basis, wenn sie eine endliche Basis im üblichen Sinne ist. Definition 2.4.16 funktioniert aber auch für unendliche Mengen B. Das Entscheidende an dieser algebraischen Definition einer Basis (im Unterschied zu den in der Analysis gebräuchlichen Definitionen) ist, dass immer nur endlich viele Elemente von B gleichzeitig betrachtet werden. Man kann unendliche Basen genau wie endliche Basen auf viele verschiedene Weisen charakterisieren.

Satz 2.4.17 (Charakterisierung von Basen)**.** *Für eine Teilmenge $B \subseteq V$ sind die folgenden Aussagen äquivalent:*

(i) *B ist eine Basis von V.*

(ii) *B ist ein Erzeugendensystem von V und keine echte Teilmenge $B' \subsetneq B$ ist ein Erzeugendensystem.*

(iii) *B ist ein Erzeugendensystem und jede endliche Teilmenge $B' \subseteq B$ ist eine endliche Basis von $\langle B'\rangle$.*

(iv) *Für jedes $v \in V \setminus \{\mathbf{0}\}$ existieren ein eindeutiges $n \in \mathbb{N}$ und eindeutige paarweise verschiedene Elemente $b_1,\dots,b_n \in B$ und $\lambda_1,\dots,\lambda_n \in \mathbb{K} \setminus \{0\}$, so dass*

$$v = \sum_{i=1}^{n} \lambda_i b_i. \tag{2.4.4}$$

(v) *B ist linear unabhängig und $B \cup \{v\}$ ist nicht linear unabhängig für jedes $v \in V \setminus B$.*

Der Beweis ist analog zu Satz 2.4.2 und sei zur Übung überlassen. Wir kommen nun zum zentralen Satz dieses Abschnitts:

Satz 2.4.18 (Hauptsatz über Basen)**.** *Es sei V ein Vektorraum und es seien $B_-, B_+ \subseteq V$ zwei Teilmengen mit $B_- \subseteq B_+$. Ist B_- linear unabhängig und B_+ ein Erzeugendensystem, so existiert eine Basis B von V mit $B_- \subseteq B \subseteq B_+$.*

Einige Spezialfälle dieses Satzes sind so wichtig, dass sie eigene Namen tragen:

Korollar 2.4.19 (Basisexistenzsatz)**.** *Jeder Vektorraum hat eine Basis.*

Beweis. Wende Satz 2.4.18 auf $B_- := \emptyset$ und $B_+ := V$ an. □

Korollar 2.4.20 (Basisauswahlsatz)**.** *Jedes Erzeugendensystem B_+ von V enthält eine Basis.*

Beweis. Wende Satz 2.4.18 mit $B_- := \emptyset$ an. □

Wir erinnern daran, dass ein Vektorraum *endlichdimensional* heißt, wenn er ein endliches Erzeugendensystem besitzt.

Korollar 2.4.21 (Endlichkeitssatz)**.** *Jeder endlichdimensionale Vektorraum hat eine endliche Basis.*

Beweis. Ist B_+ ein beliebiges endliches Erzeugendensystem, so enthält es nach dem Basisauswahlsatz eine Basis, die dann ebenfalls endlich sein muss. □

Korollar 2.4.22 (Klassifikation endlich erzeugter Vektorräume)**.** *Jeder endlichdimensionale Vektorraum ist isomorph zu $\mathbb{K}^n$ für ein $n \in \mathbb{N} \cup \{0\}$.*

Beweis. Korollar 2.4.21 und Korollar 2.4.10. □

Korollar 2.4.23 (Basisergänzungssatz)**.** *Ist $U \leq V$ und B' eine Basis von U, so lässt sich B' zu einer Basis B von V ergänzen.*

Beweis. Wende Satz 2.4.18 auf $B_- := B'$ und $B_+ := V$ an. □

Wir steuern nun den Beweis von Satz 2.4.18 an. Ab jetzt seien stets B_- und B_+ wie in Satz 2.4.18. Wir benötigen die folgende Vorüberlegung:

Lemma 2.4.24. *Ist $X \subseteq B_+$ linear unabhängig, so tritt einer der beiden folgenden Fälle ein:*

(i) X ist eine Basis von V.

(ii) Es existiert eine linear unabhängige Menge X' mit $X \subsetneq X' \subseteq B_+$.

Beweis. Wir nehmen an, dass (i) nicht gilt. Wäre $B_+ \subseteq \langle X \rangle$, so wäre $V = \langle B_+ \rangle \subseteq \langle X \rangle$, also X ein Erzeugendensystem und folglich eine Basis, was ein Widerspruch ist. Sei nun $v \in B_+ \setminus \langle X \rangle$ und $X' := X \cup \{v\}$, so dass $X \subsetneq X' \subseteq B_+$. Wir behaupten, dss X' linear unabhängig ist. Andernfalls fänden wir $b_1, \ldots, b_n \in X$ und $\lambda_1, \ldots, \lambda_n, \mu \in \mathbb{K}$, nicht alle gleich 0, so dass

$$\lambda_1 b_1 + \cdots + \lambda_n b_n + \lambda v = \mathbf{0}.$$

Da $\{b_1, \ldots, b_n\}$ linear unahängig sind, muss $\lambda \neq 0$ gelten. Dann ist aber

$$v = -\frac{\lambda_1}{\lambda} b_1 - \cdots - \frac{\lambda_n}{\lambda} b_n \in \langle X \rangle,$$

was ein Widerspruch ist. Folglich ist X' linear unabhängig. □

Unter der Zusatzannahme, dass B_+ *endlich* ist, folgt der Satz nun leicht:

Beweis von Satz 2.4.18 für endliche B_+. Sei $B_0 := B_-$. Ist B_0 eine Basis, so wählen wir $B := B_0$. Andernfalls existiert nach dem Lemma eine linear unabhängige Menge B_1 mit $B_0 \subsetneq B_1 \subseteq B_+$. Ist B_1 eine Basis, so wählen wir $B := B_1$, andernfalls existiert eine linear unabhängige Menge B_2 mit $B_0 \subsetneq B_1 \subsetneq B_2 \subseteq B_+$ usw. Da B_+ endlich ist, kann es keine unendlich lange Kette der Form

$$B_0 \subsetneq B_1 \subsetneq B_2 \subsetneq B_3 \subsetneq \dots$$

geben. Nach spätestens $|B_+|$ Schritten finden wir also eine Basis. □

Für unendliche Erzeugendensysteme B_+ können wir so nicht argumentieren, denn hier kann es in der Tat eine unendlich lange Kette von Teilmengen von B_+ geben. Trotzdem findet man stets eine "maximale" lineare unabhängige Teilmenge in B_+, die B_- enthält. Der Beweis dieser Tatsache verwendet allerdings eines der Axiome der Mengenlehre, auf das wir hier nicht näher eingehen können. Wir geben daher den Beweis des allgemeinen Falls im Kleingedruckten für Genießer; in der Vorlesung wird er nicht behandelt.

Definition 2.4.25. Sei $\mathscr{A} \neq \emptyset$ ein Mengensystem über einer Menge M und $\mathscr{K} \subseteq \mathscr{A}$.

(i) $\mathscr{K}$ heißt *Kette*, falls für alle $K_1, K_2 \in \mathscr{K}$ gilt: $(K_1 \subseteq K_2) \vee (K_2 \subseteq K_1)$.

(ii) $A \in \mathscr{A}$ heißt *obere Schranke* für $\mathscr{K}$ in $\mathscr{A}$, falls $K \subseteq A$ für alle $K \in \mathscr{K}$.

(iii) $A \in \mathscr{A}$ heißt *maximal*, falls für alle $A' \in \mathscr{A}$ gilt: $A \subseteq A' \Longrightarrow A = A'$.

Beispiel 2.4.26. Sei $\mathscr{A}$ das Mengensystem über $\mathbb{N}$ gegeben durch $\mathscr{A} := \{\{1\},\{2\},\{2,3\}\}$. Dann sind $\{1\}$ und $\{2,3\}$ maximal und $\{2,3\}$ ist obere Schranke für die Kette $\{\{2\},\{2,3\}\}$.

Das folgende Axiom der Mengenlehre ist eine von vielen äquivalenten Formulierungen des Auswahlaxioms. (Das werden wir hier aber nicht beweisen.)

Axiom 2.4.27 (Zornsches Lemma[16])**.** Sei $\mathscr{A} \neq \emptyset$ ein Mengensystem über einer Menge M. Hat jede nichtleere Kette $\mathscr{K} \subseteq \mathscr{A}$ eine obere Schranke in $\mathscr{A}$, so hat $\mathscr{A}$ ein maximales Element.

Unter Verwendung dieses Axioms können wir nun den Satz beweisen:

Beweis von Satz 2.4.18, allgemeiner Fall. Es sei

$$\mathscr{A} := \{A \subseteq V \mid A \text{ linear unabhängig}, B_- \subseteq A \subseteq B_+\}.$$

Wegen $B_- \in \mathscr{A}$ ist dies ein nichtleeres Mengensystem über V. Sei nun $\mathscr{K} \subseteq \mathscr{A}$ eine nicht-leere Kette und $A := \bigcup \mathscr{K}$. Wir zeigen, dass $A \in \mathscr{A}$ ist:

- A ist linear unabhängig: Seien $v_1, \dots, v_n \in A$ paarweise verschieden. Dann existieren $K_1, \dots, K_n \in \mathscr{K}$ mit $v_1 \in K_1, \dots v_n \in K_n$. Da $\mathscr{K}$ eine Kette ist, gilt entweder $K_1 \subseteq K_2$ oder $K_2 \subseteq K_1$, also jedenfalls $K_1 \cup K_2 \in \mathscr{K}$. Induktiv folgt, dass $K := K_1 \cup \dots \cup K_n \in \mathscr{K}$. Da $v_1, \dots, v_n \in K$ und K linear unabhängig ist, sind $v_1, \dots, v_n$ linear unabhängig. Folglich ist A linear unabhängig.
- Für alle $K \in \mathscr{K}$ gilt $B_- \subseteq K \subseteq B_+$, und folglich gilt auch $B_- \subseteq A \subseteq B_+$.

Mit dem Zornschen Lemma folgt nun, dass es ein maximales Element $B \in \mathscr{A}$ gibt. Dieses ist eine Basis: Andernfalls gäbe es nämlich nach Lemma 2.4.24 ein linear unabhängiges B' mit $B_- \subseteq B \subsetneq B' \subseteq B_+$, und insbesondere $B' \in \mathscr{A}$, im Widerspruch zur Maximalität von B. □

Wir schließen diesen Abschnitt mit zwei Aussagen über Unterräume und Basen.

[16] MAX AUGUST ZORN, dt. Mathematiker, 1906-1993, bewies die Äquivalenz diese Axioms zum Auswahlaxiom.

Proposition 2.4.28 (Direkte Summe)**.** *Es seien $U, W \leq V$ und B_U, B_W Basen von U bzw. W. Ist die Summe $U+W$ direkt, so ist $B_U \cap B_W = \emptyset$ und $B := B_U \sqcup B_W$ ist eine Basis von $U \oplus W$.*

Beweis. Wäre $v \in B_U \cap B_W \subseteq U \cap W = \{\mathbf{0}\}$, so wäre $v = \{\mathbf{0}\}$, aber der Nullvektor kann nicht Element einer Basis sein. Ist $v \in U \oplus W$, so ist $v = u + w$ für (eindeutige) $u \in U$, $w \in W$. Dann existieren $b_1, \ldots, b_m \in B_U$ und $b'_1, \ldots, b'_n \in B_W$ und $\lambda_1, \ldots, \lambda_m, \lambda'_1, \ldots, \lambda'_n \in \mathbb{K}$ mit

$$u = \lambda_1 b_1 + \cdots + \lambda_m b_m,\ w = \lambda'_1 b'_1 + \cdots + \lambda'_n b'_n \implies v = \lambda_1 b_1 + \cdots + \lambda_m b_m + \lambda'_1 b'_1 + \cdots + \lambda'_n b'_n,$$

also $v \in \langle B \rangle$ und B ist Erzeugendensystem. Wäre B linear abhängig, so gäbe es $b_1, \ldots, b_m \in B_U$ und $b'_1, \ldots, b'_n \in B_W$ und $\lambda_1, \ldots, \lambda_m, \lambda'_1, \ldots, \lambda'_n \in \mathbb{K}$ nicht alle 0 mit

$$\lambda_1 b_1 + \cdots + \lambda_m b_m + \lambda'_1 b'_1 + \cdots + \lambda'_n b'_n = \mathbf{0}.$$

Dann wäre aber

$$\underbrace{\lambda_1 b_1 + \cdots + \lambda_m b_m}_{\in U} = \underbrace{-(\lambda'_1 b'_1 + \cdots + \lambda'_n b'_n)}_{\in W} \in U \cap W = \{0\},$$

und daher

$$\lambda_1 b_1 + \cdots + \lambda_m b_m = \lambda_1 b_1 + \cdots + \lambda_m b_m = \mathbf{0},$$

im Widerspruch zur linearen Unabhängigkeit von B_U und B_W. □

Proposition 2.4.29 (Komplementärsatz)**.** *Für jeden Unterraum $U \leq V$ existiert ein Unterraum $W \leq V$ mit $U \oplus W = V$.*

Beweis. Nach Korollar 2.4.19 besitzt U eine Basis B_U, die sich nach Korollar 2.4.23 zu einer Basis B von V ergänzen lässt. Es sei $B_W := B \setminus B_U$ und $W := \langle B_W \rangle$. Wir behaupten, dass dann $U \oplus W = V$ gilt. Ist $v \in V$, so können wir v als Linearkombination von endlich vielen Elementen aus $B = B_U \cup B_W$ schreiben, also existieren $\lambda_i, \lambda'_j \in \mathbb{K}$ und $b_i \in B_U$, $b_j \in B_W$ mit

$$v = \sum_{i=1}^{m} \lambda_i b_i + \sum_{j=1}^{n} \lambda'_j b'_j \in U + W.$$

Dies zeigt, dass $V = U + W$. Um zu sehen, dass die Summe direkt ist, sei $v \in U \cap W$. Es existieren dann $\lambda_i, \lambda'_j \in \mathbb{K}$ und $b_i \in B_U$, $b_j \in B_W$ mit

$$\sum_{i=1}^{m} \lambda_i b_i = v = \sum_{j=1}^{n} \lambda'_j b'_j \implies \sum_{i=1}^{m} \lambda_i b_i - \sum_{j=1}^{n} \lambda'_j b'_j.$$

Aufgrund der linearen Unabhängigkeit von B folgt dann $\lambda_i = 0$ für alle i, und daher $v = 0$. □

Ein Unterraum W wie in Proposition 2.4.29 heißt ein *Vektorraumkomplement*[17] zu U in V.

[17] Häufig sagt man auch kurz „Komplement“ statt „Vektorraumkomplement“. Man sollte diesen Begriff aber nicht mit dem Begriff des Komplements aus der Mengenlehre verwechseln.

Zusammenfassung von Abschnitt 2.4

(1) Basen von Vektorräumen sind minimale Erzeugendensysteme. Sie verallgemeinern die Standardbasis in $\mathbb{R}^2$, jedoch gibt es in einem abstrakten Vektorraum viele gleichwertige Basen und nicht eine bevorzugte Basis.

(2) Lineare Unabhängigkeit liefert ein Kriterium um zu entscheiden, ob ein Erzeugendensystem eine Basis ist.

(3) Jeder endlichdimensionale Vektorraum hat eine endliche Basis. Genauer gilt: Jedes endliche Erzeugendensystem enthält eine endliche Basis, und jede Basis eines Unterraums lässt sich zu einer Basis des gesamten Raums ergänzen.

(4) Eine Wahl einer geordneten endlichen Basis in einem endlich erzeugten $\mathbb{K}$-Vektorraum liefert einen Isomorphismus zu einem $\mathbb{K}^n$, indem man jedem Vektor seinen Koordinatenvektor bzgl. dieser Basis zuordnet. Insbesondere ist jeder endlichdimensionale $\mathbb{K}$-Vektorraum isomorph zu einem $\mathbb{K}^n$.

[24.11.23]

2.5 Dimension endlichdimensionaler Vektorräume

In diesem Abschnitt sei weiterhin $\mathbb{K}$ wie in Abschnitt 2.3, und es sei V ein $\mathbb{K}$-Vektorraum. Im letzten Abschnitt haben wir gesehen, dass V stets eine Basis besitzt; anders als im $\mathbb{R}^2$ gibt es aber keine bevorzugte Basis mehr, und es stellt sich daher die Frage, inwieweit sich verschiedene Basen unterscheiden können. Es wäre theoretisch denkbar, dass ein Vektorraum eine Basis mit 2 Elementen, eine Basis mit 3 Elementen und eine weitere Basis mit unendlich vielen Elementen besitzt. Es stellt sich aber heraus, dass dies nicht der Fall ist:

Satz 2.5.1 (Vergleichssatz für Basen)**.** *Sind B_1 und B_2 zwei Basen von V, so existiert eine Bijektion zwischen B_1 und B_2.*

Wir werden Satz 2.5.1 hier nur für endlichdimensionale Vektorräume beweisen; in diesen Fall lässt er sich wie folgt formulieren:

Satz 2.5.2 (Vergleichssatz für endliche Basen)**.** *Ist V ein endlichdimensionaler Vektorraum, so sind alle Basen von V endlich und haben dieselbe Anzahl Elemente.*

Definition 2.5.3. Ist V ein endlichdimensionaler $\mathbb{K}$-Vektorraum, so heißt die Anzahl der Elemente einer beliebigen Basis von V die *Dimension* von V über $\mathbb{K}$, geschrieben $\dim_{\mathbb{K}}(V)$.

Beispiel 2.5.4. (i) Da die Standardbasis von $\mathbb{K}^n$ genau n Elemente hat, gilt $\dim_{\mathbb{K}} \mathbb{K}^n = n$.

(ii) Für $i \in \{1,\dots,m\}$ und $j \in \{1,\dots,n\}$ sei $E_{ij} \in \mathbb{K}^{m\times n}$ die Matrix mit (i,j)-tem Eintrag = 1 und allen anderen Einträgen = 0. Dann ist $\{E_{ij} \mid i \in \{1,\dots,m\}, j \in \{1,\dots,n\}\}$ eine Basis von $\mathbb{K}^{m\times n}$ (Übung!), und daher gilt $\dim_{\mathbb{K}} \mathbb{K}^{m\times n} = mn$.

Übung 2.5.5. Zeigen Sie: Sind zwei $\mathbb{K}$-Vektorräume V und W isomorph, so gilt $\dim_{\mathbb{K}}(V) = \dim_{\mathbb{K}}(W)$.

Aus Korollar 2.4.22, Beispiel 2.5.4 und Übung 2.5.5 folgt sofort:

Korollar 2.5.6 (Invarianz der Dimension)**.** *Ist V ein endlichdimensionaler Vektorraum, so ist V isomorph zu $\mathbb{K}^n$ für ein eindeutiges bestimmtes $n \in \mathbb{N} \cup \{0\}$ (nämlich $n = \dim V$). Insbesondere sind $\mathbb{K}^n$ und $\mathbb{K}^m$ für $n \neq m$ nicht isomorph.*

Der Beweis von Satz 2.5.2 basiert auf dem folgenden berühmten Hilfssatz:

Lemma 2.5.7 (Steinitzscher Austauschsatz[18])**.** *Sei B eine (potentiell unendliche) Basis von V und $v \in V \setminus \{o\}$. Dann existiert ein $b_1 \in B$, so dass $B' := B \setminus \{b_1\} \cup \{v\}$ eine Basis von V ist.*

Beweis. Nach Satz 2.4.17 existieren paarweise verschiedene Elemente $b_1,\dots,b_n \in B$ und $\lambda_1,\dots,\lambda_n \in \mathbb{K} \setminus \{0\}$, so dass

$$v = \sum_{i=1}^{n} \lambda_i b_i. \tag{2.5.1}$$

Wir zeigen, dass dann $B' := B \setminus \{b_1\} \cup \{v\}$ eine Basis ist:

[18] nach ERNST STEINITZ, dt.-jüdischer Mathematiker und Pianist, 1871-1928, nicht verwandt oder verschwägert mit Wilhelm Steinitz, dem ersten Schach-Weltmeister, der ebenfalls studierter Mathematiker war.

- *B' ist Erzeugendensystem:* Wegen (2.5.1) gilt

$$b_1 = -\frac{1}{\lambda_1} - \sum_{i=2}^{n} \frac{\lambda_i}{\lambda_1} b_i \in \langle B' \rangle.$$

  Wegen $b_2, \dots, b_n \in B'$ gilt daher $B \subseteq \langle B' \rangle$ und folglich $V = \langle B \rangle \subseteq \langle B' \rangle$, also ist B' Erzeugendensystem.

- *B' ist linear unabhängig:* Angenommen, B' wäre linear abhängig. Dann wäre schon eine endliche Teilmenge $B'' \subseteq B'$ linear abhängig, und wir dürfen annehmen, dass diese $\{v, b_2, \dots, b_n\}$ enthält, also etwa $B'' = \{v, b_2, \dots, b_N\}$. Wir finden dann $\mu_j \in \mathbb{K}$, nicht alle 0, so dass

$$\mu_1 v + \sum_{j=2}^{N} \mu_j b_j = \mathbf{0}.$$

  Da $B'' \setminus \{v\}$ linear unabhängig ist, ist $\mu_1 \neq 0$. Setzen wir (2.5.1) in diese Gleichung ein, so erhalten wir

$$\mathbf{0} = \mu_1 \left(\sum_{i=1}^{n} \lambda_i b_i. \right) + \sum_{j=2}^{N} \mu_j b_j = \mu_1 \lambda_1 b_1 + \sum_{i=2}^{n} (\mu_1 \lambda_i + \mu_i) b_i + \sum_{j=n+1}^{N} \lambda_j b_j.$$

  Da B linear unabhängig ist, sind alle Koeffizenten 0, also insbesondere $\mu_1 \lambda_1 = 0$, im Widerspruch zu $\mu_1 \neq 0 \neq \lambda_1$. □

Bemerkung 2.5.8 (Austauschkriterium)**.** Der Beweis des Steinitzschen Austauschsatzes sagt uns, gegen welche Elemente von B wir v eintauschen dürfen. Ist z.B. $B = \{b_1, \dots, b_n\}$ endlich mit $|B| = n$, dann dürfen wir v gegen jedes b_i mit $b_i^*(v) \neq 0$ eintauschen.

Beispiel 2.5.9. Wir betrachten die geordnete Standardbasis (e_1, e_2, e_3) von $\mathbb{R}^3$ und die Vektoren

$$v = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} \quad \text{und} \quad w = \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}.$$

Dann können wir v gegen einen beliebigen der drei Basisvektoren eintauschen, aber w nur gegen e_1 oder e_2 (da $e_3^*(w) = 0$). Insbesondere sind (e_1, e_2, v) und (w, e_2, e_3) Basen.

Beweis von Satz 2.5.2 für endlich erzeugtes V. Es sei $B^{(0)}$ eine beliebige Basis von V (nicht notwendig endlich). Nach dem Endlichkeitssatz (Korollar 2.4.21) besitzt V auch eine endliche Basis B; es sei $n := |B|$ und $B = \{\beta_1, \dots, \beta_n\}$.

Wir wenden nun Lemma 2.5.7 insgesamt n mal an:

- Nach dem Austauschsatz existiert ein $b_1 \in B_1$, so dass $B^{(1)} := B^{(0)} \setminus \{b_1\} \cup \{\beta_1\}$ eine Basis ist.

- Wir finden nun verschiedene $b_2, \dots, b_n \in B^{(1)} \setminus \{\beta_1\}$ und $\lambda, \mu_2, \dots, \mu_n \in \mathbb{K}$, so dass

$$\beta_2 = \lambda \beta_1 + \mu_2 b_2 + \cdots + \mu_n b_n.$$

  Da β_1 und β_2 linear unabhängig sind, muss mindestens eines der μ_j nicht 0 sein, nach umnummerieren gilt also $\mu_2 \neq 0$. Nach dem Austauschsatz ist dann

$$B^{(2)} := B^{(1)} \setminus \{b_2\} \cup \{\beta_2\} = \{b_1, b_2\} \cup (B^{(0)} \setminus \{\beta_1, \beta_2\})$$

  eine Basis.

- ...
- Schließlich finden wir $b_n \in B^{(n-1)} \setminus \{\beta_1, \dots, \beta_{n-1}\}$, so dass

$$B^{(n)} := B^{(n-1)} \setminus \{b_n\} \cup \{\beta_n\} = \{\beta_1, \dots, \beta_n\} \cup (B^{(0)} \setminus \{b_1, \dots, b_n\}) = B \cup (B^{(0)} \setminus \{b_1, \dots, b_n\}).$$

Insbesondere ist $B^{(n)}$ linear unabhängig, aber B als Basis ist bereits eine maximale linear unabhängige Menge! Dies ist nur möglich, wenn $B^{(0)} \setminus \{b_1, \dots, b_n\}) = \emptyset$, also $B^{(0)} = \{b_1, \dots, b_n\}$ und insbesondere $|B^{(0)}| = n = |B|$. □

Bemerkung 2.5.10 (Steinitz-Ketten)**.** Der Beweis von Satz 2.5.2 zeigt viel mehr als die Aussage des Satzes: Man kann von einer beliebigen Basis zu einer beliebigen anderen Basis gelangen, indem man die alten Basisvektoren sukzessive durch neue Basisvektoren ersetzt. Nennt man zwei Basen B und B' *benachbart*, falls $|B \setminus B'| = |B' \setminus B| = 1$, und schreibt dafür $B \sim B'$, so gilt also: Für je zwei Basen B_1, B_2 eines n-dimensionalen Vektorraums eine Kette von Basen der Form

$$B_1 \sim B^{(1)} \sim B^{(2)} \sim \cdots \sim B^{(n-1)} \sim B_2.$$

Eine solche Kette heißt *Steinitz-Kette*.

Im Folgenden sei V ein *endlichdimensionaler* Vektorraum der Dimension $\dim_{\mathbb{K}} V = n$.

Proposition 2.5.11. *Sind $w_1, \dots, w_m \in V$ paarweise verschieden, so gilt:*

(i) $\{w_1, \dots, w_m\}$ *Erzeugendensystem* $\Longrightarrow m \geq n$.

(ii) $\{w_1, \dots, w_m\}$ *linear unabhängig* $\Longrightarrow m \leq n$.

Beweis. Da *jede* Basis von V genau n Elemente besitzt, gilt:

$$\begin{aligned} \{w_1, \dots, w_m\} \text{ Erzeugendensystem} &\overset{\text{Korollar 2.4.20}}{\Longrightarrow} \{w_1, \dots, w_m\} \text{ enthält eine Basis} \\ &\overset{\text{Satz 2.5.2}}{\Longrightarrow} m \geq n; \\ \{w_1, \dots, w_m\} \text{ linear unabhängig} &\overset{\text{Korollar 2.4.23}}{\Longrightarrow} \{w_1, \dots, w_m\} \text{ ist in einer Basis enthalten} \\ &\overset{\text{Satz 2.5.2}}{\Longrightarrow} m \leq n. \quad \square \end{aligned}$$

Eine Basis ist also ein Erzeugendensystem „mit genau der richtigen Anzahl an Elementen“. Hat man zu viele Elemente, werden diese linear abhängig, hat man zu wenige, dann können sie nicht den ganzen Raum erzeugen. Hat man die richtige Anzahl, so gilt:

Korollar 2.5.12. *Sind $w_1, \dots, w_n \in V$ paarweise verschieden, so sind die folgenden Aussagen äquivalent:*

(i) $\{w_1, \dots, w_n\}$ *ist eine Basis.*

(ii) $w_1, \dots, w_n$ *sind linear unabhängig.*

(iii) $\{w_1, \dots, w_n\}$ *ist ein Erzeugendensystem.*

Beweis. Die Implikationen (i)$\Longrightarrow$(ii) und (i)$\Longrightarrow$(iii) folgen sofort aus Satz 2.4.2. Ist $\{w_1,\dots,w_n\}$ ein Erzeugendensystem, so ist dieses nach Proposition 2.5.11.(i) minimal, also nach Satz 2.4.2 eine Basis. Sind dagegen $w_1,\dots,w_n$ linear unabhängig, so ist $\{w_1,\dots,w_n\}$ wegen Proposition 2.5.11.(ii) eine maximale lineare unabhängige Menge, also nach Satz 2.4.2 eine Basis. Dies zeigt, dass (iii)$\Longrightarrow$(i) bzw. (iii)$\Longrightarrow$(ii). □

Korollar 2.5.13 (Monotonieprinzip)**.** *Sei $U \leq V$ ein Untervektorraum. Dann ist U endlichdimensional mit* $\dim_{\mathbb{K}} U \leq n$*, und falls* $\dim_{\mathbb{K}} U = n$*, so ist schon $U = V$.*

Beweis. Die erste Aussage folgt sofort aus dem Basisergänzungssatz (Korollar 2.4.23). Gelte nun $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} V$ und sei B eine Basis von U. Dann ist B linear unabhängig und hat $\dim_{\mathbb{K}} U = \dim_{\mathbb{K}} V$ Elemente, ist also nach Korollar 2.5.12 eine Basis von V. Es gilt also $V = \langle B\rangle = U$. □

Bemerkung 2.5.14 (Auflisten aller Unterräume)**.** Um alle Unterräume von V zu finden, kann man nach Korollar 2.5.13 wie folgt vorgehen: Ist $M \subseteq V$ eine beliebige endliche Teilmenge mit höchstens $(n-1)$ Elementen, so ist $\langle M\rangle$ ein Unterraum, und jeder Unterraum von V mit Ausnahme von V selber ist von dieser Form.

Dies zeigt erneut, dass jeder Untervektorraum von $\mathbb{R}^2$ der Nullvektorraum (Dimension 0), eine Ursprungsgerade (Dimension 1) oder die ganze Ebene ist. Analog ist jeder Unterraum von $\mathbb{R}^3$ entweder der Nullvektorraum (Dimension 0), eine Ursprungsgerade (Dimension 1), also von der Form $\mathbb{R}x$ für ein $x \in \mathbb{R}^3$), eine *Ursprungsebene* (Dimension 2) von der Form

$$E_{x,y} := \langle x, y\rangle = \{\lambda x + \mu y \mid \lambda, \mu \in \mathbb{R}\} = \mathbb{R}x \oplus \mathbb{R}y$$

für linear unabhängige $x, y \in \mathbb{R}^3$ oder der ganze Raum.

Wir halten noch die folgende Konsequenz aus Proposition 2.4.28 fest:

Korollar 2.5.15. *Sind $U, W \leq V$ und ist die Summe $U + W$ direkt, so ist*

$$\dim_{\mathbb{K}}(U \oplus W) = \dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(W).$$

Ist insbesondere W ein Vektorraumkomplement zu U, so gilt $\dim_{\mathbb{K}}(W) = \dim_{\mathbb{K}}(V) - \dim_{\mathbb{K}}(U)$. □

Hieraus folgt nun die folgende wichtige Formel:

Satz 2.5.16 (Dimensionsformel)**.** *Sind $U, W \leq V$, so gilt*

$$\dim_{\mathbb{K}}(U + W) = \dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(W) - \dim_{\mathbb{K}}(U \cap W).$$

Beweis. Nach Proposition 2.4.29 existieren Vektorraumkomplemente U_1 bzw. W_1 zu $U \cap W$ in U bzw. W. Nach Korollar 2.5.15 gilt dann $\dim_{\mathbb{K}}(W_1) + \dim_{\mathbb{K}}(U \cap W) = \dim_{\mathbb{K}}(W)$, und daher

$$\dim_{\mathbb{K}}(W_1) = \dim_{\mathbb{K}}(W) - \dim_{\mathbb{K}}(U \cap W). \tag{2.5.2}$$

Ausserdem gilt

$$U + W = ((U \cap W) + U_1) + ((U \cap W) + W_1) = ((U \cap W) + U_1) + W_1 = U + W_1.$$

Wegen Direktheit der Summe $(U \cap W) + W_1$ folgt

$$U \cap W_1 = U \cap (W \cap W_1) = (U \cap W) \cap W_1 = \{\mathbf{0}\},$$

also $U + W = U \oplus W_1$. Korollar 2.5.15 liefert dann

$$\dim_{\mathbb{K}}(U+W) = \dim_{\mathbb{K}} U \oplus \dim_{\mathbb{K}} W_1 \tag{2.5.3}$$

Einsetzen von (2.5.2) in (2.5.3) liefert die gewünschte Formel. □

Beispiel 2.5.17. Seien U und W zwei Ursprungsebenen in $\mathbb{R}^3$, so dass $\dim_{\mathbb{R}} U = \dim_{\mathbb{R}} W = 2$. Es gilt dann nach dem Monotonieprinzip (Korollar 2.5.13) und der Dimensionformel, dass

$$4 - \dim_{\mathbb{R}}(U \cap W) = 2+2-\dim_{\mathbb{R}}(U \cap W) = \dim_{\mathbb{R}} U + \dim_{\mathbb{R}} W - \dim_{\mathbb{R}}(U \cap W) = \dim_{\mathbb{R}}(U+W) \leq \dim_{\mathbb{R}}(\mathbb{R}^3) = 3,$$

und folglich $\dim_{\mathbb{R}}(U \cap W) \geq 1$. Andererseits gilt $\dim_{\mathbb{R}}(U \cap W) \leq \dim_{\mathbb{R}}(U) = 2$. Es gibt also genau zwei Möglichkeiten:

(a) $\dim_{\mathbb{R}}(U \cap W) = 2$. In diesem Fall ist $U \cap W = U$ und daher $U = W = U + W$.

(b) $\dim_{\mathbb{R}}(U \cap W) = 1$. In diesem Fall ist $\dim_{\mathbb{R}}(U + W) = 3$ und daher $U + W = \mathbb{R}^3$.

Wir haben also gezeigt: Zwei verschiedene Ursprungsebenen in $\mathbb{R}^3$ schneiden sich stets in einer Geraden, und ihre Vereinigung spannt stets den ganzen $\mathbb{R}^3$ auf.

In der Geometrie ist es häufig von Vorteil, die Dimension eines Vektorraums nicht mittels Basen, sondern mittels sogenannter Fahnen zu definieren. Die folgende Übung zeigt, dass dieser Zugang äquivalent zu unserem Zugang ist:

Übung 2.5.18 (Dimension und Fahnen)**.** Sind $U_0, \ldots, U_n$ Untervektorräume mit der Eigenschaft, dass

$$U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n,$$

so heißt $(U_0, \ldots, U_n)$ eine *Fahne*[19] der Länge n in V. Die Fahne heißt *echt*, falls

$$U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_n.$$

Zeigen Sie: Ist $\dim_{\mathbb{K}} V = n$, so hat jede echte Fahne in V die Länge $\leq n$, und es gibt eine echte Fahne der Länge n. (Die Dimension eines endlichdimensionalen Vektorraums ist also genau die maximale Länge einer echten Fahne.)

Zusammenfassung von Abschnitt 2.5

(1) Je zwei endliche Basen eines endlich erzeugten Vektorraums haben dieselbe Anzahl von Elementen. Diese heißt die Dimension des Vektorraums. (Allgemeiner stehen zwei Basen eines Vektorraums zueinander in Bijektion.)

(2) Man kann zwischen verschiedenen Basen hin- und hergehen, indem man sukzessive einen Basisvektor durch einen anderen austauscht. Der Steinitzsche Austauschsatz liefert ein Kriterium, welche Vektoren ausgetauscht werden können.

(3) Dimension ist monoton bzgl. Inklusion von Unterräumen und additiv unter direkter Summe. Letzteres impliziert eine Formel für die Dimension von Summen von Unterräumen.

[19] Malt man sich im $\mathbb{R}^3$ drei ineinander enthaltene Unterräume der Dimensionen 0, 1 und 2 auf, so sieht das ein bisschen aus wie eine Fahne, daher der Name.

2.6 Affine Unterräume und Quotientenvektorräume

In diesem Abschnitt sei weiterhin $\mathbb{K}$ wie in Abschnitt 2.3, und es sei V ein $\mathbb{K}$-Vektorraum. Wir haben die folgende Definition schon im Kontext von Teilmengen des $\mathbb{R}^2$ gesehen, wo sie im Zusammenhang mit linearen Gleichungssystemen eine zentrale Rolle gespielt hat:

Definition 2.6.1. Ist $U \leq V$ ein Unterraum und $x \in V$, so heißt die Menge

$$x + U := \{x + u \mid u \in U\}$$

ein *affiner Unterraum* von V.

Bemerkung 2.6.2 (Verschiebungsvektorraum)**.** Es sei $A = x + U$ ein affiner Unterraum von V mit $x \in V$ und $U \leq V$. Wir nennen $v \in V$ eine *Verschiebung* des affinen Unterraums A, falls $a + v \in A$ für alle $a \in A$ gilt. Genau wie im Fall von affinen Unterräumen von $\mathbb{R}^2$ zeigt man, dass

$$\{v \in V \mid v \text{ Verschiebung von A}\} = U = A - A := \{a_1 - a_2 \mid a_1, a_2 \in A\}.$$

U ist daher eindeutig durch A bestimmt und heißt der *Verschiebungsvektorraum* von A. Wir nennen

$$\dim_{\mathbb{K}} A := \dim_{\mathbb{K}} U$$

die *affine Dimension* von A. Ist $\dim_{\mathbb{K}} A = 1$ bzw. $\dim_{\mathbb{K}} A = 2$, so nennen wir A eine *affine Gerade* bzw. *affine Ebene*. Zwei affine Unterräume mit demselben Verschiebungsvektorraum heißen *parallel*, in Zeichen

$$A_1 \parallel A_2 :\iff A_1 - A_1 = A_2 - A_2.$$

Dies definiert eine Äquivalenzrelation auf der Menge der affinen Unterräume. Ist A affiner Unterraum mit Verschiebungsvektorraum U, so ist die Äquivalenzklasse von A gegeben durch die *Parallelenschar*

$$\mathscr{P}_A := \{x + U \mid x \in V\}.$$

Die folgende Beobachtung verallgemeinert Beispiel 1.4.6.

Proposition 2.6.3. *Sei $A \subseteq V$ ein affiner Unterraum mit Verschiebungsvektorraum U. Dann gilt:*

(i) Die Parallelenschar $\mathscr{P}_A$ ist eine Partition von V.

(ii) Die zugehörige Äquivalenzrelation ist gegeben durch

$$x \sim_U y \quad \iff \quad x - y \in U.$$

Beweis. Wegen $A \in \mathscr{P}_A$ ist $\mathscr{P}_A \neq \emptyset$, und ist $B \in \mathscr{P}_A$, so ist $B = x + U$ für ein $x \in V$ und folglich $x = x + \mathbf{0} \in B$, also $B \neq \emptyset$. Schließlich gilt für alle $x \in V$, dass $x \in x + U \subseteq \bigcup \mathscr{P}_A$ und daher $V = \bigcup P_A$. Zum Beweis von (i) bleibt zu zeigen, dass je zwei parallele affine Unterräume entweder gleich oder disjunkt sind; dies ist anschaulich klar, muss aber formal bewiesen werden!

Seien also $x, y \in V$ mit

$$(x + U) \cap (y + U) \neq \emptyset.$$

Wir finden dann $u_1, u_2 \in U$ mit $x + u_1 = y + u_2$, und folglich $x - y = u_2 - u_1 \in U$. Daraus folgt für alle $u \in U$, dass

$$x + u = y + (x - y) + u \in y + U, \quad \text{also } x + U \subseteq y + U,$$

und mit einem symmetrischen Argument zeigt man, dass $y+U \subseteq x+U$. Wir haben also gezeigt:

$$(x+U)\cap(y+U)\neq\emptyset \Longrightarrow x-y\in U \Longrightarrow x+U=y+U.$$

Da offensichtlich die dritte Aussage die erste impliziert, sind alle drei Aussagen äquivalent. Dies zeigt einerseits, dass $\mathscr{P}_U$ eine Partition ist, und zeigt gleichzeitig, dass $x\sim_U y \iff x+U = y+U \iff x-y\in U$, also (ii). □

Im Folgenden schreiben wir für einen Unterraum $U\leq V$ kurz

$$V/U := V/\sim_U = \mathscr{P}_{\mathbf{0}+U}.$$

Es stellt sich heraus, dass die Partition V/U selbst wieder die Struktur eines Vektorraums trägt!

Proposition 2.6.4 (Quotientenvektorraum)**.** *Ist $U\leq V$ ein Unterraum, so existiert auf V/U eine eindeutige Vektorraumstruktur, so dass die kanonische Projektion $\pi: V\to V/U$ linear ist.*

Beweis. Es gibt höchstens eine Möglichkeit, wie die Vektoraddition und Skalarmultiplikation definiert sein können, denn für $x,y\in V$ und $\lambda\in\mathbb{K}$ muss ja gelten

$$(x+U)+(y+U)=\pi(x)+\pi(y)=\pi(x+y)=(x+y)+U \quad \text{und} \quad \lambda(x+U)=\lambda\pi(x)=\pi(\lambda x)=\lambda x+U.$$

Wir müssen zeigen, dass dies *wohldefiniert* ist, dass also $(x+y)+U$ bzw. $\lambda x+U$ nicht von der Wahl der Repräsentanten x und y abhängen. Seien also $x',y'\in V$ mit $x+U=x'+U$ und $y'+U=y+U$. Nach Proposition 2.6.3 gilt dann $u_x := x'-x\in U$ und $u_y := y'-y\in U$. Für alle $z\in V$ folgt

$$z\in(x'+y')+U \Longrightarrow \exists u\in U: z=x'+y'+u=x+u_x+y+u_y+u=x+y+(u_x+u_y+u)\in(x+y)+U,$$

also $(x'+y')+U\subseteq(x+y)+U$, und analog zeigt man $(x+y)+U\subseteq(x'+y')+U$. Damit ist die Addition wohldefiniert, und für die Skalarmultiplikation rechnet man analog

$$z\in\lambda x'+U \Longrightarrow \exists u\in U: z=\lambda(x+u_x)+u=\lambda x+(\lambda u_x+u)\in\lambda x+U.$$

Wir können also Addition und Skalarmultiplikation wie gewünscht definieren. Die Vektorraumaxiome folgen nun (unter Verwendung von Bemerkung 2.2.5) sofort aus den entsprechenden Axiomen für V (Übung!). □

Definition 2.6.5. Der Vektorraum V/U mit Vektoraddition und Skalarmultiplikation gegeben durch

$$(x+U)+(y+U)=(x+y)+U \quad \text{und} \quad \lambda(x+U)=\lambda x+U \quad (x,y\in V,\lambda\in\mathbb{K})$$

heißt der *Quotientenvektorraum*[20] von V modulo U.

Übung 2.6.6. Sind A und B zwei beliebige Teilmengen von V, so definieren wir die *Minkowski-Summe*

$$A+B := \{a+b \mid a\in A, b\in B\}\subseteq V.$$

Zeigen Sie, dass die Addition in V/U durch die Minkowski-Summe gegeben ist. Gilt eine analoge Aussage auch für die Skalarmultiplikation?

[20] Manche Autoren verwenden auch den Begriff „Faktorraum“.

Wie können wir uns den Quotientenraum anschaulich vorstellen? Ein Repräsenentantensystem für V/U ist durch ein beliebiges Vektorraumkomplement W von U gegeben, und es stellt sich heraus, dass die Vektorraumoperationen kompatibel sind:

Proposition 2.6.7 (Komplement vs. Quotient)**.** *Sei $U \leq V$ und $\pi : V \to V/U$ die kanonische Projektion. Ist $W \leq V$ ein Vektorraumkomplement zu U, so ist die Restriktion*

$$\pi|_W : W \to V/U$$

ein Vektorraumisomorphismus.

Beweis. Da π linear ist, ist auch $\pi|_W$ linear. Wegen $V = U + W$ kann jedes $v \in V$ geschrieben werden als $v = u + w$ mit $u \in U$ und $w \in W$. Es gilt dann

$$\pi|_W(w) = w + U = w + (u + U) = (u + w) + U = v + U,$$

also ist $\pi|_W$ surjektiv. Sind $w_1, w_2 \in W$ mit $\pi(w_1) = \pi(w_2)$, so gilt $w_1 \sim_U w_2$, also $w_1 - w_2 \in U$. Andererseits gilt aber $w_1 - w_2 \in W$, also $w_1 - w_2 \in U \cap W = \{\mathbf{0}\}$ und daher $w_1 = w_2$. Dies zeigt, dass $\pi|_W$ bijektiv, und daher ein Isomorphismus ist. □

Man beachte, dass ein Unterraum $U \leq V$ im Allgemeinen viele verschiedene Vektorraumkomplemente hat, z.B. ist jede Gerade im $\mathbb{R}^2$ komplementär zu jeder anderen Gerade. Alle diese Vektorraumkomplemente sind aber isomorph, und der Quotientenvektorraum ist ein kanonischer[21] Vektorraum, der zu allen diesen Räumen isomorph ist.

Beispiel 2.6.8. Sei $V = \mathbb{R}^3$ und $U_1 \leq V$ eine Ursprungsgerade und $U_2 \leq V$ eine Ursprungsebene, die U_1 nicht enthält. Die Elemente von V/U_1 sind die zu U_1 parallelen Geraden („Spaghetti-Modell“ von V/U_1). Jede dieser Geraden schneidet U_2 in einem eindeutigen Punkt, und dies liefert eine Bijektion zwischen der Menge der Spaghetti und der Ebene U_2. Wenn wir zwei Spaghetti punktweise addieren, so addieren sich auch die Schnittpunkte. U_2 ist also auch Modell für den Quotienten V/U_1, eines von vielen möglichen „Scheibenmodellen“.

Man kann die Rollen von U_1 und U_2 auch umtauschen: Die Elemente von V/U_2 sind die zu U_2 parallelen Ebenen („Lasagne-Modell“ von V/U_2). Jede dieser Ebenen schneidet U_1 in genau einem Punkt, und dies liefert einen Isomorphismus zwischen dem Lasagne-Modell und dem Spieß-Modell U_1, das wieder nur eines von vielen möglichen solcher Modelle ist.

Definition 2.6.9. Ist $U \leq V$ und V/U endlichdimensional, so heißt

$$\operatorname{codim}_{\mathbb{K}}(U, V) := \dim_{\mathbb{K}}(V/U)$$

die *Codimension* von U in V. Ein Unterraum von Codimension 1 heißt *Hyperebene*.

Man beachte, dass hier nicht vorausgesetzt ist, dass V endlichdimensional ist.

Korollar 2.6.10. *Ist V endlichdimensional und $U \leq V$, so gilt*

$$\operatorname{codim}_{\mathbb{K}}(U, V) = \dim V - \dim U$$

[21] „Kanonisch“ bedeutet in diesem Zusammenhang Kompatibilität mit linearen Abbildungen im folgenden Sinne: Ist $\Phi : V \to W$ eine lineare Abbildung und $U \leq V$ mit $\Phi[U] = U'$, so erhalten wir eine wohldefinierte lineare Abbildung

$$V/U \to W/U', \quad x + U \mapsto \Phi(x) + U'.$$

Andererseits ist zwar das Bild eines Vektorraumkomplements von U in V wieder ein Vektorraumkomplement von U' in W, aber welches Vektorraumkomplement genau wir erhalten, hängt von der linearen Abbildung ab.

Beweis. Ist W ein Vektorraumkomplement von U, so gilt $V/U \cong W$, und daher

$$\operatorname{codim}_{\mathbb{K}}(U,V) = \dim_{\mathbb{K}}(V/U) = \dim_{\mathbb{K}} W = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} U$$

nach Korollar 2.5.15. □

Bemerkung 2.6.11. Zu Beginn der Linearen Algebra kann man Quotientenkonstruktionen häufig umgehen, indem man stattdessen mit Vektorraumkomplementen arbeitet. Auch wenn manche Lehrbücher so vorgehen, ist das aber eine schlechte Idee. Quotientenkonstruktionen spielen in vielen Teilgebieten der Algebra eine große Rolle - wir werden später noch Quotientengruppen, Quotientenringen, Quotientenalgebren usw. begegnen - und sind ab einem gewissen Punkt auch in der Linearen Algebra unerlässlich. Es ist daher besser, sich möglichst schnell an Quotienten (also das „Rechnen mit Äquivalenzklassen“) zu gewöhnen.

Zusammenfassung von Abschnitt 2.6

(1) Jeder affine Unterraum eines Vektorraums V definiert einen Verschiebungsvektorraum; affine Unterräume mit dem selben Verschiebungsvektorraum U bilden eine Partition V/U von V, genannt die zugehörige Parallelenschar.

(2) Auf der Parallelenschar V/U kann man eine eindeutige Vektorraumstruktur (Quotientenvektorraum) definieren mit der Eigenschaft, dass die kanonische Projektion $\pi : V \to V/U$ linear ist. (Man addiert und multipliziert also durch Addieren oder Mulitplizieren von Repräsentanten.)

(3) Jedes Vektorraumkomplement von U in V ist ein Repräsentantensystem für die Parallelenschar und mittels der Einschränkung der kanonischen Projektion isomorph zu V/U. Ist V endlichdimensional, so folgt $\dim_{\mathbb{K}} V/U = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} U$.

3 Lineare Abbildungen und Matrizen

[29.11.23]

Im gesamten Kapitel ist stets $\mathbb{K}$ ein Körper (wenn Sie noch nicht wissen, was das ist, nehmen Sie an, dass $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{Q}$ gilt) und U, V, W sind $\mathbb{K}$-Vektorräume.

3.1 Matrizenformalismus

Notation 3.1.1 (Matrixeinträge)**.** Sind $p, q \in \mathbb{N}$, so schreiben wir kurz $A = (a_{ij})_{1 \le i \le p, 1 \le j \le q}$ (oder noch kürzer $A = (a_{ij})$) für die Matrix

$$A = \begin{pmatrix} a_{11} & \dots & a_{1q} \\ \vdots & & \vdots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} \in \mathbb{K}^{p \times q}.$$

Hierbei sind $a_{11}, \dots, a_{pq} \in \mathbb{K}$ die *Matrixeinträge* von A. Gegeben $k \in \{1, \dots, p\}$ und $l \in \{1, \dots, q\}$ schreiben wir E_{kl} für die Matrix $E_{kl} = (a_{ij})$ mit $a_{ij} = 1$ falls $(i,l) = (k,l)$ und $a_{ij} = 0$ sonst. Die Matrizen E_{kl} bilden eine Basis des $\mathbb{K}$-Vektorraums $\mathbb{K}^{p \times q}$ (genannt die *Standardbasis*) und es gilt

$$A = (a_{ij}) = \sum_{i=1}^{p} \sum_{j=1}^{q} a_{ij} E_{ij},$$

also sind die Matrixeinträge genau die Koordinaten bzgl. der Standardbasis.

Im Folgenden identifizieren wir $\mathbb{K}^n$ und $\mathbb{K}^{n \times 1}$, fassen also Spaltenvektoren der Länge n als $(n \times 1)$-Matrizen auf.

Definition 3.1.2. Ist $A = (a_{ij}) \in \mathbb{K}^{p \times q}$ und $B = (b_{ij}) \in \mathbb{K}^{q \times r}$, so heißt die Matrix $C = (c_{ij}) \in \mathbb{K}^{p \times r}$ gegeben durch

$$c_{ik} = \sum_{j=1}^{q} a_{ij} b_{jk} \quad (1 \le i \le p, 1 \le k \le r)$$

das *Produkt* von A und B, und wird mit $A \cdot B$ oder kurz AB bezeichnet.

Die graphische Interpretation der Matrizenmultiplikation ist analog zu Bemerkung 2.1.27.

Beispiel 3.1.3. (i) Es gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 10 & 16 \end{pmatrix}$$

(ii) Wir definieren das *Kronecker-Symbol* durch

$$\delta_{ij} := \begin{cases} 1, & i = j, \\ 0 & i \neq j. \end{cases}$$

Dann sind die Produkte der Standardbasismatrizen gegeben durch

$$E_{ij}E_{kl} = \delta_{jk}E_{il}.$$

(iii) Die Matrix $\mathbf{1}_n = E_{11} + \cdots + E_{nn} \in \mathbb{K}^{n\times n}$ heißt die *nte Einheitsmatrix*. Es gilt $\mathbf{1}_n A = A$ und $B\mathbf{1}_n = B$ für beliebige Matrizen A und B von geeigneter Größe. Wie im (2×2)-Fall nennen wir eine quadratische Matrix $A \in \mathbb{K}^{n\times n}$ *invertierbar*, falls es eine Matrix $A^{-1} \in \mathbb{K}^n$ gibt mit $AA^{-1} = A^{-1}A = \mathbf{1}_n$.

Bemerkung 3.1.4 (Bilinearität)**.** Sind $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times r}$, so sind die Abbildung

$$\mathbb{K}^{q\times r} \to \mathbb{K}^{p\times r}, \quad C \mapsto AC$$

und die Abbildung

$$\mathbb{K}^{p\times q} \to \mathbb{K}^{p\times r}, \quad C \mapsto CB$$

beide linear. Beides rechnet man sofort nach (Übung!).

Der Spezialfall $r = 1$ liefert:

Beispiel 3.1.5. Jedes $A \in \mathbb{K}^{p\times q}$ definiert eine lineare Abbildung

$$\Phi_A : \mathbb{K}^q \to \mathbb{K}^p, \quad v \mapsto Av.$$

WARNUNG ! A hat die Maße $(p\times q)$, bildet aber $\mathbb{K}^q$ nach $\mathbb{K}^p$ ab, nicht umgekehrt. Damit wir das nicht verwechseln, schreiben wir bisweilen lineare Abbildungen **von rechts nach links**, also

$$\mathbb{K}^p \xleftarrow{\Phi_A} \mathbb{K}^q.$$

Bemerkung 3.1.6 (Lineare Abbildungen via Matrizen)**.** Genau wie in Bemerkung 2.1.11 sieht man, dass die Spalten $s_1,\ldots,s_q$ von $A = (a_{ij}) \in \mathbb{K}^{p\times q}$ die Bilder der Standardbasisvektoren $e_1,\ldots,e_q$ unter Φ_A sind. Man kann diesen Sachverhalt mittels der dualen Basis $(e_1^*,\ldots,e_p^*)$ von $(e_1,\ldots,e_p)$ auch ausdrücken als

$$a_{ij} = e_i^*(\Phi_A(e_j)).$$

Daraus folgt, genau wie im Beweis von Satz 2.1.10, dass die Abbildung

$$\iota : \mathbb{K}^{p\times q} \to \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}^q,\mathbb{K}^p), \quad A \mapsto \Phi_A$$

eine Bijektion ist. Ist $\Phi \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}^q,\mathbb{K}^p)$, so heißt $D(\Phi) := \iota^{-1}(\Phi)$ die *darstellende Matrix* von Φ bzgl. der Standardbasen. Man überlegt sich leicht, dass ι sogar linear, also ein Vektorraumisomorphismus ist, insbesondere gilt

$$\dim_{\mathbb{K}} \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}^q,\mathbb{K}^p) = pq.$$

Bemerkung 3.1.7 (Matrizenmultiplikation als Verkettung)**.** Wie in Bemerkung 2.1.27 kann man sich überlegen, dass die Matrizenmultiplikation genau der Verkettung linearer Abbildungen entspricht, für $A = (a_{ij}) \in \mathbb{K}^{p\times q}$ und $B = (b_{ij}) \in \mathbb{K}^{q\times r}$ gilt also

$$\Phi_A \circ \Phi_B = \Phi_{AB}.$$

Will man sich dies als kommutatives Diagramm veranschaulichen, so empfiehlt es sich, die Abbildungen **von rechts nach links** zu schreiben, also

$$\mathbb{K}^p \xleftarrow{\Phi_A} \mathbb{K}^q \xleftarrow{\Phi_B} \mathbb{K}^r, \qquad \mathbb{K}^p \xleftarrow{\Phi_{AB}} \mathbb{K}^r.$$

Bemerkung 3.1.8 (Darstellende Matrizen bzgl. allgemeiner Basen)**.** Es seien V und W endlichdimensionale $\mathbb{K}$-Vektorräume mit geordneten Basen $\mathscr{B}_V = (v_1, \ldots, v_q)$ bzw. $\mathscr{B}_W = (w_1, \ldots, w_p)$. Es seien

$$\iota_{\mathscr{B}_V} : V \to \mathbb{K}^q,\ v \mapsto [v]_{\mathscr{B}_V} \quad \text{und} \quad \iota_{\mathscr{B}_W} : W \to \mathbb{K}^p,\ w \mapsto [w]_{\mathscr{B}_W}$$

die zugehörigen Koordinatenisomorphismen. Ist nun $\Phi : V \to W$ linear, so ist $\iota_{\mathscr{B}_W} \circ \Phi \circ \iota_{\mathscr{B}_V}^{-1}$ eine lineare Abbildung von $\mathbb{K}^q$ nach $\mathbb{K}^p$, und ist $A \in \mathbb{K}^{p\times q}$ die zugehörige Darstellungsmatrix, so kommutiert das Diagramm

$$\begin{array}{ccc} W & \xleftarrow{\Phi} & V \\ {\scriptstyle \iota_{\mathscr{B}_W}}\downarrow & & \downarrow{\scriptstyle \iota_{\mathscr{B}_V}} \\ \mathbb{K}^p & \xleftarrow[\Phi_A]{} & \mathbb{K}^q, \end{array} \tag{3.1.1}$$

und da die vertikalen Abbildungen Isomorphismen sind, ist A durch dieses kommtuative Diagramm eindeutig bestimmt. Wir nennen dann A die *darstellende Matrix* von Φ bzgl. der Basen $\mathscr{B}_W$ und $\mathscr{B}_V$ und schreiben $D_{\mathscr{B}_W,\mathscr{B}_V}(\Phi)$. Die folgende Proposition liefert eine explizite Formel für diese Matrix.

Proposition 3.1.9. *Ist $(w_1^*, \ldots, w_p^*)$ die duale Basis zu $(w_1, \ldots, w_p)$, so gilt $D_{\mathscr{B}_W,\mathscr{B}_V}(\Phi) = (a_{ij})$ mit*

$$a_{ij} = w_i^*(\Phi(v_j)) \tag{3.1.2}$$

Beweis. Es sei $A = (a_{ij})$ mit a_{ij} wie in (3.1.2). Es genügt zu zeigen, dass dann das Diagramm 3.1.1 kommutiert. Nach Definition gilt

$$\Phi(v_i) = w_1^*(\Phi(v_i))w_1 + \cdots + w_p^*(\Phi(v_i))w_p = a_{1i}w_1 + \cdots + a_{pi}w_p$$

Sei nun $v = \lambda_1 v_1 + \cdots + \lambda_q v_q \in V$. Es gilt dann

$$\Phi(v) = \lambda_1(a_{11}w_1 + \ldots a_{p1}w_p) + \cdots + \lambda_q(a_{1q}w_1 + \cdots + a_{pq}w_p),$$

also

$$(\iota_{\mathscr{B}_W} \circ \Phi)(v) = \begin{pmatrix} a_{11}\lambda_1 + \cdots + a_{1q}\lambda_q \\ \vdots \\ a_{p1}\lambda_1 + \cdots + a_{pq}\lambda_q \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1q} \\ \vdots & & \vdots \\ a_{p1} & \ldots & a_{pq} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_q \end{pmatrix} = (\Phi_A \circ \iota_{\mathscr{B}_V})(v).$$

□

Auch hier erhalten wir wieder einen Isomorphismus

$$\mathrm{Hom}_{\mathbb{K}}(V, W) \to \mathbb{K}^{p\times q}, \quad \Phi \mapsto D_{\mathscr{B}_W,\mathscr{B}_V}(\Phi).$$

Beachte, dass dieser Isomorphismus nun aber von der Wahl der Basen abhängt!

WARNUNG! Es gibt in der Literatur keine einheitliche Notation für die darstellende Matrix einer linearen Abbildung. Die Matrix, die bei uns $D_{\mathscr{B}_W,\mathscr{B}_V}(\Phi)$ heißt, heißt bei anderen Autoren $D_{\mathscr{B}_V,\mathscr{B}_W}(\Phi)$ oder auch $D^{\mathscr{B}_V}_{\mathscr{B}_W}(\Phi)$ oder auch $D^{\mathscr{B}_W}_{\mathscr{B}_V}(\Phi)$ oder auch ${}_{\mathscr{B}_V}D_{\mathscr{B}_W}(\Phi)$. Auch der Buchstabe D ist nicht unbedingt Standard - M wie „Matrix“ ist eine häufige Variante. Wenn Sie also etwas im Internet oder in einem Buch nachlesen, dann müssen Sie immer zuerst überprüfen, was in Ihrer Quelle mit einer Notation wie $D_{\mathscr{B}_V,\mathscr{B}_W}(\Phi)$ gemeint ist!

Beispiel 3.1.10. Wir betrachten die lineare Abbildung

$$\Phi : \mathbb{R}^2 \to \mathbb{R}^3, \quad x \mapsto \begin{pmatrix} x_1 + 2x_2 \\ 3x_1 + 4x_2 \\ 5x_1 + 6x_2 \end{pmatrix}.$$

(i) Die darstellende Matrix von Φ bzgl. der Standardbasen ist wie folgt gegeben:

$$\Phi(e_1) = \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}, \Phi(e_2) = \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} \Longrightarrow D(\Phi) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$$

(ii) Wir betrachten die geordneten Basen $\mathscr{B}_1 := (e_1, e_1 + e_2)$ von $\mathbb{R}^2$ und $\mathscr{B}_2 := (e_1, e_1 + e_2, e_1 + e_2 + e_3)$ von $\mathbb{R}^3$. Es gilt

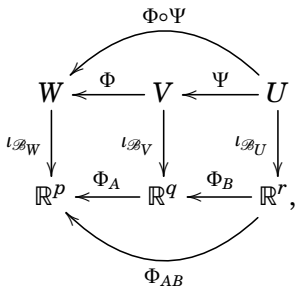
$$\begin{aligned} \Phi(e_1) &= \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} = -2e_1 - 2(e_1 + e_2) + 5(e_1 + e_2 + e_3) \\ \Phi(e_1 + e_2) &= \begin{pmatrix} 3 \\ 7 \\ 11 \end{pmatrix} = -4e_1 - 4(e_1 + e_2) + 11(e_1 + e_2 + e_3), \end{aligned}$$

und folglich

$$D_{\mathscr{B}_2, \mathscr{B}_1}(\Phi) = \begin{pmatrix} -2 & -4 \\ -2 & -4 \\ 5 & 11 \end{pmatrix}.$$

Auf den ersten Blick haben die beiden darstellenden Matrizen $D(\Phi)$ und $D_{\mathscr{B}_2, \mathscr{B}_1}(\Phi)$ nicht viel miteinander zu tun. Wir wollen uns nun überlegen, dass es hier doch einen tieferen Zusammenhang gibt.

Bemerkung 3.1.11 (Darstellende Matrix einer Verkettung)**.** Sind $\mathscr{B}_U$, $\mathscr{B}_V$ und $\mathscr{B}_W$ geordnete Basen von U, V und W, und sind $\Phi : V \to W$ und $\Psi : U \to V$ linear und setzten wir $A := D_{\mathscr{B}_W, \mathscr{B}_V}(\Phi)$ und $B := D_{\mathscr{B}_V, \mathscr{B}_U}(\Psi)$, so kommutiert das Diagramm



und daher sehen wir, dass

$$D_{\mathscr{B}_W, \mathscr{B}_U}(\Phi \circ \Psi) = D_{\mathscr{B}_W, \mathscr{B}_V}(\Phi) D_{\mathscr{B}_V, \mathscr{B}_U}(\Psi). \tag{3.1.3}$$

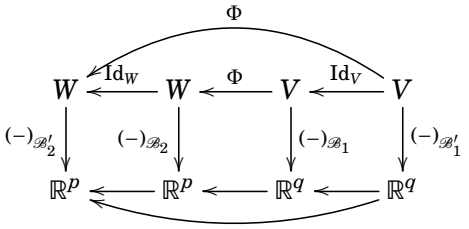
Bemerkung 3.1.12 (Basiswechsel)**.** Sei $\Phi : V \to W$, seien $\mathscr{B}_1, \mathscr{B}_1'$ zwei geordnete Basen von V und $\mathscr{B}_2, \mathscr{B}_2'$ zwei geordnete Basen von W. Wie hängen dann die darstellenden Matrizen

$$D_{\mathscr{B}_2,\mathscr{B}_1}(\Phi) \quad \text{und} \quad D_{\mathscr{B}_2',\mathscr{B}_1'}(\Phi)$$

zusammen? Wir können diese Frage nur mittels der Formel (3.1.3) beantworten, indem wir verwenden, dass $\Phi = \mathrm{Id}_W \circ \Phi \circ \mathrm{Id}_V$. Zweimaliges anwenden von (3.1.3) liefert dann

$$D_{\mathscr{B}_2',\mathscr{B}_1'}(\Phi) = D_{\mathscr{B}_2',\mathscr{B}_2}(\mathrm{Id}_W) D_{\mathscr{B}_2,\mathscr{B}_1}(\Phi) D_{\mathscr{B}_1,\mathscr{B}_1'}(\mathrm{Id}_V).$$

Dies ist die *allgemeine Basiswechselformel*. Schematisch können wir die allgemeine Basiswechselformel durch das folgende Diagramm ausdrücken:



Die Matrizen $D_{\mathscr{B}_2',\mathscr{B}_2}(\mathrm{Id}_W)$ und $D_{\mathscr{B}_1,\mathscr{B}_1'}(\mathrm{Id}_V)$ heißen die *Basiswechselmatrizen* zu den Basispaaren $(\mathscr{B}_2', \mathscr{B}_2)$ bzw. $(\mathscr{B}_1, \mathscr{B}_1')$. Basiswechselmatrizen sind stets invertierbar. Für jede Basis $\mathscr{B}$ eines Vektorraums U gilt nämlich

$$D_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_U) = \mathbf{1}$$

Es folgt daher für jede andere Basis $\mathscr{B}'$, dass

$$D_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_U) D_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_U) = D_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_U) = \mathbf{1} \quad \Longrightarrow \quad D_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_U)^{-1} = D_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_U),$$

d.h. die Inverse zur Basiswechselmatrix ist die Basiswechselmatrix zum umgekehrten Basiswechsel.

Wir betrachten nun noch einen wichtigen Spezialfall:

Beispiel 3.1.13 (Spezielle Basiswechselformel)**.** Es sei $V = \mathbb{R}^q$, $W = \mathbb{R}^p$ und $\mathscr{B}_1$ und $\mathscr{B}_2$ die Standardbasen. In diesem Fall ist $D_{\mathscr{B}_1,\mathscr{B}_1'}(\mathrm{Id}_V) =: [\mathscr{B}_1']$ einfach die Matrix, deren Spalten die Vektoren aus $\mathscr{B}_1'$ sind, und es gilt $D_{\mathscr{B}_2',\mathscr{B}_2}(\mathrm{Id}_W) = D_{\mathscr{B}_2,\mathscr{B}_2'}(\mathrm{Id}_W)^{-1} = [\mathscr{B}_2']^{-1}$. Aus der allgemeinen Basiswechselformel folgt dann die *spezielle Basiswechselformel*

$$D_{\mathscr{B}_2',\mathscr{B}_1'}(\Phi) = [\mathscr{B}_2']^{-1} D(\Phi) [\mathscr{B}_1']$$

für $\Phi : \mathbb{R}^q \to \mathbb{R}^p$, wobei die Matrix $D(\Phi)$ die darstellende Matrix bzgl. der Standardbasen ist.

Beispiel 3.1.14. Wir betrachten noch einmal Beispiel 3.1.10. Hier war $\Phi : \mathbb{R}^2 \to \mathbb{R}^3$ gegeben durch

$$D(\Phi) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix},$$

und wir hatten die Basen $\mathscr{B}_1 := (e_1, e_1+e_2)$ von $\mathbb{R}^2$ und $\mathscr{B}_2 := (e_1, e_1+e_2, e_1+e_2+e_3)$ von $\mathbb{R}^3$ betrachtet. Es gilt also

$$[\mathscr{B}_1] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad [\mathscr{B}_2] = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

und man kann nachrechnen, dass

$$[\mathscr{B}_2]^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

Daraus folgt

$$[\mathscr{B}_2]^{-1} \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} [\mathscr{B}_1] = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -2 & -4 \\ -2 & -4 \\ 5 & 11 \end{pmatrix}.$$

Dies ist aber gerade die Matrix $D_{\mathscr{B}_2,\mathscr{B}_1}(\Phi)$, die wir in Beispiel 3.1.10 berechnet haben.

Bemerkung 3.1.15 (Äquivalenz von Matrizen)**.** Ist $\Phi : V \to W$ linear und sind A und A' zwei darstellende Matrizen für Φ zu verschiedenen Basen, so existieren nach der Basiswechselformel invertierbare Matrizen S und T mit $A' = SAT$. Umgekehrt kann man zeigen (Übung 3.1.16), dass zwei Matrizen darstellende Matrizen für dieselbe lineare Abbildung sind, wenn solche Matrizen S und T existieren. In diesem Fall schreiben wir $A \approx A'$ und nennen die Matrizen A und A' *äquivalent* .

Übung 3.1.16. Zeigen Sie: Ist A eine Matrix und sind S und T invertierbare Matrizen, so ist $A' := SAT$ eine darstellende Matrix für Φ_A bzgl. geeignet gewählter Basen.

Definition 3.1.17. Ist V ein Vektorraum, so heißt eine lineare Abbildung $\Phi : V \to V$ ein *Endomorphismus*. Sie heißt ein *Automorphismus*, falls sie zusätzlich bijektiv ist.

Bemerkung 3.1.18 (Darstellende Matrix eines Endomorphismus)**.** Ist $\Phi : V \to V$ ein Endomorphismus, so bevorzugen wir darstellende Matrizen für Φ, bei denen wir zweimal *dieselbe* geordnete Basis $\mathscr{B}$ von V verwenden, also darstellende Matrizen der Form

$$\mathscr{D}_{\mathscr{B}}(\Phi) := \mathscr{D}_{\mathscr{B},\mathscr{B}}(\Phi).$$

Der Grund dafür ist, dass nur für solche Matrizen nach (3.1.3) die Gleichheit

$$\mathscr{D}_{\mathscr{B}}(\Phi^n) = \mathscr{D}_{\mathscr{B}}(\Phi)^n \tag{3.1.4}$$

gilt. Als Spezialfall der allgemeinen Basiswechselformel erhalten wir dann die folgende *Basiswechselformel für Endomorphismen*: Ist $\Phi : V \to V$ ein Endomorphismus und sind $\mathscr{B}, \mathscr{B}'$ zwei Basen von V, so gilt

$$D_{\mathscr{B}'}(\Phi) = D_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_V) D_{\mathscr{B}}(\Phi) D_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_V)^{-1} = D_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_V)^{-1} D_{\mathscr{B}}(\Phi) D_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_V).$$

Sind nun $A = D_{\mathscr{B}}(\Phi)$ und $A' = D_{\mathscr{B}'}(\Phi)$, so existiert also eine invertierbare Matrix S, so dass $A' = SAS^{-1}$. In diesem Fall schreiben wir $A \sim A'$ und nennen die beiden quadratischen Matrizen A und A' *ähnlich*. Analog zu Übung 3.1.16 zeigt man, dass zwei quadratische Matrizen genau dann ähnlich sind, wenn sie (im obigen Sinne) denselben Endomorphismus bzgl. verschiedener Basen darstellen.

Beispiel 3.1.19 (Spiegelungen diagonalisieren)**.** Sei $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ die Spiegelung an einer Ursprungsgeraden im $\mathbb{R}^2$, die mit der e_1-Achse einen Winkel $\theta \in [0, 2\pi)$ einschließt. In Übung 2.1.40 haben wir gesehen, dass die darstellende Matrix von Φ bzgl. der Standardbasis gegeben ist durch

$$D(\Phi) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}.$$

Wir können aber auch eine andere geordnete Basis von $\mathbb{R}^2$ wählen, die speziell auf unsere Spiegelung zugeschnitten ist: Es sei b_1 ein beliebiger Vektor, der die Spiegelungsachse aufspannt und b_2 ein Vektor, der die dazu senkrechte Ursprungsgerade aufspannt, so dass $\Phi(b_1) = b_1$ und $\Phi(b_2) = -b_2$. Es ist dann $\mathscr{B} := (b_1, b_2)$ eine geordnete Basis von $\mathbb{R}^2$ und

$$D_{\mathscr{B}}(\Phi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Die Matrizen

$$\begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

sind also ähnlich. Die zweite Matrix ist natürlich viel einfacher, und sie enthüllt das wahre Gesicht von Φ: Ein Vektor wird fixiert, und ein anderer am Ursprung gespiegelt. Dieser Matrix sieht man auch unmittelbar an, dass Φ^2 die Identität ist, während dies bei der anderen Matrix eine Rechnung erfordert.

Problem 3.1.20 (Normalformenproblem)**.** (i) Gegeben eine lineare Abbildung $\Phi : V \to W$, finde Basen von V und W, so dass die zugehörige darstellende Matrix von Φ möglichst einfach ist. (In Matrizensprache: Zu einer gegebenen Matrix A, finde eine äquivalente Matrix, die möglichst einfach ist.)

(ii) Gegeben einen Endomorphismus $\Phi : V \to V$, finde eine Basis von V, so dass die zugehörige darstellende Matrix von Φ möglichst einfach ist. (In Matrizensprache: Zu einer gegebenen quadratischen Matrix A, finde eine ähnliche Matrix, die möglichst einfach ist.)

Das erste Problem werden wir sehr bald (in Korollar 3.3.10), aber das zweite Problem ist sehr viel schwieriger und wird sich wie ein roter Faden durch den Rest der Linearen Algebra ziehen. Es ist bedeutsam in Anwendungen, weil es uns erlauben wird, effizient mittels (3.1.4) Potenzen von Matrizen zu berechnen.

Bemerkung 3.1.21 (Matrizen vs. lineare Abbildungen)**.** Wir haben gesehen, dass sich lineare Abbildungen zwischen endlichdimensionalen Vektorräumen nach Wahl von Basen durch Matrizen beschreiben lassen. Die Matrizentheorie ist daher zur Theorie der linearen Abbildung äquivalent. Für theoretische Zwecke ist es oft besser, mit linearen Abbildungen zu arbeiten, während man zum Rechnen meist lieber Matrizen verwendet.

[01.12.23]

Matrizen sind aber nicht nur dafür gut, um lineare Abbildungen zu beschreiben, sondern tauchen in vielen Gebieten der Mathematik in natürlicher Weise auf. Man kann dann häufig die Theorie der linearen Abbildungen heranziehen, um Probleme zu lösen, die ursprünglich nicht direkt mit linearen Abbildungen zu tun hatten. Wir geben drei Beispiele – eines haben wir bereits gesehen, auf die anderen werden wir noch zurückkommen.

Beispiel 3.1.22 (Lineare Gleichungssysteme)**.** Ist $y \in \mathbb{K}^m$ und sind $a_{11}, \dots, a_{mn} \in \mathbb{K}$, so lässt sich das LGS

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= y_1 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= y_m \end{aligned}$$

mittels der Matrix $A = (a_{ij}) \in \mathbb{K}^{m \times n}$ in *Matrix-Vektor-Schreibweise* darstellen als

$$Ax = y.$$

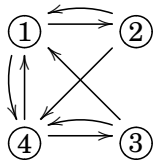
Die Lösungsmenge dieses LGS ist $L = \Phi_A^{-1}[y]$, das Lösen linearer Gleichungssysteme (in beliebig vielen Unbestimmten) ist also äquivalent zum Bestimmen der Fasern von linearen Abbildungen (zwischen Vektorräumen beliebiger endlicher Dimension).

Beispiel 3.1.23 (Pfadprobleme in Graphen)**.** In vielen praktischen Anwendungen geht es darum, Flüsse von Daten, Strom oder Gütern in Netzwerken zu untersuchen. Das mathematische Teilgebiet, dass sich mit solchen Netzwerken beschäftigt ist die sogenannte GRAPHENTHEORIE.

Das einfachst mögliche Modell eines Netzwerks ist ein sogenannter *einfacher gerichteter Graph* $\mathcal{G} = (V, E)$. Ein solcher einfacher gerichteter Graph besteht aus einer nicht-leeren Menge V und einer Teilmenge $E \subseteq V \times V$; die Elemente von V heißen *Ecken* (engl. „vertices“), die Elemente von E *Kanten* (engl. „edges“). Ab jetzt sei $\mathcal{G} = (V, E)$ ein *endlicher* einfacher gerichteter Graph; damit ist gemeint, dass V (und folglich E) endlich ist. Wir visualisieren die Ecken von $\mathcal{G}$ durch Punkte in der Ebene, und ziehen einen Pfeil von $i \in V$ zu $j \in V$, falls $(i, j) \in E$. Den Graphen

$$\mathcal{G} = (\{1,2,3,4\}, \{(1,2),(1,4),(2,1),(2,4),(3,1),(3,4),(4,1),(4,3)\})$$

können wir also z.B. so visualisieren:



Sind $v_1, v_2 \in V$, so schreiben wir $v_1 \sim v_2$, falls $(v_1, v_2) \in E$. Wir nennen $(v_1, \dots, v_{n+1}) \in V^{n+1}$ einen *Pfad* der Länge n von v_1 nach v_{n+1}, falls $v_1 \sim v_2 \sim \cdots \sim v_n \sim v_{n+1}$. Das sogenannte *Pfadproblem* der Graphentheorie fragt nun nach der Anzahl der Pfade von gegebener Länge n zwischen zwei Ecken. Z.B. gibt es im obigen Graphen 3 Pfade der Länge 3 von Ecke 2 zu Ecke 1 (nämlich (2,1,2,1), (2,1,4,1) und (2,4,3,1)).

Auf den ersten Blick hat dieses Problem nichts mit linearen Abbildungen zu tun – auf den zweiten aber doch. Dazu nummerieren wir die Eckenmenge V durch, etwa $V = \{v_1, \ldots, v_n\}$ und definieren die *Adjazenzmatrix* $A = (a_{ij})$ von $\mathscr{G}$ durch

$$a_{ij} := \begin{cases} 1, & \text{falls } (v_i, v_j) \in E \\ 0, & \text{sonst} \end{cases}$$

Im obigen Beispiel ist etwas

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

Offensichtlich gibt es von v_i nach v_j genau a_{ij} Pfade der Länge 1. In der Übung werden wir beweisen, dass der (i,j)te Eintrag der Matrix A^n genau die Anzahl der Pfade der Länge n von v_i nach v_j liefert. Um das Pfadproblem zu lösen, müssen wir also die Potenzen der Adjazenzmatrix bestimmen. Für kleine Graphen und kleine n kann man das von Hand tun, z.B. ist die Anzahl der Wege der Länge 3 im obigen Graphen gegeben durch

$$A^3 = \begin{pmatrix} 2 & 2 & 1 & 3 \\ 3 & 1 & 1 & 3 \\ 3 & 1 & 1 & 3 \\ 3 & 1 & 2 & 2 \end{pmatrix}.$$

Für große Graphen und große Werte von n benötigt man aber für eine effiziente Bestimmung Hilfsmittel aus der Theorie der linearen Abbildungen (Eigenwerte und Eigenvektoren), die wir in dieser Vorlesung entwickeln werden.

Beispiel 3.1.24 (Fibonacci-Folge)**.** Die *Fibonacci-Folge*[1] 1,1,2,3,5,8,13,… ist die eindeutig bestimmte Folge (f_n) natürlicher Zahlen mit $f_2 := f_1 := 1$, die der Rekursionsvorschrift

$$f_{n+1} = f_n + f_{n-1} \quad (n \geq 2) \tag{3.1.5}$$

genügt. Die sogenannte[2] *Formel von de Moivre-Binet* besagt, dass

$$f_n = \frac{1}{\sqrt{5}} \cdot \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Sehr überraschend taucht in dieser Formel der *goldene Schnitt* $\varphi := \frac{1+\sqrt{5}}{2}$ auf, der in der Kunst seit der Proportionenlehre der Renaissance eine zentrale Rolle spielt. Auch hier kommen überraschend Matrizen und lineare Abbildungen ins Spiel: Definieren wir $A \in \mathbb{R}^{2\times 2}$ und $v_1, v_2, \cdots \in \mathbb{R}^2$ durch

$$A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad v_n := \begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} \quad (n \in \mathbb{N}),$$

so können wir die Rekursionsvorschrift schreiben als

$$v_{n+1} = \begin{pmatrix} f_{n+2} \\ f_{n+1} \end{pmatrix} = \begin{pmatrix} f_{n+1} + f_n \\ f_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = A v_n \quad (n \in \mathbb{N}).$$

[1] Diese Folge geht auf ein klassisches Problem im *Liber abbaci* des mittelalterlichen Mathematikers Leonardo von Pisa (ca. 1170-1240), Sohn von Bonaccio ("Fibonacci") zurück.

[2] Diese Formel wurde vermutlich zuerst 1728 von Daniel Bernoulli bewiesen.

Induktiv erhalten wir die Formel

$$v_n = Av_{n-1} = A^2 v_{n-2} = \cdots = A^{n-1} v_1.$$

Auch hier müssen wir also die Potenzen einer Matrix bestimmen. Mittels der Theorie der Eigenwerte und Eigenvektoren kann man zeigen, dass

$$A^{n-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} \varphi & \varphi^{-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \varphi^{n-1} & 0 \\ 0 & (\varphi^*)^{n-1} \end{pmatrix} \begin{pmatrix} 1 & -\varphi^{-1} \\ -1 & \varphi \end{pmatrix}.$$

mit $\varphi^{-1} = \frac{1-\sqrt{5}}{2}$. Die Formel von de Moivre-Binet folgt dann unmittelbar.

Die folgende Aufgabe skizziert einen Beweis der Formel von de Moivre-Binet, der lediglich die bis hierhin entwickelte Theorie der linearen Abbildungen benutzt. (Implizit ist hier die Theorie der Eigenwerte und Eigenvektoren versteckt.)

Übung 3.1.25. Es sei V der $\mathbb{R}$-Vektorraum aller reellwertiger Folgen (a_n) mit Vektorraddition $(a_n) + (b_n) := (a_n + b_n)$ und Skalarmultiplikation $\lambda(a_n) = (\lambda a_n)$. Eine Folge $(a_n) \in V$ heißt *geometrisch* mit Basis $q \in \mathbb{R}$, falls $a_n = q^n$ und eine *verallgemeinerte Fibonacci-Folge*, falls $a_{n+2} = a_{n+1} + a_n$ für alle $n \in \mathbb{N}$. Zeigen Sie:

(a) Es gibt genau zwei geometrische verallgemeinerte Fibonacci-Folgen, nämlich $\beta_1 = (\varphi^n)$ und $\beta_2 = ((-1)^n \varphi^{-n})$, wobei die Basen durch

$$\varphi = \frac{1+\sqrt{5}}{2} \quad \text{und} \quad -\varphi^{-1} = \frac{1-\sqrt{5}}{2}$$

gegeben sind. (φ ist der berühmte *goldene Schnitt*.)

(b) Zeigen Sie, dass die Teilmenge $F \subseteq V$ der verallgemeinerten Fibonacci-Folge ein Untervektorraum ist, und dass $\mathscr{B} = (\beta_1, \beta_2)$ eine geordnete Basis von F ist.

(c) Bestimmen Sie die Koordinaten der Fibonacci-Folge bzgl. der geordneten Basis $\mathscr{B}$.

(d) Zeigen Sie, dass sich der sogenannte *Linksshift* $S : V \to V$, $S(a_n) = (a_{n+1})$ zu einem Automorphismus

$$S_F := S|_F^F : F \to F$$

einschränkt, und bestimmen Sie die darstellende Matrix $A = D_{\mathscr{B}}(S_F)$ von S_F bzgl. der geordneten Basis $\mathscr{B}$ von F.

(e) Berechnen Sie für alle $k \in \mathbb{N}$ die Matrix A^k. Bestimmen Sie daraus $S_F^k(\beta_1)$ und $S_F^k(\beta_2)$.

(f) Bestimmen Sie für alle $k \in \mathbb{N}$ die Folge $S_F^k(f_n)$, wobei (f_n) die Fibonacci-Folge ist. Folgern Sie, dass

$$f_n = \frac{1}{\sqrt{5}} \cdot \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Das soll an dieser Stelle zunächst als erste Motivation genügen. Wir werden im Folgenden zunächst einige theoretische Resultate über lineare Abbildungen zusammentragen und diese dann anschließend auf Matrixprobleme anwenden.

Zusammenfassung von Abschnitt 3.1

(1) Matrizen passender Größe lassen sich miteinander (und mit Vektoren) multiplizieren. Die Matrizenmultiplikation ist linear in beiden Variablen.

(2) Jede lineare Abbildung $\Phi : \mathbb{K}^q \to \mathbb{K}^p$ ist durch Multiplikation mit einer eindeutigen $(p \times q)$-Matrix $A = D(\Phi)$ gegeben; die Spalten von A sind genau die Bilder der Standardbasis.

(3) Allgemeiner lässt sich jede lineare Abbildung zwischen endlichdimensionalen Vektorräumen sich durch eine Matrix darstellen. Die darstellende Matrix hängt dabei von der Wahl von geordneten Basen ab, bei einer anderen Basenwahl erhält man gemäß der Basiswechselformel eine andere (aber äquivalente) Matrix.

(4) Verkettung von linearen Abbildungen entspricht der Matrixmultiplikation, solange die Basen kompatibel gewählt sind.

(5) Matrizen spielen auch unabhängig von linearen Abbildungen in vielen Bereichen der Mathematik eine Rolle, z.B. in der Theorie linearen Gleichungssysteme, in der Graphentheorie oder beim Lösen von Rekursionsgleichungen.

3.2 Kanonische Zerlegungen linearer Abbildungen

Im Folgenden sei $\Phi : V \to W$ eine beliebige lineare Abbildung. Nach Konstruktion 1.4.12 besitzt Φ eine kanonische Zerlegung in eine surjektive, bijektive und injektive Abbildung, gegeben durch

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ \mathscr{P}_\Phi & \xrightarrow[\overline{\Phi}]{} & \mathrm{Bild}(\Phi), \end{array}$$

wobei $\mathscr{P}_\Phi$ die Faserpartition zu $\Phi|^{\mathrm{Bild}(\Phi)}$ ist und die drei Abbildungen gegeben sind durch

$$\pi(x) = [x], \quad \overline{\Phi}([x]) = \Phi(x) \quad \text{und} \quad \iota(y) = y.$$

Wir wollen nun diese Zerlegung genauer betrachten.

Bemerkung 3.2.1 (Fasern einer linearen Abbildung)**.** Nach Definition ist die Faser $\Phi^{-1}(\mathbf{0})$ genau der Kern $\ker(\Phi) \leq V$ von Φ. Allgemein gilt für $x, y \in V$:

$$\Phi(x) = \Phi(y) \iff \Phi(x) - \Phi(y) = \mathbf{0} \iff \Phi(x - y) = \mathbf{0} \iff x - y \in \ker(\Phi) \iff y \in x + \ker(\Phi).$$

Ist $z \in \mathrm{Bild}(\Phi)$ und x ein beliebiges Urbild von z, so gilt also

$$\Phi^{-1}(\{z\}) = x + \ker(\Phi),$$

Die nicht-leeren Fasern von Φ sind also genau die zu $\ker(\Phi)$ parallelen affinen Unterräume von V, also

$$\mathscr{P}_\Phi = V/\ker(\Phi).$$

Speziell sind alle nicht-leeren Fasern von Φ affine Unterräume der affinen Dimension

$$\operatorname{def}(\Phi) := \dim \ker(\Phi).$$

Diese heißt auch der *Defekt* von Φ.

Da eine Abbildung genau dann injektiv ist, wenn alle ihre nicht-leeren Fasern einelementig sind, folgt daraus insbesondere:

Korollar 3.2.2 (Injektivitiätskriterium)**.** *Für eine lineare Abbildung $\Phi : V \to W$ gilt*

$$\Phi \text{ injektiv} \iff \operatorname{def}(\Phi) = 0 \iff \ker(\Phi) = \{\mathbf{0}\}. \qquad \square$$

Bemerkung 3.2.3 (Anwendung auf lineare Gleichungssysteme)**.** Ist $A \in \mathbb{K}^{p\times q}$ und $y \in \mathbb{K}^p$, so ist die Lösungsmenge des LGS $Ax = y$ genau die Faser $\Phi_A^{-1}[y]$. Diese ist also entweder leer oder ein affiner Unterraum der affinen Dimension $\operatorname{def}(A) := \operatorname{def}(\Phi_A)$ von $\mathbb{K}^q$. Ist dieser Defekt gleich 0, so gibt es zu jeder gegebenen Inhomogenität y höchstens eine Lösung.

Wir erinnern daran, dass eine injektive/surjektive lineare Abbildung auch ein Monomorphismus/Epimorphismus heißt.

Korollar 3.2.4 (Kanonische Zerlegung)**.** *Ist Φ eine lineare Abbildung mit kanonischer Zerlegung*

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ V/\ker(\Phi) & \xrightarrow[\overline{\Phi}]{} & \operatorname{Bild}(\Phi), \end{array}$$

so ist π ein Epimorphismus, $\overline{\Phi}$ ein Isomorphismus und ι ein Monomorphismus. Speziell gilt

$$\operatorname{Bild}(\Phi) \cong V/\ker(\Phi). \tag{3.2.1}$$

Beweis. Nur die Linearität von π, $\overline{\Phi}$ und ι ist zu zeigen. Letztere ist offensichtlich, und erstere wurde bereits in Proposition 2.6.4 nachgewiesen. Für $\lambda, \mu \in \mathbb{K}$ und $x, y \in V$ gilt schließlich

$$\begin{aligned} \overline{\Phi}(\lambda(x+\ker(\Phi)) + \mu(y+\ker(\Phi))) &= \overline{\Phi}(\lambda x + \mu y + \ker(\Phi)) = \Phi(\lambda x + \mu y) \\ &= \lambda\Phi(x) + \mu\Phi(y) = \lambda\overline{\Phi}(x+\ker(\Phi)) + \mu\overline{\Phi}(y+\ker(\Phi)), \end{aligned}$$

also ist auch $\overline{\Phi}$ linear. $\square$

Definition 3.2.5. Ist $\operatorname{Bild}(\Phi)$ endlich-dimensional, so heißt

$$\operatorname{rk}(\Phi) := \dim \operatorname{Bild}(\Phi)$$

der *Rang* von Φ.

Ist V endlichdimensional, so gilt nach Korollar 2.6.10, dass $\dim_{\mathbb{K}}(V/\ker(\Phi)) = \dim_{\mathbb{K}} V - \operatorname{def}(\Phi)$. Wir erhalten daher mit (3.2.1):

Korollar 3.2.6 (Rang-Defekt-Formel)**.** *Für eine lineare Abbildung $\Phi : V \to W$ mit $\dim_{\mathbb{K}}(V) < \infty$ gilt*

$$\operatorname{rk}(\Phi) = \dim(V) - \operatorname{def}(\Phi). \qquad \square$$

Dies erklärt auch den Namen Defekt: Der Defekt gibt an, wie viele Dimensionen verloren gehen, wenn man von V zu seinem Bild übergeht.

Korollar 3.2.7 (Rangkriterium)**.** *Eine lineare Abbildung $\Phi : V \to W$ mit V endlichdimensional ist genau dann injektiv, wenn* $\mathrm{rk}(\Phi) = \dim_{\mathbb{K}}(V)$ *und genau dann surjektiv, wenn* $\mathrm{rk}(\Phi) = \dim_{\mathbb{K}}(W)$.

Beweis. Die erste Aussage folgt aus Korollar 3.2.2 und Korollar 3.2.6, die zweite aus Korollar 2.5.13. □

Wir werden uns in den nächsten beiden Abschnitten genauer ansehen, wie man den Rang einer linearen Abbildung bestimmen kann. Zunächst aber erhalten wir ein überraschendes theoretisches Resultat

Korollar 3.2.8. *Es sei $\Phi : V \to W$ linear und V, W endlichdimensional.*

(i) Ist $\dim_{\mathbb{K}} V \neq \dim_{\mathbb{K}} W$*, so ist Φ kein Isomorphismus.*

(ii) ist $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W = d$*, so gilt*

$$\Phi \textit{ Isomorphismus} \iff \Phi \textit{ Monomorphismus} \iff \Phi \textit{ Epimorphismus} \iff \mathrm{rk}(\Phi) = d.$$

Beweis. (i) Korollar 2.5.6. (ii) Alle drei Bedingungen sind nach Korollar 3.2.7 äquivalent zu $\mathrm{rk}(\Phi) = \dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W$. □

Als Spezialfall von Korollar 3.2.8 erhalten wir:

Korollar 3.2.9. *Ist V endlichdimensional und besitzt ein Endomorphismus $\Phi : V \to V$ eine Links- oder Rechtsinverse Ψ, so ist Φ ein Automorphismus und $\Psi = \Phi^{-1}$.*

Wir erhalten nun eine erste Anwendung auf Matrizen. Wörtlich wie in Lemma 2.1.25 sieht man, dass das Inverse einer bijektiven linearen Abbildung Φ wieder linear ist. Ist A eine Matrix, so dass Φ_A bijektiv ist, so ist $D(\Phi_A^{-1})$ die inverse Matrix zu A. Da jede quadratische Matrix $A \in \mathbb{K}^{n\times n}$ einen Endomorphismus $\Phi_A : \mathbb{K}^n \to \mathbb{K}^n$ definiert, folgt aus Korollar 3.2.9:

Korollar 3.2.10. *Für eine quadratische Matrix $A \in \mathbb{K}^{p\times p}$ gilt*

$$A \textit{ invertierbar} \iff \exists B \in \mathbb{K}^{p\times p} : BA = \mathbf{1} \iff \exists C \in \mathbb{K}^{p\times p} : AC = \mathbf{1}.$$

In diesem Fall gilt $B = C = A^{-1}$. □

Bei unserer ersten Begegnung mit linearen Gleichungssystemen haben wir in Bemerkung 2.1.44 gelernt, durch Multiplikation mit Elementarmatrizen das Linksinverse zu einer linksinvertierbaren Matrix zu bestimmen. Wir haben dann mehrmals überrascht festgestellt, dass dieses Linksinverse „zufällig“ schon das Inverse der Matrix war. Wir verstehen nun, dass hier kein Zufall im Spiel war: Jede Links- oder Rechtsinverse einer quadratischen Matrix ist automatisch die Inverse.

Bemerkung 3.2.11 (Bijektivität von Endomorphismen)**.** Als Speziallfall von Korollar 3.2.8 erhalten wir die Aussage, dass jeder injektive oder surjektive Endomorphismus eines *endlichdimensionalen* Vektorraums V automatisch ein Automorphismus ist. Die Annahme der Endlichdimensionalität ist hier wesentlich: Es sei V der Vektorraum der Abbildungen von $\mathbb{N}$ nach $\mathbb{R}$ und

$$S : V \to V, \quad S(f)(n) := f(n+1)$$

der sogenannte *Linksshift*. Man überlegt sich dann leicht dass S ein Endomorphismus ist, der surjektiv, aber nicht injektiv ist.

Übung 3.2.12. Finden Sie analog einen Endomorphimus eines unendlichdimensionalen Vektorraums, der injektiv, aber nicht surjektiv ist. [Hinweis: „Rechtsshift“.]

Zusammenfassung von Abschnitt 3.2

(1) Jede lineare Abbildung $\Phi : V \to W$ zerlegt sich kanonisch in je einen Monomorphismus, Isomorphimsus und Epimorphismus.

(2) Die nicht-leeren Fasern von Φ sind zu $\ker(\Phi)$ parallele affine Unterräume, insbesondere ist Φ genau dann injektiv, wenn $\ker(\Phi) = \{\mathbf{0}\}$ gilt.

(3) Der Quotientenvektorraum $V/\ker(\Phi)$ ist isomorph zum Bild von Φ. Im endlichdimensionalen Fall gilt insbesondere die Rang-Defekt-Formel $\mathrm{rk}(\Phi) = \dim(V) - \mathrm{def}(\Phi)$.

(4) Sind V und W von der selben endlichen Dimension, so ist Φ genau dann ein Isomorphismus, wenn es injektiv oder surjektiv ist.

(5) Jede Links- oder Rechtsinverse einer quadratischen Matrix ist eine beidseitige Inverse.

3.3 Rang und Smith-Normalform

Wir wenden uns nun der Frage zu, wie man den Rang einer linearen Abbildung $\Phi : V \to W$ zwischen endlichdimensionalen $\mathbb{K}$-Vektorräumen V und W bestimmen kann. Wir benötigen die folgenden elementaren Beobachtungen:

Proposition 3.3.1. *Sei $(b_1, \dots, b_n)$ eine geordnete Basis von V und $\Phi : V \to W$ linear. Dann gilt:*

(i) *Φ ist durch $(\Phi(b_1), \dots, \Phi(b_n))$ eindeutig bestimmt.*

(ii) *$\{\Phi(b_1), \dots, \Phi(b_n)\}$ ist ein Erzeugendensystem von* $\mathrm{Bild}(\Phi)$.

(iii) *Φ ist genau dann surjektiv, wenn $\{\Phi(b_1), \dots, \Phi(b_n)\}$ ein Erzeugendensystem von W ist. In diesem Fall ist* $\dim_{\mathbb{K}} V \geq \dim_{\mathbb{K}} W$.

(iv) *Φ ist genau dann injektiv, wenn $\Phi(b_1), \dots, \Phi(b_n)$ linear unabhängig sind. In diesem Fall ist* $\dim_{\mathbb{K}} V \leq \dim_{\mathbb{K}} W$.

(v) *Φ ist genu dann bijektiv, wenn $(\Phi(b_1), \dots, \Phi(b_n))$ eine geordnete Basis von W ist.*

Übung 3.3.2. Beweisen Sie Proposition 3.3.1.

Definition 3.3.3. Ist $A \in \mathbb{K}^{p \times q}$ eine Matrix mit Spalten $s_1, \dots, s_q$, so heißt $\mathrm{Sp}(A) := \langle s_1, \dots, s_q \rangle \leq \mathbb{R}^p$ der *Spaltenraum* von A und $\mathrm{rk}(A) := \dim_{\mathbb{K}}(\mathrm{Sp}(A))$ der *Spaltenrang* von A.

Korollar 3.3.4. *Ist $A \in \mathbb{K}^{p \times q}$ so ist der Rang von $\Phi_A : \mathbb{K}^q \to \mathbb{K}^p$ der Spaltenrang von A, in Zeichen*

$$\mathrm{rk}(\Phi_A) = \mathrm{rk}(A)$$

Beweis. Wenden Proposition 3.3.1.(ii) auf die Standardbasis an, und beachte, dass $\Phi(e_1), \dots, \Phi(e_q)$ genau die Spalten von A sind. □

Beispiel 3.3.5 (Matrizen in Smith[3] -Normalform)**.** Wir sagen, dass eine Matrix A in *Smith-Normalform* ist, wenn sie von der Form

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

ist. Ist r die Anzahl der Einsen in einer solchen Matrix, so gilt $\mathrm{rk}(A) = r$. Es gibt also genau eine $(p \times q)$-Matrix vom Rang r in Smith-Normalform, und wir bezeichnen diese mit $\mathrm{SNF}(p,q,r)$.

Das folgende Lemma ist der Schlüssel zur konkreten Berechnung des Spaltenrangs allgemeiner Matrizen:

Lemma 3.3.6. *Es seien V, W, V', W' endlichdimensionale Vektorräume, und es seien $\Phi : V \to W$, $\Psi_1 : V' \to V$ und $\Psi_2 : W \to W'$ lineare Abbildungen. Dann gilt:*

$$\mathrm{rk}(\Psi_2 \circ \Phi \circ \Psi_1) \leq \mathrm{rk}(\Phi). \tag{3.3.1}$$

Sind Ψ_1 und Ψ_2 bijektiv, so gilt Gleichheit in (3.3.1)*.*

Beweis. Ist B eine Basis von $\mathrm{Bild}(\Phi \circ \Psi_1)$, so ist $\Psi_2(B)$ nach Proposition 3.3.1 ein Erzeugendensystem von $\mathrm{Bild}(\Psi_2 \circ \Phi \circ \Psi_1)$ und enthält daher eine Basis B' von $\mathrm{Bild}(\Psi_2 \circ \Phi \circ \Psi_1)$. Es gilt dann

$$\mathrm{rk}(\Psi_2 \circ \Phi \circ \Psi_1) = |B'| \leq |\Psi_2(B)| \leq |B| = \mathrm{rk}(\Phi \circ \Psi_1).$$

Wegen $\mathrm{Bild}(\Phi \circ \Psi_1) \subseteq \mathrm{Bild}(\Phi)$ gilt andererseits

$$\mathrm{rk}(\Phi \circ \Psi_1) \leq \mathrm{rk}(\Phi).$$

Dies zeigt (3.3.1), und sind Ψ_1 und Ψ_2 invertierbar so liefert Anwenden von (3.3.1) die Ungleichung

$$\mathrm{rk}(\Phi) = \mathrm{rk}(\Psi_2^{-1} \circ \Psi_2 \circ \Phi \circ \Psi_1 \circ \Psi_1^{-1}) \leq \mathrm{rk}(\Psi_2 \circ \Phi \circ \Psi_1),$$

woraus die Behauptung folgt. □

Aus Lemma 3.3.1 und Korollar 3.3.4 folgt sofort:

Korollar 3.3.7. *Ist $\Phi : V \to W$ linear, so gilt für jede darstellende Matrix A von Φ, dass* $\mathrm{rk}(\Phi) = \mathrm{rk}(A)$*. Insbesondere haben alle darstellenden Matrizen von Φ denselben Spaltenrang.* □

Satz 3.3.8 (Smith-Normalform)**.** *Zu jeder linearen Abbildung $\Phi : V \to W$ existieren geordnete Basen $\mathscr{B}_W$ von W und $\mathscr{B}_V$ von V, so dass $D_{\mathscr{B}_W, \mathscr{B}_V}(\Phi) = \mathrm{SNF}(p,q,r)$ in Smith-Normalform ist. Es gilt dann $p = \dim_{\mathbb{K}} W$, $q = \dim_{\mathbb{K}} V$ und $r = \mathrm{rk}(\Phi)$.*

[3] Henry John Stephen Smith (1826-1883), engl. Mathematiker

Beweis. Nach Proposition 2.4.29 existiert ein Vektorraumkomplement V' zu $\ker(\Phi)$ in V. Es sei $(v_1,\dots,v_r)$ eine geordnete Basis von V' und $(v_{r+1},\dots,v_q)$ eine geordnete Basis von $\ker(\Phi)$. Nach Proposition 2.5.15 ist dann $\mathscr{B}_V := (v_1,\dots,v_q)$ eine geordnete Basis von V. Die Abbildung

$$\Phi|_{V'} : V' \to W$$

ist injektiv, denn ist $\Phi(x) = \Phi(y)$ für $x, y \in V'$, so gilt

$$\Phi(x-y) = \mathbf{0} \quad \Longrightarrow \quad x - y \in \ker(\Phi) \cap V' = \{\mathbf{0}\} \quad \Longrightarrow \quad x = y.$$

Definieren wir also $w_i := \Phi(v_i)$ für $i \in \{1,\dots,r\}$, so ist $\{w_1,\dots,w_r\}$ linear unabhängig, und wir finden eine geordnete Basis $\mathscr{B}_W$ von W von der Form $\mathscr{B}_W := (w_1,\dots,w_p)$. Es gilt dann

$$\Phi(v_i) = \begin{cases} w_i, & \text{falls } i \in \{1,\dots,r\}, \\ \mathbf{0}, & \text{falls } i \in \{r+1,\dots,q\}, \end{cases}$$

und daher hat $D_{\mathscr{B}_W,\mathscr{B}_V}(\Phi)$ die gewünschte Form. □

Wir können Lemma 3.3.6 und Satz 3.3.8 auch in Matrizensprache formulieren.

Korollar 3.3.9 (Rang und Smith-Normalform von Matrizen)**.** *Sei $A \in \mathbb{K}^{p\times q}$.*

(i) Für alle $B \in \mathbb{K}^{p'\times p}$ und $C \in \mathbb{K}^{q\times q'}$ gilt $\operatorname{rk}(BAC) \le \operatorname{rk}(A)$.

(ii) Sind $B \in \mathbb{K}^{p\times p}$ und $C \in \mathbb{K}^{q\times q}$ beide invertierbar, so gilt $\operatorname{rk}(BAC) = \operatorname{rk}(A)$.

(iii) Es existieren invertierbare Matrizen $B \in \mathbb{K}^{p\times p}$ und $C \in \mathbb{K}^{q\times q}$, so dass $BAC = \operatorname{SNF}(p,q,\operatorname{rk}(A))$.

Wir können nun Problem 3.1.20.(i) lösen. Wir erinnern daran, dass zwei Matrizen A und A' *äquivalent* heißen (geschrieben $A \approx A'$), wenn $A' = BAC$ für invertierbare Matrizen B und C gilt.

Korollar 3.3.10 (Klassifikation der Äquivalenzklassen)**.** *Für zwei Matrizen $A, A' \in \mathbb{K}^{p\times q}$ gilt*

$$A \approx A' \iff \operatorname{rk}(A) = \operatorname{rk}(A')$$

Beweis. „$\Longrightarrow$“ folgt sofort aus Korollar 3.3.9.(ii). Gilt $\operatorname{rk}(A) = \operatorname{rk}(A') = r$, so sind A und A' beide äquivalent zu $\operatorname{SNF}(p,q,r)$, also zueinander, und daher gilt „$\Longleftarrow$“. □

Mit anderen Worten: In $\mathbb{K}^{p\times q}$ gibt es genau $\min\{p,q\}+1$ Äquivalenzklassen von Matrizen, und die Menge $\{\operatorname{SNF}(p,q,r) \mid 0 \le r \le \min\{p,q\}\}$ ist ein Repräsentantensystem für die zugehörige Partition.

[6.12.23]

Wir haben den Spaltenrang einer Matrix $A \in \mathbb{K}^{p\times q}$ als die Dimension des Spaltenraums, also der linearen Hülle der Spalten von A in $\mathbb{K}^p$ definiert. Analog definiert man den *Zeilenraum* von A als die lineare Hülle der Zeilen von A in $\mathbb{K}^{1\times q}$ und den *Zeilenrang* von A als die Dimension dieses Zeilenraums. Dies führt jedoch auf keinen wirklich neuen Begriff:

Satz 3.3.11 (Spaltenrang vs. Zeilenrang)**.** *Für jede Matrix $A \in \mathbb{K}^{p\times q}$ stimmen der Zeilenrang und der Spaltenrang überein.*

Zum Beweis ist es zweckmäßig den folgenden Begriff einzuführen:

Definition 3.3.12. Ist $A = (a_{ij}) \in \mathbb{K}^{p\times q}$, so heißt die Matrix $A^\top = (b_{ij}) \in \mathbb{K}^{q\times p}$, gegeben durch $b_{ij} := a_{ji}$, die zu A *transponierte* Matrix.

Beispiel 3.3.13. Es gilt

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

Nach Definition ist also der Zeilenrang von A gerade der Spaltenrang von $A^\top$.

Lemma 3.3.14 (Transposition als Antiautomorphismus)**.** *Für alle $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times r}$ gilt*

$$(AB)^\top = B^\top A^\top$$

Ist $p = q$ und A invertierbar, so gilt insbesondere $(A^{-1})^\top = (A^\top)^{-1} =: A^{-\top}$.

Beweis. Es sei $A = (a_{ij})$, $B = (b_{ij})$ und $C := AB = (c_{ij})$. Weiter sei $A^\top = (a'_{ij})$, $B^\top = (b'_{ij})$ und $D := B^\top A^\top = (d_{ij})$. Dann gilt

$$d_{ik} = \sum_{j=1}^{q} b'_{ij} a'_{jk} = \sum_{j=1}^{q} b_{ji} a_{kj} = \sum_{j=1}^{q} a_{kj} b_{ji} = c_{ki},$$

und daher $D = C^\top$. □

Satz 3.3.11 folgt nun unmittelbar:

Beweis von Satz 3.3.11. Ist $\mathrm{rk}(A) = r$, so existieren invertierbare Matrizen B und C mit $BAC = \mathrm{SNF}(p,q,r)$. Dann gilt aber auch

$$C^\top A^\top B^\top = (BAC)^\top = \mathrm{SNF}(p,q,r)^\top = \mathrm{SNF}(q,p,r),$$

und da $C^\top$ und $B^\top$ invertierbar sind, folgt $\mathrm{rk}(A^\top) = r$. □

Wir haben die transponierte Matrix hier als reines Hilfsmittel zum Rechnen eingeführt. Die folgenden Aufgaben klären die konzeptionelle Bedeutung dieser Rechenoperation:

Übung 3.3.15. Es seien $\Phi : V \to W$ und $\Psi : U \to V$ lineare Abbildungen. Zeigen Sie:

(i) Ist $\mu \in W^*$, so gilt $\Phi^*\mu := \mu \circ \Phi \in V^*$.

(ii) Die Abbildung $\Phi^* : W^* \to V^*$, $\mu \mapsto \Phi^*\mu$ ist linear. (Sie heißt die zu Φ *duale lineare Abbildung*).

(iii) $(\Phi \circ \Psi)^* = \Psi^* \circ \Phi^*$ und ist Φ ein Isomorphismus, so gilt $(\Phi^{-1})^* = (\Phi^*)^{-1}$.

Übung 3.3.16. Seien V und W endlichdimensional mit geordneten Basen $\mathscr{B}_V$ und $\mathscr{B}_W$ und seien $\mathscr{B}_W^*$ und $\mathscr{B}_V^*$ die dualen Basen von W^* bzw. V^*. Zeigen Sie: Ist $\Phi : V \to W$ linear, so gilt

$$D_{\mathscr{B}_V^*, \mathscr{B}_W^*}(\Phi^*) = D_{\mathscr{B}_W, \mathscr{B}_V}(\Phi)^\top.$$

Die transponierte Matrix repräsentiert also die duale Abbildung bzgl. der dualen Basen.

Wir fassen nun zum Ende dieses Abschnitts noch einmal alles zusammen, was wir in diesem Abschnitt über den Rang gelernt haben:

Satz 3.3.17. *Es seien V und W endlichdimensionale Vektorräume der Dimensionen q und p und $\Phi : V \to W$. Dann sind die folgenden Aussagen äquivalent:*

(i) $\mathrm{rk}(\Phi) = r$.

(ii) Es existiert eine darstellende Matrix A von Φ mit Spaltenrang r.

(iii) Es existiert eine darstellende Matrix A von Φ mit Zeilenrang r.

(iv) Jede darstellende Matrix A von Φ hat Spaltenrang r.

(v) Jede darstellede Matrix A von Φ hat Zeilenrang r.

(vi) Die Äquivalenzklasse der darstellenden Matrizen von Φ wird repräsentiert von $\mathrm{SNF}(p, q, r)$.

In Kombination mit Korollar 3.2.8 folgt daraus (wegen $\mathrm{SNF}(p, p, p) = \mathbf{1}_p$):

Korollar 3.3.18. *Für eine quadratische Matrix $A \in \mathbb{K}^{p \times p}$ sind äquivalent:*

(i) A ist invertierbar.

(ii) A hat Spaltenrang p.

(iii) A hat Zeilenrang p.

(iv) Es existieren invertierbare Matrizen S und T mit $SAT = \mathbf{1}_p$.

Zusammenfassung von Abschnitt 3.3

(1) Der Rang einer linearen Abbildung stimmt mit dem Spaltenrang und Zeilenrang einer beliebigen darstellenden Matrix überein.

(2) Äquivalente Matrizen haben denselben Rang, und die Äquivalenzklasse einer Matrix ist durch ihren Rang eindeutig bestimmt.

(3) Jede Äquivalenzklasse von Matrizen besitzt einen eindeutigen Repräsentanten in Smith-Normalform.

3.4 Matrixalgorithmen

In diesem Abschnitt diskutieren wir verschiedene grundlegende Algorithmen für Matrizen. Diese werden es uns erlauben,

(i) den Rang einer beliebigen Matrix zu bestimmen;

(ii) das Inverse zu einer beliebigen invertierbaren Matrix zu bestimmen;

(iii) die Lösungsmenge eines beliebigen linearen Gleichungssystems zu bestimmen.

Die hier vorgestellten Algorithmen sind allesamt sehr einfach gestrickt und in keiner Weise optimiert. Sie haben den Vorteil, dass sie sich in kleinen Fällen sehr leicht per Hand durchführen lassen. In der Praxis gibt es weit bessere Algorithmen, und natürlich lässt man die von seinem Computer durchführen und führt sie nicht selber durch. Wichtig ist, dass Sie theoretisch verstehen, wie diese Algorithmen funktionieren, denn die Prinzipien dahinter sind für die Lineare Algebra fundamental. Alle unsere Algorithmen basieren auf Elementarmatrizen, die die in Abschnitt 2.1 eingeführten (2×2)-Elementarmatrizen verallgemeinern.

Beispiel 3.4.1 (Elementarmatrizen)**.** In $\mathbb{K}^{p\times p}$ betrachten wir die folgenden speziellen Matrizen:

(1) Eine Matrix mit genau einer 1 in jeder Zeile und Spalte und sonst nur 0en heißt eine *Permutationsmatrix* (weil die zugehörige lineare Abbildung die Vektoren der Standardbasis „permutiert“, also miteinander vertauscht). Speziell heißt für $1 \le i < j \le p$ die Permutationsmatrix

$$S_{ij} := (e_1, \dots, e_{i-1}, e_j, e_{i+1}, \dots, e_{j-1}, e_i, e_{j+1}, \dots, e_p)$$

eine *Transpositionsmatrix*. Linksmultiplikation mit S_{ij} vertauscht in einer Matrix die i-te und j-te Zeile, Rechtsmultiplikation mit S_{ij} vertauscht die i-te und j-te Spalte. Insbesondere gilt $S_{ij}^2 = \mathbf{1}$, also ist S_{ij} invertierbar mit $S_{ij}^{-1} = S_{ij}$.

(2) Für zwei verschiedene Elemente $i, j \in \{1, \dots, p\}$ und $t \in \mathbb{R}$ definieren wir die *unipotenten Elementarmatrix* $U_{ij}(t)$ durch

$$U_{ij}(t) := \mathbf{1}_p + tE_{ij}.$$

Linksmultiplikation mit $U_{ij}(t)$ addiert das t-fache der j-ten Zeile zur i-ten. Rechtsmultiplikation entspricht analog dem Dazuaddieren des t-fachen der $i$ten Spalte zur j-ten, und $U_{ij}(t)$ ist invertierbar mit $U_{ij}(t)^{-1} = U_{ij}(-t)$.

(3) Für $\lambda_1, \dots, \lambda_p \in \mathbb{K}$ heißt die Matrix

$$\operatorname{diag}(\lambda_1, \dots, \lambda_p) := \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_p \end{pmatrix}$$

eine *Diagonalmatrix*. Links-/Rechtsmultiplikation mit $\operatorname{diag}(\lambda_1, \dots, \lambda_p)$ multipliziert die j-te Zeile/Spalte mit λ_j, und $\operatorname{diag}(\lambda_1, \dots, \lambda_p)$ ist invertierbar genau dann, wenn $\lambda_j \neq 0$ für alle $j \in \{1, \dots, p\}$, und in diesem Fall ist

$$\operatorname{diag}(\lambda_1, \dots, \lambda_p)^{-1} = \operatorname{diag}(\lambda_1^{-1}, \dots, \lambda_p^{-1}).$$

Definition 3.4.2. Die Multiplikation einer gegebenen Matrix A mit einer invertierbaren Elementarmatrix von links (bzw. von rechts) bezeichnen wir als *elementare Zeilenumformung* (bzw. elementare Spaltenumformung).

Satz 3.4.3 (Smith-Gauß-Algorithmus)**.** *Jede Matrix $A \in \mathbb{K}^{p\times q}$ lässt sich durch elementare Zeilen- und Spaltenumformungen in eine Matrix in Smith-Normalform überführen.*

Beweis. Wir argumentieren mit Induktion nach der Anzahl p der Zeilen. Ist $p = 0$, so ist nichts zu zeigen. Ist A nicht die Nullmatrix, so kann man die Spalten so permutieren, dass die erste Spalte nicht nur 0en enthält. Nach Zeilenpermutation ist dann der Eintrag an der Stelle (1,1) nicht 0 und kann auf 1 normiert werden. Durch Subtrahieren geeigneter Vielfacher der ersten Zeile von den anderen Zeilen erhält man dann eine Matrix der Form

$$\begin{pmatrix} 1 & a_{12} & \dots & a_{1q} \\ 0 & b_{11} & \dots & b_{1,q-1} \\ \vdots & \vdots & & \vdots \\ 0 & b_{p-1,1} & \dots & b_{p-1,q-1} \end{pmatrix} \quad \text{mit } B = (b_{ij}) \in \mathbb{K}^{p-1,q-1}.$$

Durch Subtrahieren von Vielfachen der ersten von den anderen Spalten können wir erreichen, dass $a_{12} = \dots = a_{1q} = 0$. Nach Induktionsvorraussetzung können wir nun B durch Zeilen- und Spaltenumformungen auf Smith-Normalform bringen. Führen wir die entsprechenden Umformungen an der großen Matrix A aus, so werden dabei lediglich die Einträge $a_{12},\dots,a_{1q}$ in Mitleidenschaft gezogen, da diese aber bereits 0 waren, passiert hier nichts mehr. Bringen wir B auf diese Weise auf Smith-Normalform $\mathrm{SNF}(p-1,q-1,r)$, so haben wir A auf die Smith-Normalform $\mathrm{SNF}(p,q,r+1)$ gebracht. □

Der Beweis von Satz 3.4.3 ist konstruktiv und ermöglicht die Rangbestimmung einer Matrix in konkreten Fällen. Da Matrixmultiplikationen von links mit Matrixmultiplikationen von rechts vertauschen, kann man stets *zuerst* Zeilenumformungen und dann Spaltenumformungen durchführen. Wir führen dies in einem Beispiel vor:

Beispiel 3.4.4. Sei Φ eine lineare Abbildung mit darstellender Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 9 \end{pmatrix}$$

bzgl. irgendwelcher Basen. Mittels Zeilenumformungen formen wir A um zu

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} =: A'.$$

Weitere Spaltenumformungen liefern nun

$$A' = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \mathrm{SNF}(3,3,2).$$

Insbesondere gilt dann

$$\mathrm{rk}(\Phi) = \mathrm{rk}(A) = \mathrm{rk}(A') = \mathrm{rk}(\mathrm{SNF}(3,3,2)) = 2.$$

Bemerkung 3.4.5 (Invertierbarer Fall)**.** Ist $A \in \mathbb{K}^{p\times p}$ so besagt Satz 3.4.3, dass man A mittels elementarer Zeilen- und Spaltenumformungen in die Matrix $\mathrm{SNF}(p,p,p) = \mathbf{1}_p$ überführen kann. Wir finden also in diesem Fall invertierbare Elementarmatrizen $X_1,\dots,X_m,Y_1,\dots,Y_n$

$$X_1\cdots X_m A Y_1\cdots Y_n = \mathbf{1}_p.$$

Wir können dies umschreiben als

$$A = X_m^{-1}\cdots X_1^{-1}Y_n^{-1}\cdots Y_1^{-1} \iff Y_1\cdots Y_n X_1\cdots X_m A = \mathbf{1}_p \iff AY_1\cdots Y_n X_1\cdots X_m = \mathbf{1}_p.$$

Damit haben wir das folgende Korollar bewiesen.

Korollar 3.4.6. *Jede invertierbare Matrix $A \in \mathbb{K}^{p\times p}$ ist ein Produkt invertierbarer Elementarmatrizen und lässt sich durch elementare Zeilenumformungen (oder durch elementare Spaltenumformungen) in die Einheitsmatrix überführen.* □

Bemerkung 3.4.7 (Explizites Invertieren einer Matrix)**.** Ist $A \in \mathbb{K}^{p\times p}$ eine invertierbare Matrix und sind $X_1,\dots,X_n$ invertierbare Elementarmatrizen mit $X_1\cdots X_n A = \mathbf{1}_p$, so gilt wegen Korollar 3.2.10, dass $A^{-1} = X_1\cdots X_n\mathbf{1}$. Man erhält also A^{-1} indem man an der Einheitsmatrix dieselben Zeilenumformungen durchführt, die man braucht, um A selbst auf die Einheitsmatrix zu bringen.

Beispiel 3.4.8. Wir bestimmen die Inverse der Matrix

$$A := \begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & -2 \\ 0 & -1 & 1 \end{pmatrix}$$

durch simultane Zeilenumformungen an A und der Einheitsmatrix:

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

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

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 2 & -2 \\ 0 & -5 & 4 \\ 0 & -1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 2 & -2 \\ 0 & -1 & 1 \\ 0 & -5 & 4 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -2 & 0 \end{pmatrix}$$

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & -1 \\ 0 & -5 & 4 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & -2 & 0 \end{pmatrix}$$

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & -1 \\ 1 & -2 & -5 \end{pmatrix}$$

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & -1 \\ -1 & 2 & 5 \end{pmatrix}$$

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ -1 & 2 & 4 \\ -1 & 2 & 5 \end{pmatrix}.$$

Wir erhalten also

$$A^{-1} = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 2 & 4 \\ -1 & 2 & 5 \end{pmatrix}.$$

Bemerkung 3.4.9 (Zeilen- vs. Spaltenumformungen)**.** Sei $A \in \mathbb{K}^{p \times p}$ eine quadratische Matrix. Finden wir invertierbare Elementarmatrizen $Y_1, \ldots, Y_n$ mit $AY_1 \cdots Y_n = \mathbf{1}$, so gilt wegen Korollar 3.2.10, dass $A^{-1} = \mathbf{1}Y_1 \cdots Y_n$. Man erhält also A^{-1}, indem man an der Einheitsmatrix dieselben Spaltenumformungen durchführt, die man braucht, um A selbst auf die Einheitsmatrix zu bringen.

Beispiel 3.4.10. Wir können die Inverse der obigen Matrix A auch durch Spaltenumformungen bestimmen, z.B. so:

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

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

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

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

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

$$\rightsquigarrow \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ -1 & 2 & 4 \\ -1 & 2 & 5 \end{pmatrix}$$

WARNUNG! Man darf Zeilen- und Spaltenumformungen im Allgemeinen nicht mischen. Ist nämlich $X_1 \cdots X_n A Y_1 \cdots Y_n = \mathbf{1}$, so kann man daraus *nicht* schließen, dass $X_1 \cdots X_n \mathbf{1} Y_1 \cdots Y_n$ die Inverse zu A ist. Stattdessen erhält man

$$AY_1 \cdots Y_n = X_n^{-1} \cdots X_1^{-1} \Longrightarrow A = X_n^{-1} \cdots X_1^{-1} Y_n^{-1} \cdots Y_1^{-1} \Longrightarrow A^{-1} = Y_1 \cdots Y_n X_1 \cdots X_n.$$

Man kann das schreiben als $A^{-1} = Y_1 \cdots Y_n \mathbf{1} X_1 \cdots X_n$ oder als $A^{-1} = \mathbf{1} Y_1 \cdots Y_n X_1 \cdots X_n \mathbf{1}$. Verwendet man die erste Formel, so führt man für jede Zeilenumformung von A eine entsprechende Spaltenumformung an der Einheitsmatrix durch und umgekehrt - und das auch noch in

umgekehrter Reihenfolge. Folgt man der zweiten Interpretation, so führt man an einer Einheitsmatrix die Zeilenumformungen durch und an einer anderen die Spaltenumformungen und multipliziert die Ergebnisse am Ende. Das Fehlerpotential ist in beiden Fällen hoch. Wir empfehlen nachdrücklich, von solchen Verfahren die Finger zu lassen!

Bemerkung 3.4.11 (Elementare Zeilenumformungen und lineare Gleichungssysteme)**.** Gegeben sei ein LGS in Matrix-Vektor-Form, also

$$Ax = y \quad \text{mit } A \in \mathbb{K}^{p\times q}, y \in \mathbb{K}^p. \tag{3.4.1}$$

Ist X eine invertierbare Elementarmatrix, so ist (3.4.1) äquivalent zu

$$(XA)x = (Xy).$$

Wir ändern die Lösungsmenge also nicht, wenn wir simultan elementare Zeilenumformungen an A und y vornehmen. Buchführungstechnisch ist es zweckmäßig, die *erweiterte Matrix* $\widetilde{A} \in \mathbb{K}^{p\times(q+1)}$ zu bilden, indem wir y als letzte Spalte an A anhängen. Wir können dann das System durch elementare Zeilenumformungen an $\widetilde{A}$ vereinfachen; wir führen dies zunächst an einem Beispiel vor.

Beispiel 3.4.12. Wir betrachten das rationale LGS

$$\begin{aligned} x_1 + 2x_2 + 2x_3 + 3x_4 &= 1,\\ 4x_1 + 8x_2 + 5x_3 + 6x_4 &= 2,\\ 5x_1 + 10x_2 + 7x_3 + 9x_4 &= 3, \end{aligned}$$

mit 4 Variablen und 3 Gleichungen. In Matrix-Vektor-Schreibweise können wir dies schreiben als

$$\underbrace{\begin{pmatrix} 1 & 2 & 2 & 3\\ 4 & 8 & 5 & 6\\ 5 & 10 & 7 & 9 \end{pmatrix}}_{=:A} x = \underbrace{\begin{pmatrix} 1\\ 2\\ 3 \end{pmatrix}}_{=:y}, \tag{3.4.2}$$

wobei nun $x \in \mathbb{Q}^4$ gesucht ist. Die erweiterte Matrix ist

$$\widetilde{A} := \begin{pmatrix} 1 & 2 & 2 & 3 & 1\\ 4 & 8 & 5 & 6 & 2\\ 5 & 10 & 7 & 9 & 3 \end{pmatrix}$$

und wir nehmen elementare Zeilenumformungen wie folgt vor:

$$\begin{aligned} \widetilde{A} &= \begin{pmatrix} 1 & 2 & 2 & 3 & 1\\ 4 & 8 & 5 & 6 & 2\\ 5 & 10 & 7 & 9 & 3 \end{pmatrix}\\ &\rightsquigarrow \begin{pmatrix} 1 & 2 & 2 & 3 & 1\\ 0 & 0 & -3 & -6 & -2\\ 0 & 0 & -3 & -6 & -2 \end{pmatrix}\\ &\rightsquigarrow \begin{pmatrix} 1 & 2 & 2 & 3 & 1\\ 0 & 0 & -3 & -6 & -2\\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Das LGS (3.4.2) ist daher äquivalent zu

$$\begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 0 & -3 & -6 \\ 0 & 0 & 0 & 0 \end{pmatrix} x = \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}.$$

oder ausgeschrieben,

$$\begin{aligned} x_1 + 2x_2 + 2x_3 + 3x_4 &= 1, \\ -3x_3 - 6x_4 &= -2, \\ 0 &= 0. \end{aligned}$$

Die letzte Zeile ist offensichtlich redundant. Wir können nun $x_2 = s$ und $x_4 = t$ frei wählen und erhalten

$$\begin{aligned} x_1 &= 1 - 2s - 2x_3 - 3t, \\ x_3 &= 2/3 - 2t. \end{aligned}$$

Einsetzen der zweiten Gleichung in die erste liefert

$$x_1 = 1 - 2s - 2(2/3 - 2t) - 3t = -1/3 - 2s + t.$$

Die Lösungsmenge ist daher gegeben durch die affine Ebene

$$L = \left\{ \begin{pmatrix} -1/3 - 2s + t \\ s \\ 2/3 - 2t \\ t \end{pmatrix} \mid s,t \in \mathbb{Q} \right\} = \begin{pmatrix} -1/3 \\ 0 \\ 2/3 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \end{pmatrix} \right\rangle \subseteq \mathbb{Q}^4.$$

In diesem Fall haben wir die erweiterte Matrix durch elementare Zeilenumformungen in

$$\widetilde{A}' := \begin{pmatrix} 1 & 2 & 2 & 3 & 1 \\ 0 & 0 & -3 & -6 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

überführt. Diese Matrix ist nicht in Smith-Normalform (um dahin zu kommen, bräuchten wir zusätzlich elementare Spaltenumformungen), aber doch einfach genug, um die Lösungsmenge des LGS direkt abzulesen. Wir wollen uns nun überlegen, dass man jede beliebige Matrix durch elementare Zeilenumformungen in eine solche Form bringen kann.

Definition 3.4.13. Eine Matrix $A = (a_{ij}) \in \mathbb{K}^{p \times q}$ ist in *Zeilenstufenform*, falls entweder $A = \mathbf{0}$ gilt oder Elemente $r \in \{1,\dots,p\}$ und $j_1,\dots,j_r \in \mathbb{N}$ mit $1 \le j_1 < \cdots < j_r \le q$ existieren, sodass für alle $i \in \{1,\dots,p\}$ und $j \in \{1,\dots,q\}$ gilt:

(i) $i > r \implies a_{ij} = 0$.

(ii) $(i \in \{1,\dots,r\}) \wedge (j < j_i) \implies a_{ij} = 0$.

(iii) $i \in \{1,\dots,r\} \implies a_{ij_i} \neq 0$.

Schematisch sieht eine Matrix in Zeilenstufenform also wie folgt aus:

$$\begin{pmatrix}
0 & \dots & 0 & a_{1j_1} & * & \dots & \dots & \dots & \dots & \dots & \dots & \dots & * \\
0 & \dots & \dots & \dots & \dots & 0 & a_{2j_2} & * & \dots & \dots & \dots & \dots & * \\
\vdots & & & & & & & & & & & & \vdots \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & a_{rj_r} & * & \dots & * \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\
\vdots & & & & & & & & & & & & \vdots \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0
\end{pmatrix}$$

Der (Zeilen-)Rang dieser Matrix ist offensichtlich r, und es gibt genau r von 0 verschiedene Zeilen, wobei jede Zeile tiefer eingerückt ist als die vorhergehende.

Proposition 3.4.14 (Gauß-Algorithmus)**.** *Jede Matrix A lässt sich durch Linksmultiplikation mit unipotenten Elementarmatrizen und Permutationsmatrizen auf Zeilenstufenform bringen.*

Beweis. Ist $A = \mathbf{0}$ so sind wir fertig. Andernfalls sei j_1 die erste Spalte, die nicht nur 0en enthält. Durch Permutieren von Zeilen kann man dann erreichen, dass $a_{1j_1} \neq 0$. Durch Abziehen geeigneter Vielfacher der ersten Zeile von den anderen Zeilen erreicht man nun, dass $a_{ij_1} = 0$ für $i > 1$. Damit hat man nun eine Matrix der folgenden Form erreicht:

$$\begin{pmatrix}
0 & \dots & 0 & a_{1j_1} & * & \dots & \dots & \dots & * \\
0 & \dots & \dots & 0 & * & \dots & \dots & \dots & * \\
\vdots & & & \vdots & \vdots & & & & \vdots \\
0 & \dots & \dots & 0 & * & \dots & \dots & \dots & *
\end{pmatrix}$$

Nun betrachtet man die Matrix, die aus allen Zeilen außer der ersten und allen Spalten außer den Spalten 1 bis j_1 besteht usw. Nach endlich vielen Schritten erreicht man eine Matrix in Zeilenstufenform. □

Die Tatsache, dass wir hier nur unipotente Elementarmatrizen und Permutationsmatrizen, aber keine Diagonalmatrizen verwenden, wird sich später bei der Berechnung von Determinanten noch als nützlich erweisen.

Der Beweis von Proposition 3.4.14 ist formal etwas unbefriedigend, weil wir eigentlich nur einen Schritt ausgeführt haben und uns dann mit einem „usw." beholfen haben. Wenn man formal ganz korrekt sein will, muss man hier eine vollständige Induktion durchführen. Für die Formalisten unter Ihnen sei hier ein ganz formaler Beweis nachgeliefert:

Formaler Beweis von Proposition 3.4.14: Für diesen Beweis nennen wir eine Zeilenumformung „speziell", wenn sie durch Linksmultiplikation mit einer unipotenten Elementarmatrix oder Permutationsmatrix entsteht. Es sei $P(n)$ die Aussage

$P(n) \quad :\Longleftrightarrow$ Jede Matrix mit höchstens n Spalten lässt sich durch spezielle Zeilenumformungen auf Zeilenstufenform bringen.

Wir beweisen mit vollständiger Induktion, dass $P(n)$ für alle $n \in \mathbb{N}$ gilt.

Wir betrachten zunächst den Fall $n = 1$. Sei also A eine Matrix mit einer Spalte. Ist $A = \mathbf{0}$, so sind wir fertig. Andernfalls finden wir einen Eintrag a_{i1} mit $a_{i1} \neq 0$. Durch Permutieren von Zeilen kann man dann erreichen, dass $a_{11} \neq 0$. Durch Abziehen geeigneter Vielfacher der ersten Zeile von den anderen Zeilen erreicht man nun, dass $a_{i1} = 0$ für $i > 1$, also hat A Zeilenstufenform. Dies zeigt $P(1)$.

Wir zeigen nun $P(n)$ für $n \geq 2$ unter der Annahme, dass $P(n-1)$ (und insbesondere $P(1)$) gilt. Sei also A eine Matrix mit n Spalten (und p Zeilen) und erster Spalte

$$s_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{p1} \end{pmatrix}.$$

Weil $P(1)$ gilt, können wir spezielle Zeilenumformungen auf s_1 anwenden, die s_1 in Zeilenstufenform überführen. Wenden wir nun dieselben speziellen Zeilenumformungen auf A an, so erhalten wir eine Matrix der Form

$$A' = \begin{pmatrix} a'_{11} & * & \dots & * \\ 0 & b_{11} & \dots & b_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & b_{p-1,1} & \dots & b_{p,n-1} \end{pmatrix}.$$

Die Matrix $B = (b_{ij})$ hat nun $(n-1)$ Spalten. Da $P(n-1)$ gilt, können wir nun spezielle Zeilenumformungen auf B anwenden, so dass die resultierende Matrix $B' = (b'_{i,j})$ in Zeilenstufenform ist. Dann ist aber auch die Matrix

$$A'' = \begin{pmatrix} a'_{11} & * & \dots & * \\ 0 & b'_{11} & \dots & b'_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & b'_{p-1,1} & \dots & b'_{p,n-1} \end{pmatrix}$$

in Zeilenstufenform, und da diese aus A' (und daher aus A) durch spezielle Zeilenumformungen hervorgeht, sind wir fertig. □

Bemerkung 3.4.15. Das im Beweis von Proposition 3.4.14 präsentierte Verfahren ist eine Form des aus der Schule bekannten *Gauß-Algorithmus*. Das Verfahren ist ähnlich dem bereits diskutierten Gauß-Smith-Algorithmus, allerdings wenden wir hier ausschließlich Zeilenumformungen an – daher ist die Matrix, die wir am Ende erhalten auch nicht ganz so schön wie eine Matrix in Smith-Normalform.

Streng genommen haben wir im Beweis keinen Algorithmus angegeben, weil wir nicht festgelegt haben, welche Zeile wir nach oben permutieren, wenn es in der entsprechenden Spalte mehrere Einträge gibt, die alle nicht 0 sind. Man könnte aus dem Beweis einen Algorithmus gewinnen, indem man z.B. immer die erste oder immer die letzte mögliche Zeile nach oben permutiert. Raffiniertere Wahlen können den Algorithmus beschleunigen. Mehr dazu lernen sie in einer Einführungsvorlesung zur NUMERISCHEN MATHEMATIK. (Dort lernen Sie aber auch, dass der Gauß-Algorithmus zum praktischen Rechnen oft zu langsam ist - bessere Verfahren benötigen Methoden aus der Vorlesung LINEARE ALGEBRA II.)

Bemerkung 3.4.16. Wie löst man nun also ein LGS? Man schreibt das LGS zunächst in Matrix-Vektor-Form

$$Ax = y, \quad x \in \mathbb{K}^q, y \in \mathbb{K}^p, A \in \mathbb{K}^{p \times q}.$$

und stellt die erweiterte Matrix $\widetilde{A}$ auf. Durch „Gaußen“, also Linksmultiplikation mit unipotenten Elementarmatrizen und Permutationsmatrizen (d.h. entsprechenden Zeilenumformungen an $\widetilde{A}$), erhält man ein äquivalentes LGS

$$A'x = y' \tag{3.4.3}$$

mit der Eigenschaft, dass die aus A' und y' gebildete erweiterte Matrix $\widetilde{A}'$ in Zeilenstufenform ist. Nun gibt es 2 Fälle:

FALL 1. $r := \mathrm{rk}(\widetilde{A}) > \mathrm{rk}(A)$.
In diesem Fall gilt auch $\mathrm{rk}(\widetilde{A}') > \mathrm{rk}(A')$, da sich der Rang unter Multiplikation mit invertierbaren Matrizen nicht ändert. Die r-te Zeile des LGS (3.4.3) liefert dann eine unerfüllbare Bedingung der Form $0 = a_{rj_r}$. Die Lösungsmenge ist also in diesem Fall leer.

FALL 2. $r := \mathrm{rk}(\widetilde{A}) = \mathrm{rk}(A)$.
In diesem Fall gilt auch $\mathrm{rk}(\widetilde{A}') = \mathrm{rk}(A')$. Alle Zeilen unterhalb der r-ten liefern dann die Bedingung $0 = 0$, die immer erfüllt ist. Die r-te Zeile ist von der Form

$$a_{rj_r}x_{j_r} + \cdots + a_{rq}x_q = y_r.$$

Wenn wir $x_{j_r+1}, \ldots, x_q$ beliebig wählen, dann erhalten wir eine Formel für x_{j_r}. Die $(r-1)$-te Zeile lautet nun

$$a_{r-1,j_{r-1}}x_{j_{r-1}} + \cdots + a_{(r-1)q}x_q = y_{r-1}.$$

Die hinteren Variablen ab x_{j_r} sind alle bereits gewählt oder bestimmt, die mittleren Variablen $x_{j_{r-1}+1}, \ldots, x_{r_j-1}$ können wir wieder frei wählen und für die Variable $x_{j_{r-1}}$ erhalten wir dann eine Formel durch Auflösen. Analog arbeiten wir die Zeilen $r-2, \ldots, r-3, \ldots, 1$ ab. Am Ende haben wir alle Variablen mit Ausnahme von $x_{j_1}, x_{j_2}, \ldots, x_{j_r}$ frei gewählt und für letztere eine Formel bestimmt. Damit ist die Lösungsmenge vollständig beschrieben. Sie ist, wie wir bereits vorher wussten, ein affiner Unterraum der Dimension $q - \mathrm{rk}(A)$ (denn das ist die Anzahl der frei gewählten Variablen).

Wir halten fest:

Proposition 3.4.17. *Dass LGS $Ax = y$ mit Matrix $A \in \mathbb{K}^{p\times q}$ und erweiterter Matrix $\widetilde{A}$ ist genau dann lösbar, wenn* $\mathrm{rk}(A) = \mathrm{rk}(\widetilde{A})$ *gilt, und in diesem Fall ist die Lösungsmenge ein affiner Unterraum der affinen Dimension $q - \mathrm{rk}(A)$.* □

Zusammenfassung von Abschnitt 3.4

(1) Elementare Zeilen-/Spaltenumformungen von Matrizen sind Links-/Rechtsmultiplikationen mit Elementarmatrizen.

(2) Mittels elementarer Zeilen- und Spaltenumformungen kann man jede Matrix auf Smith-Normalform bringen (Gauß-Smith Algorithmus) und dadurch ihren Rang bestimmen.

(3) Mittels elementarer Zeilenumformungen (oder Spaltenumformungen) kann man jede invertierbare Matrix invertieren.

(4) Mittels elementarer Zeilenumformungen kann man jede Matrix auf Zeilenstufenform bringen (Gauß-Algorithmus). Damit kann man die Lösungsmengen beliebiger linearer Gleichungssysteme bestimmen.

3.5 Zerlegungen von linearen Abbildungen und Matrizen

Eine der wichtigsten Techniken der fortgeschrittenen Linearen Algebra ist das Zerlegen von komplizierten Matrizen in einfachere Grundbausteine. Wir wollen davon einen ersten Eindruck

geben. Wir haben bereits gesehen, dass man jede invertierbare quadratische Matrix in ein Produkt invertierbarer Elementarmatrizen zerlegen kann. Dieses Resultat wollen wir nun noch ein wenig verfeinern, um eine erste berühmte Matrizenzerlegung zu erhalten. Weitere wichtige Zerlegungen werden wir in der LINEAREN ALGEBRA II diskutieren.

Definition 3.5.1. Eine Matrix der Form

$$\begin{pmatrix} b_{11} & * & \dots & * \\ 0 & b_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & b_{pp} \end{pmatrix}$$

heißt eine *oberer Dreiecksmatrix* mit *Diagonaleinträgen* $b_{11},\dots,b_{pp}$. Sie heißt *unipotente obere Dreiecksmatrix*, wenn alle Diagonaleinträge 1 sind.

Man überlegt sich leicht, dass eine obere Dreiecksmatrix genau dann invertierbar ist, wenn keiner ihrer Diagonaleinträge gleich 0 ist. Typische Beispiele sind unipotente Elementarmatrizen $U_{ij}(t)$ mit $i < j$; wir nennen diese Matrizen *obere unipotente Elementarmatrizen*.

Übung 3.5.2. Zeigen Sie: Produkte und Inverse von invertierbaren oberen Dreiecksmatrizen sind wieder obere Dreiecksmatrizen. Analog sind Produkte und Inverse von invertierbaren unipotenten oberen Dreiecksmatrizen wieder unipotente obere Dreiecksmatrizen.

Aus Proposition 3.4.14 folgt sofort:

Korollar 3.5.3. *Ist $A \in \mathbb{K}^{p\times p}$ invertierbar, so existieren unipotente Elementarmatrizen und Permutationsmatrizen $X_1,\dots,X_n$, so dass $X_1\cdots X_nA$ eine invertierbare obere Dreiecksmatrix ist.*

Beweis. Nach Proposition 3.4.14 können wir A in Zeilenstufenform bringen. Wegen $\mathrm{rk}(A) = p$ hat die resultierende Matrix genau p Stufen, ist also eine invertierbare obere Dreiecksmatrix. □

Wir können dieses Ergebnis noch etwas verfeinern:

Proposition 3.5.4. *Ist $A \in \mathbb{K}^{p\times p}$ invertierbar, so existieren obere unipotente Elementarmatrizen $X_1,\dots,X_n$ und eine Permutationsmatrix P, so dass $PX_n\cdots X_1A$ eine invertierbare obere Dreiecksmatrix ist.*

Beweis. Multiplikation mit einer oberen unipotenten Elementarmatrix bedeutet gerade, dass man eine Zeile zu einer darüberliegenden Zeile addiert. Wir wollen nun sehen, wie wir A mittels solcher Multiplikationen vereinfachen können.

Da A vollen Rang hat, ist die erste Spalten nicht $\mathbf{0}$. Wir wählen nun zunächst die *unterste* Zeile, die in der ersten Spalte einen Eintrag $\neq 0$ hat und ziehen geeignete Vielfache dieser Zeile von den darüberliegenden Zeilen ab; diese liefert obere unipotente Elementarmatrizen $X_1,\cdots X_k$, so dass

$$X_k\cdots X_1A = \begin{pmatrix} 0 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ 0 & \vdots & & \vdots \\ * & \vdots & & \vdots \\ 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & * & \dots & * \end{pmatrix}.$$

Analog räumt man jetzt die folgenden Spalten ab: Man wählt nun unter den *anderen* Zeilen die unterste mit einem Eintrag $\neq 0$ in der zweiten Spalte, und räumt damit alle darüberliegenden Zeilen ab. Nach r solchen Schritten findet man eine Matrix mit höchstens j von 0 verschiedenen Einträgen in der j-ten Spalte. Schematisch sieht eine solche Matrix etwa so aus:

$$\begin{pmatrix} 0 & * & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & * & * \\ * & * & * & * \end{pmatrix}.$$

Durch eine Zeilenpermutation (gegeben durch eine Permutationsmatrix P) wird daraus eine invertierbare obere Dreiecksmatrix. □

Korollar 3.5.5 (Bruhat[4]-Zerlegung)**.** *Für jede invertierbare Matrix $A \in \mathbb{K}^{p\times p}$ existieren invertierbare obere Dreiecksmatrizen B_1, B_2 und eine Permutationsmatrix W mit $A = B_1 W B_2$. Die Matrix B_1 kann zusätzlich unipotent gewählt werden.*

Beweis. Wähle $P, X_1, \ldots, X_n$ wie in der Proposition und setze $B_2 := PX_n \cdots X_1 A$. Dann gilt

$$A = \underbrace{X_1^{-1} \cdots X_n^{-1}}_{=:B_1} \underbrace{P^{-1}}_{=:W} B_2,$$

und dies liefert die gewünschte Zerlegung. □

Der Beweis zeigt, dass wir B_1 stets mit 1en auf der Diagonale wählen können. Jede Zerlegung von A in Matrizen wie in Korollar 3.5.5 heißt eine *Bruhat-Zerlegung* von A.

[4] François Georges René Bruhat, frz. Mathematiker (1929-2007)

[8.12.23]

Beispiel 3.5.6. Wir betrachten die (invertierbare) Matrix

$$A := \begin{pmatrix} 6 & 11 & 19 \\ 4 & 6 & 10 \\ 2 & 3 & 4 \end{pmatrix} \in \mathbb{R}^{3\times 3}.$$

Multiplizieren wir A mit $U_{13}(-3)U_{23}(-2)$, so erhalten wir

$$U_{13}(-3)U_{23}(-2)\begin{pmatrix} 6 & 11 & 19 \\ 4 & 6 & 10 \\ 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 7 \\ 0 & 0 & 2 \\ 2 & 3 & 4 \end{pmatrix}$$

Vertauschen wir nun zuerst die zweite und dritte Zeile, und dann die erste und zweite Zeile, so erhalten wir

$$P_{12}P_{23}U_{13}(-3)U_{23}(-2)A = P_{12}\begin{pmatrix} 0 & 2 & 7 \\ 2 & 3 & 4 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 \\ 0 & 2 & 7 \\ 0 & 0 & 2 \end{pmatrix} =: B_2.$$

Eine Bruhat-Zerlegung von A ist daher gegeben durch

$$A = B_1 W B_2$$

mit

$$W := P_{23}^{-1}P_{12}^{-1} = P_{23}P_{12} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

und

$$B_1 := U_{23}(-2)^{-1}U_{13}(-3)^{-1} = U_{23}(2)U_{13}(3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

In der Tat rechnet man leicht nach, dass

$$\begin{pmatrix} 6 & 11 & 19 \\ 4 & 6 & 10 \\ 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 2 & 3 & 4 \\ 0 & 2 & 7 \\ 0 & 0 & 2 \end{pmatrix}.$$

Bemerkung 3.5.7 (Nicht-Eindeutigkeit der Bruhat-Zerlegung)**.** Die Bruhat-Zerlegung einer invertierbaren Matrix ist nicht eindeutig. Z.B. ist auch

$$\begin{pmatrix} 6 & 11 & 19 \\ 4 & 6 & 10 \\ 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 2 & 3 & 4 \\ 0 & 2 & 3 \\ 0 & 0 & 2 \end{pmatrix}.$$

eine Bruhat-Zerlegung der Matrix aus dem letzten Beispiel. Man kann aber immerhin zeigen, dass die Permutationsmatrix W durch A eindeutig bestimmt ist. Sind nämlich

$$A = B_1 W B_2 = B_1' W' B_2'$$

zwei Bruhat-Zerlegungen von A, so sind $C_1 := (B_1')^{-1}B_1$ und $C_2 := B_2'B_2^{-1}$ invertierbare obere Dreiecksmatrizen mit

$$C_1 W = W' C_2.$$

Dies ist aber nur möglich, wenn $W = W'$, weil sonst C_1W und $W'C_2$ verschiedene Gestalt haben (Übung!).

Übung 3.5.8 (Birkhoff-Zerlegung)**.** Eine Matrix, die transponiert zu einer invertierbaren oberen Dreiecksmatrix ist, heißt *invertierbare untere Dreiecksmatrix*. Zeigen Sie für eine invertierbare Matrix $A \in \mathbb{K}^{p\times p}$ die folgenden Aussagen:

(a) $A = B_1 W B_2$, wobei B_1 und B_2 invertierbare untere Dreiecksmatrizen und W eine Permutationsmatrix ist. Dabei kann B_1 oder B_2 unipotent gewählt werden. [Hinweis: Dies folgt sofort aus der Bruhat-Zeregung - warum?].

(b) $A = B_1 W B_2$, wobei B_1 eine invertierbare untere Dreiecksmatrix, B_2 eine invertierbare obere Dreiecksmatrix und W eine Permutationsmatrix ist. Dabei kann B_1 oder B_2 als unipotent gewählt werden. Eine solche Zerlegung heißt *Birkhoff*[5]*-Zerlegung* von A. [Hinweis: Imitieren Sie den Beweis der Bruhat-Zerlegung.]

Die Bruhat- und Birkhoff-Zerlegung sind fundamentale Zerlegungen in der Theorie der algebraischen Gruppen, ihre volle Bedeutung wurde erst in den 1960er Jahren durch JACQUES TITS[6] im Rahmen seiner Theorie der sogenannten Gebäude erkannt. Sie wurden (wie viele andere Matrixzerlegungen) zuerst aus theoretischen Gründen studiert, und Jahrzehnte später zu Beginn des Computer-Zeitalters von Anwendern (meist unter anderem Namen) wiederentdeckt. In der numerischen Mathematik ist die Birkhoff-Zerlegung unter dem Namen „LR-Zerlegung“ (für „Links-Rechts-Zerlegung“ bzw. „left-right decomposition“) bekannt.

Bemerkung 3.5.9. Die Bruhat- und Birkhoff-Zerlegung behandeln ausschließlich invertierbare Matrizen. Was können wir über nicht-invertierbare Matrizen sagen? Ist $A \in \mathbb{K}^{p\times q}$ eine nicht-invertierbare Matrix vom Rang r, so existieren invertierbare Matrixen $S \in \mathbb{K}^{p\times p}$ und $T \in \mathbb{K}^{q\times q}$, so dass $A = S \cdot \mathrm{SNF}(p,q,r) \cdot T$. Die Matrizen S und T kann man als Produkte (spezieller) invertierbarer Elementarmatrizen schreiben, z.B. via Bruhat- oder Birkhoff-Zerlegung. Geometrisch entsprechen diese Matrizen Streckungen, Stauchungen, Spiegelungen und Scherungen. Wie kann man nun die Matrix $\mathrm{SNF}(p,q,r)$ geometrisch interpretieren?

Beispiel 3.5.10 (Projektionen)**.** Sind $U, W < V$ mit $V = U \oplus W$, so existieren für jedes $v \in V$ genau ein $u(v) \in U$ und $w(v) \in W$ mit $v = u(v) + w(v)$. Die Abbildung

$$\pi_U^W : V \to V, \quad v \mapsto u(v)$$

ist dann linear, also ein Endomorphismus von V. Sie heißt die *Projektion* auf U entlang W. Es gilt $\ker(\pi_U^W) = W$ und $\mathrm{Bild}(\pi_U^W) = U$. Wählt man geordnete Basen $(u_1,\dots,u_m)$ von U und $(w_1,\dots,w_n)$ von W, so ist $\mathscr{B} = (u_1,\dots,u_m,w_1,\dots,w_n)$ eine geordnete Basis von V, und es gilt

$$D_{\mathscr{B}}(\pi_U^W) = SNF(m+n, m+n, m).$$

Korollar 3.5.11. *Jeder Endomorphismus von $\mathbb{K}^n$ ist eine Verkettung von Streckungen, Stauchungen, Spiegelungen, Scherungen und Projektionen.* □

Kombiniert man Beispiel 3.5.10 mit Satz 2.4.29, so erhält man:

Korollar 3.5.12. *Für jeden Unterraum $U \le V$ existieren Endomorphismen π_1, π_2 von V mit* $\ker(\pi_1) = U = \mathrm{Bild}(\pi_2)$. □

[5] George David Birkhoff (1884-1944), US-amerikanischer Mathematiker, Vater des ebenfalls berühmten US-Mathematikers Garrett Birkhoff (1911-1996) und mein Doktor-Ur-Ur-Urgroßvater

[6] belgischer Mathematiker, 1930-2021

Projektionen besitzen eine Reihe interessanter Charakterisierungen:

Proposition 3.5.13 (Projektionen als Idempotente)**.** *Für einen Endomorphismus $\pi : V \to V$ sind die folgenden Aussagen äquivalent:*

(i) *π ist eine Projektion.*

(ii) *π ist* idempotent*, d.h. $\pi^2 = \pi$.*

(iii) *$\ker(\pi) \cap \mathrm{Bild}(\pi) = \{\mathbf{0}\}$ und $\pi(u) = u$ für alle $u \in \mathrm{Bild}(\pi)$.*

(iv) *$V = \ker(\pi) \oplus \mathrm{Bild}(\pi)$ und $\pi(u) = u$ für alle $u \in \mathrm{Bild}(\pi)$.*

In diesem Fall gilt $\pi = \pi_U^W$ mit $W := \ker(\pi)$ und $U := Bild(\pi)$.

Beweis. (i) $\Longrightarrow$ (ii): Ist $\pi = \pi_U^W$, so gilt in der obigen Notation, dass $\pi(v) = u(v)$ und daher $\pi^2(v) = \pi(u(v)) = u(v) = \pi(v)$, also $\pi^2 = \pi$.

(ii) $\Longrightarrow$ (iii): Sei $u \in \mathrm{Bild}(\pi)$. Wähle $x \in V$ mit $\pi(x) = u$. Es gilt dann $\pi(u) = \pi^2(x) = \pi(x) = u$. Ist speziell $u \in \ker(\pi) \cap \mathrm{Bild}(\pi)$, so gilt $u = \pi(u) = \mathbf{0}$.

(iii) $\Longrightarrow$ (iv): Nach (iii) ist die Summe $\ker(\pi) \oplus \mathrm{Bild}(\pi)$ direkt. Nach Korollar 3.2.6 ist die Dimension dieser Summe gerade $\dim V$, und mit Korollar 2.5.13 folgt $\ker(\pi) \oplus \mathrm{Bild}(\pi) = V$.

(iv) $\Longrightarrow$ (i): Setzen wir $W := \ker(\pi)$ und $U := \mathrm{Bild}(\pi)$, so ist $V = U \oplus W$, und ist $v = u + w$ mit $u \in U$ und $w \in W$, so gilt nach Annahme $\pi(u) = u$. Nach Definition des Kerns ist $\pi(w) = \mathbf{0}$, also $\pi(v) = u = \pi_U^W(v)$. □

Dasselbe Argument zeigt (Übung!):

Korollar 3.5.14. *Für einen Endomorphismus $\pi : V \to V$ mit $W := \ker(\pi)$ und $U := Bild(\pi)$ sind äquivalent:*

(i) *$U \cap W = \{\mathbf{0}\}$.*

(ii) *$V = U \oplus W$.*

(iii) *Es existiert ein Automorphismus $\psi : U \to U$, so dass $\pi(x) = \psi(\pi_U^W(x))$ für alle $x \in V$.*

Es hält sich - insbesondere auch in Klausuren - hartnäckig das Gerücht[7], dass für *jeden* Endomorphismus π schon $V = \mathrm{Bild}(\pi) \oplus \ker(\pi)$ gilt (sogenannte „Erstemesterzerlegung“). Das ist aber nicht der Fall, wie das folgende Beispiel zeigt:

Beispiel 3.5.15. Betrachte die lineare Abbildung $\Phi = \Phi_A : \mathbb{R}^2 \to \mathbb{R}^2$ mit darstellender Matrix

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

In diesem Fall ist $A^2 = \mathbf{0}$, also $\Phi^2 = \mathbf{0}$ und daher $\ker(\Phi^2) = \mathbb{R}^2$, aber wegen $\Phi \neq \mathbf{0}$ ist $\ker(\Phi) \neq \mathbb{R}^2$. In diesem Fall gilt $\ker(\Phi) = \mathbb{R}e_1 = \mathrm{Bild}(\Phi)$, und insbesondere ist die Summe von Kern und Bild nicht direkt.

[7] Ich vermute, dass hier die Rang-Defekt-Formel falsch verstanden wurde. Bitte machen Sie diesen Fehler nicht!

Zusammenfassung von Abschnitt 3.5

(1) Die Bruhat- und Birkhoff-Zerlegung sind wichtige Zerlegungen invertierbarer Matrizen und beruhen auf einer verfeinerten Versionen des Gauß-Algorithmus.

(2) Beliebige Endomorphismens lassen sich in Streckungen, Stauchungen, Spiegelungen, Scherungen und Projektionen zerlegen.

(3) Projektionen sind genau die linearen Abbildungen mit $\pi^2 = \pi$, und für diese gilt stets die „Erstsemesterzerlegung“ $V = \mathrm{Bild}(\pi) \oplus \ker(\pi)$.

4 Determinanten

4.1 Prolog: Permutationen endlicher Mengen

Definition 4.1.1. Ist M eine Menge, so heißt eine bijektive Abbildung $\sigma : M \to M$ eine *Permutation* von M.

Im folgenden bezeichen wir die Menge aller Permutationen von M mit $\mathrm{Sym}(M)$. Wir interessieren uns besonders für Permutationen *endlicher* Mengen. Ist $M = \{1, \dots, n\}$, so schreiben wir kurz Sym_n für $\mathrm{Sym}(M)$.

Bemerkung 4.1.2 (Beschreibung von Permutationen in Sym_n, Teil I)**.** Wir können Elemente von Sym_n auf verschiedene Arten beschreiben. Wir geben zunächst zwei einfache Möglichkeiten an:

(i) als *Tabellen*: Wir schreiben $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ für σ. Die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ bildet z.B. 4 auf 1 ab. Diese Darstellung ist sehr explizit, aber zum praktischen Rechnen oft wenig geeignet.

(ii) als *Zöpfe*: Wir stellen eine Permutation graphisch dar, indem wir zweimal n Punkte übereinander malen, und jeweils den n-ten Punkt oben mit dem $\sigma(n)$-ten Punkt unten verbinden. Abbildung 4.1 zeigt einen Zopf, der die Permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ repräsentiert.

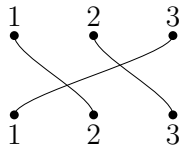


Abbildung 4.1: Ein Zopf

Die Verkettung von Permutation entspricht dann dem Verketten von Zöpfen, wobei man auf die Reihenfolge achten muss: Der Zopf zu $\sigma_1 \circ \sigma_2$ entsteht, indem man den Zopf von σ_1 unten an den Zopf von σ_2 anhängt und das resultierende Bild „gerade zieht“.

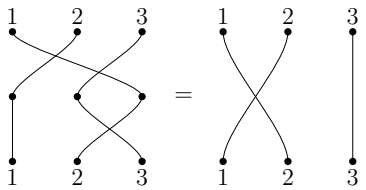


Abbildung 4.2: Verkettung zweier Zöpfe

Abbildung 4.2 zeigt, wie ein Zopf zu $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ aus den Zöpfen von $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ und $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ entsteht. Beachte, dass der Zopf von $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ oben steht.

Wir werden später noch bessere Beschreibungen für Elemente von Sym_n geben. Dazu benötigen wir die folgende Beobachtung.

Lemma 4.1.3 (Rekurrenz)**.** *Ist $\sigma\in\mathrm{Sym}_n$ und $j\in\{1,\dots,n\}$ so existiert ein $m\in\mathbb{N}$ mit $\sigma^m(j)=j$.*

Beweis. Das *Schubfachprinzip* besagt[1]: Teilt man mehr als n Elemente auf n „Schubladen“ auf, so liegen in einer Schublade mindestens 2 Elemente. Es gibt unendlich viele natürliche Zahlen $l\in\mathbb{N}$, aber nur endlich viele mögliche Werte von $\sigma^l(j)$, also muss es nach dem Schubfachprinzip zwei verschiedenen $l_1,l_2\in\mathbb{N}$ geben mit $\sigma^{l_1}(j)=\sigma^{l_2}(j)$, und wir dürfen annehmen, dass $l_1<l_2$ gilt. Dann ist aber

$$\sigma^{l_2-l_1}(j)=\sigma^{-l_1}(\sigma^{l_2}(j))=\sigma^{-l_1}(\sigma^{l_1}(j))=j,$$

also können wir $m:=l_2-l_1$ wählen. □

Bemerkung 4.1.4 (Bahnen)**.** Ist $\sigma\in\mathrm{Sym}_n$, so heißt eine Menge $M\subseteq\{1,\dots,n\}$ *σ-invariant*, falls $\sigma(M)=M$. Wir konstruieren solche Mengen wie folgt: Für $j\in\{1,\dots,n\}$ sei $m\in\mathbb{N}$ minimal mit $\sigma^m(j)=j$. Wir definieren dann die *Bahn* von j unter σ als $B_j:=\{j,\sigma(j),\dots,\sigma^{m-1}(j)\}$.

Die Elemente $j,\sigma(j),\dots,\sigma^{m-1}(j)$ sind alle verschieden, denn wäre $\sigma^k(j)=\sigma^l(j)$ mit $0\le k<l<m-1$, so wäre $\sigma^{l-k}(j)=j$ und $1\le l-k<m$, im Widerspruch zur Minimalität von m. Es gilt also $|B_j|=m$, und wir nennen m die *Bahnlänge* von j unter σ. Jedes der Elemente $j,\sigma(j),\dots,\sigma^{m-1}(j)$ wird unter σ auf das nächste abgebildet, und das letzte Element $\sigma^{m-1}(j)$ wieder auf das erste. Schematisch gilt also

$$\begin{array}{ccccccc} j & \longrightarrow & \sigma(j) & \longrightarrow & \dots & \longrightarrow & \sigma^{k-1}(j)\\ \uparrow & & & & & & \downarrow\\ \sigma^{m-1}(j) & \longleftarrow & \sigma^{m-2}(j) & \longleftarrow & \dots & \longleftarrow & \sigma^k(j)\end{array}$$

Insbesondere ist B_j invariant unter σ und σ^{-1}, also positiven und negativen Potenzen von σ.

Übung 4.1.5. Zeigen Sie, dass eine Teilmenge $M\subseteq\{1,\dots,n\}$ genau dann invariant unter σ ist, wenn sie eine Vereinigung von Bahnen ist. Insbesondere ist sie dann auch invariant unter σ^n für alle $n\in\mathbb{Z}$.

Proposition 4.1.6 (Bahnenpartition)**.** *Die Bahnen von σ bilden eine Partition $\mathscr{B}_\sigma$ von $\{1,\dots,n\}$.*

Beweis. Aus der Definition ist sofort klar, dass $\emptyset\notin\mathscr{B}_\sigma\neq\emptyset$ und $\bigcup\mathscr{B}_\sigma=\{1,\dots,n\}$. Sei nun

$$B_j\cap B_k\neq\emptyset.$$

Dann existiert $i\in B_j\cap B_k$, also gibt es $a,b\in\mathbb{N}$ mit

$$\sigma^a(j)=i=\sigma^b(k)\Longrightarrow\sigma^{a-b}(j)=k\Longrightarrow k\in B_j\Longrightarrow\forall\,n\in\mathbb{N}:\sigma^n(k)\in B_j\Longrightarrow B_k\subseteq B_j.$$

Analog zeigt man $B_j\subseteq B_k$, also $B_j=B_k$. □

[1] Allgemeiner sagt das Schubfachprinzip: Ist M eine Menge, die echt mächtiger als eine Menge N ist, so gibt es keine injektive Abbildung von M nach N

Beispiel 4.1.7. Wir betrachten die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 5 & 4 \end{pmatrix} \in \mathrm{Sym}_6. \tag{4.1.1}$$

Wegen $1 \mapsto 6 \mapsto 4 \mapsto 1$, $2 \mapsto 3 \mapsto 2$ und $5 \mapsto 5$ ist die Bahnenpartition von σ durch

$$\mathscr{B}_\sigma = \{\{1,4,6\},\{2,3\},\{5\}\}$$

gegeben. Schematisch können wir σ darstellen als

Notation 4.1.8. Sei $\sigma \in \mathrm{Sym}_n$. Wir nennen $j \in \{1,\dots,n\}$ einen *Fixpunkt* von σ, falls $\sigma(j) = j$ (also $|B_j| = 1$) und bezeichnen mit $\mathrm{Fix}(\sigma)$ die Menge der Fixpunkte von σ. Das Komplement $\mathrm{supp}(\sigma) := \{1,\dots,n\} \setminus \mathrm{Fix}(\sigma)$ heißt der *Träger* (engl. „support“) von σ uns ist nach Proposition 4.1.6 gerade die Vereinigung der *nicht-trivialen Bahnen* (also Bahnen der Länge ≥ 2).

Beispiel 4.1.9 (Zykel)**.** Eine Permutation, die genau eine nicht-triviale Bahn besitzt, heißt ein *Zykel*. Wir bezeichnen mit $(j_1,\dots,j_m)$ den Zykel, der j_1 auf j_2, j_2 auf j_3, ... und j_m auf j_1 abbildet, also ist z.B.

$$(1,3,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 1 \end{pmatrix}.$$

Wir nennen dann m die *Zykellänge* von $(j_1,\dots,j_m)$; Zykel der Länge 2 heißen *Transpositionen*. Wir nennen zwei Zykel σ_1,σ_2 *disjunkt*, wenn ihre Träger diskunkt sind. In diesem Fall gilt $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$, da beide Permutationen auf dem Träger von σ_j durch σ_j operieren. Allgemeiner gilt: Sind $\sigma_1,\dots,\sigma_n$ paarweise disjunkte Zykel, so ist $\sigma_1 \cdots \dots \sigma_n$ die Permutation, die auf dem Träger von σ_j durch σ_j operiert.

Beispiel 4.1.10. Die Permutation (4.1.1) operiert auf ihren beiden nicht-trivialen Bahnen durch die Zykel (1,6,4) bzw. (2,3). Es gilt also

$$\sigma = (1,6,4) \circ (2,3) = (2,3) \circ (1,6,4).$$

Statt (1,6,4) kann man auch (6,4,1) oder (4,1,6) (aber nicht (1,4,6)) schreiben.

Diese Art von Zerlegung funktioniert ganz allgemein:

Bemerkung 4.1.11 (Zykelzerlegung)**.** Jede nicht-triviale Permutation $\sigma \in \mathrm{Sym}_k$ lässt sich als Produkt disjunkter Zykel $\sigma_1,\dots,\sigma_k$ schreiben. Dazu numeriert man einfach die nicht-trivialen Bahnen von σ als $B_1,\dots,B_k$ durch und wählt in jeder Bahn B_j einen Startpunkt x_j; dann setzt man $\sigma_j = (x, \sigma(x), \dots, \sigma^{m-1}(x))$, wobei $m = |B_j|$. Da die verschiedenen Bahnen disjunkt sind, sind die Zykel $\sigma_1,\dots,\sigma_k$, und nach Konstruktion macht $\sigma_1 \cdots \sigma_k$ auf jeder Bahn B_j dasselbe wie σ (nämlich σ_j).

Da $\sigma_1,\dots,\sigma_k$ vertauschen, ist die Reihenfolge nicht eindeutig. Es gilt also z.B.

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_k = \sigma_2 \circ \sigma_1 \circ \sigma_3 \circ \cdots \circ \sigma_k = \sigma_k \circ \cdots \circ \sigma_1.$$

Bis auf Reihenfolge ist die Zerlegung aber eindeutig (Übung!).

Wenn man bereit ist, die Eindeutigkeit aufzugeben, kann man diese Zerlegung noch weiter verfeinern.

Bemerkung 4.1.12 (Zerlegung in Transpositionen)**.** Es seien $j_1,\dots,j_m \in \{1,\dots,n\}$ paarweise verschieden. Wir betrachten die Permutation

$$\sigma := (j_1,j_2)\circ(j_2,j_3)\circ\cdots\circ(j_{m-1},j_m).$$

Alle $j \in \{1,\dots,n\}\setminus\{j_1,\dots,j_m\}$ sind Fixpunkte von σ, und die Wirkung von σ auf $j_1,\dots,j_m$ ist wie folgt:

$$\begin{array}{ccccccccccc}
j_1 & \mapsto & j_1 & \mapsto & j_1 & \mapsto & \dots & \mapsto & j_1 & \mapsto & j_2 \\
j_2 & \mapsto & j_2 & \mapsto & j_2 & \mapsto & \dots & \mapsto & j_3 & \mapsto & j_3 \\
\vdots & & & & & & & & & & \vdots \\
j_{m-1} & \mapsto & j_m & \mapsto & j_m & \mapsto & \dots & \mapsto & j_m & \mapsto & j_m \\
j_m & \mapsto & j_{m-1} & \mapsto & j_{m-2} & \mapsto & \dots & \mapsto & j_2 & \mapsto & j_1.
\end{array}$$

Dies zeigt, dass

$$(j_1,\dots,j_m) = (j_1,j_2)\circ(j_2,j_3)\circ\cdots\circ(j_{m-1},j_m).$$

Man kann daher jede nicht-triviale Permutation als Produkt von Transpositionen schreiben, z.B.

$$\begin{pmatrix}1&2&3&4&5&6\\6&3&2&1&5&4\end{pmatrix} = (1,6,4)\circ(2,3) = (1,6)\circ(6,4)\circ(2,3).$$

Das ist zum Rechnen sehr praktisch, es gelten nämlich die folgenden einfachen Rechenregeln: Zunächst ist $(i,j)\circ(i,j) = \mathrm{Id}$, außerdem gilt

$$(i,j)\circ(k,l) = (k,l)\circ(i,j), \text{ falls } \{i,j\}\cap\{k,l\} = \emptyset,$$

und die *Zopfrelation* (Abbildung 4.3)

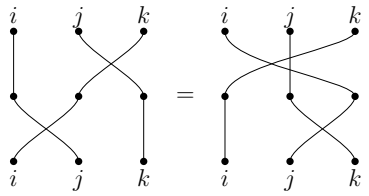


Abbildung 4.3: Zopfrelation

$$(i,j)\circ(j,k) = (j,k)\circ(k,i),$$

Mit diesen Rechenregeln kann man Produkte von Transpositionen oft in eine einfache Form bringen.

Wir haben nun also vier Darstellungen für Permutationen in Sym_n kennengelernt: Als Tabellen, als Zöpfe, als Zykelprodukte und als Produkte von Transpositionen.

Bemerkung 4.1.13 (Fehlstände)**.** Es seien $i,j \in \{1,\dots,n\}$ und $\sigma \in \mathrm{Sym}_n$. Wir nennen (i,j) einen *Fehlstand* von σ, falls $i < j$, aber $\sigma(i) > \sigma(j)$. Im zugehörigen Zopf bedeutet dies gerade, dass sich die Stränge von i nach $\sigma(i)$ und j nach $\sigma(j)$ schneiden. Die Anzahl $q(\sigma)$ der Fehlstände von σ ist also genau die Anzahl der Kreuzungen des Zopfes von σ.

Wir kommen nun zum entscheidenden Begriff dieses Abschnitts:

Definition 4.1.14. Das *Signum* von $\sigma \in \mathrm{Sym}_n$ ist definiert als

$$\mathrm{sgn}(\sigma) := (-1)^{q(\sigma)},$$

wobei $q(\sigma)$ die Anzahl der Fehlstände von σ ist.

Lemma 4.1.15. *Für alle $\sigma \in \mathrm{Sym}_n$ gilt*

$$\mathrm{sgn}(\sigma) = \frac{\prod_{1\le i<j\le n}(\sigma(j)-\sigma(i))}{\prod_{1\le i<j\le n}(j-i)}. \tag{4.1.2}$$

Beweis. Wegen $\sigma(\{1,\dots,n\}) = \{1,\dots,n\}$ sind die Faktoren im Zähler und Nenner bis auf Reihenfolge und Vorzeichen dieselben - jede Differenz taucht genau einmal auf - also ist das Produkt 1 oder -1. Das Vorzeichen von $(\sigma(j)-\sigma(i))/(j-i)$ ist genau dann negativ, wenn (i,j) ein Fehlstand ist, also erhält man für jeden Fehlstand ein Vorzeichen und daher insgesamt $(-1)^{q(\sigma)}$. □

Formel 4.1.2 ist für das praktische Rechnen unbrauchbar, da auf der rechten Seite einfach viel zu viele Terme stehen. Aus dieser Formel lässt sich aber die folgende Aussage beweisen, mit der man das Signum praktisch berechnen kann.

Proposition 4.1.16 (Multiplikativität)**.** *Es gilt* $\mathrm{sgn}(\mathrm{Id}) = 1$ *und für* $\sigma,\tau \in \mathrm{Sym}_n$ *gilt*

$$\mathrm{sgn}(\sigma\circ\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

Bevor wir das beweisen, wollen wir uns überlegen, wie man damit das Signum praktisch berechnen kann.

Bemerkung 4.1.17 (Signumsberechnung)**.** Ist (i,j) eine Transposition mit $1 \le i < j \le n$, so ist stets $\mathrm{sgn}((i,j)) = -1$. Für die Transposition (1,2) ist dies klar, da $q((1,2)) = 1$. im Allgemeinen gilt aber

$$(i,j) = (i,1)(j,2)(1,2)(i,1)(j,2) \Rightarrow \mathrm{sgn}((i,j)) = \mathrm{sgn}((i,1))^2\mathrm{sgn}((j,2))^2\mathrm{sgn}((1,2)) = -1.$$

Ist nun σ eine beliebige Permutation, so ist entweder $\sigma = \mathrm{Id}$ und daher $\mathrm{sgn}(\sigma) = 1$, oder σ lässt sich als Produkt von Zykeln schreiben. Es ist dann $\mathrm{sgn}(\sigma) = 1$ genau dann, wenn σ ein Produkt von einer *geraden* Anzahl Transpositionen ist.

Ist nun $(j_1,\dots,j_m)$ ein Zykel der Länge m, so ist wegen der Multiplikativität

$$\mathrm{sgn}((j_1,\dots,j_m)) = \mathrm{sgn}((j_1,j_2)\circ\cdots\circ(j_{m-1},j_m)) = \mathrm{sgn}((j_1,j_2))\cdots\mathrm{sgn}(j_{m-1},j_m) = (-1)^{m+1}.$$

Zykel gerader Länge haben also Signum -1 und Zykel ungerader Länge haben Signum 1. Nochmaliges Anwenden der Multiplikativität liefert dann den folgenden Satz.

Satz 4.1.18. *Eine Permutation $\sigma \in \mathrm{Sym}_n$ hat genau dann Signum* 1*, wenn die Anzahl der Zykel von gerader Länge in ihrer Zykelzerlegung gerade ist.* □

Man kann also das Signum direkt aus der Zykelzerlegung ablesen, und die Zykelzerlegung lässt sich sehr schnell berechnen.

Beweis von Proposition 4.1.16. Die Formel $\operatorname{sgn}(\mathrm{Id}) = 1$ ist klar. Seien nun $\sigma, \tau \in \mathrm{Sym}_n$. Dann gilt

$$\operatorname{sgn}(\sigma \circ \tau) = \frac{\prod_{1 \le i < j \le n} (\sigma \circ \tau(j) - \sigma \circ \tau(i))}{\prod_{1 \le i < j \le n} (j - i)} = \frac{\prod_{1 \le i < j \le n} (\sigma(\tau(j)) - \sigma(\tau(i)))}{\prod_{1 \le i < j \le n} (\tau(j) - \tau(i))} \underbrace{\frac{\prod_{1 \le i < j \le n} (\tau(j) - \tau(i))}{\prod_{1 \le i < j \le n} (j - i)}}_{= \operatorname{sgn}(\tau)}.$$

Wegen

$$\frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)},$$

und da τ bijektiv ist, kann man die Reihenfolge im ersten Faktor umsortieren zu

$$\frac{\prod_{1 \le i < j \le n} (\sigma(\tau(j)) - \sigma(\tau(i)))}{\prod_{1 \le i < j \le n} (\tau(j) - \tau(i))} = \frac{\prod_{1 \le \tau(i) < \tau(j) \le n} (\sigma(\tau(j)) - \sigma(\tau(i)))}{\prod_{1 \le \tau(i) < \tau(j) \le n} (\tau(j) - \tau(i))} = \frac{\prod_{1 \le i < j \le n} (\sigma(j) - \sigma(i))}{\prod_{1 \le i < j \le n} (j - i)},$$

also ist der erste Faktor gerade $\operatorname{sgn}(\sigma)$, und daher $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. □

Zusammenfassung von Abschnitt 4.1

(1) Permutationen endlicher Mengen lassen sich in Produkte von Transpositionen oder (eindeutig bis auf Reihenfolge) in disjunkte Zykel zerlegen.

(2) Die nicht-trivialen Bahnen einer solchen Permutation sind genau die nicht-trivialen Bahnen der Zykel in der Zykelzerlegung.

(3) Das Signum einer Permutation ist definiert als $(-1)^q$, wobei q die Anzahl der Fehlstände der Permutation ist.

(4) Ist die Anzahl gerader Zykel in der Zykelzerlegung einer Permutation gerade, so hat die Permutation Signum 1, andernfalls Signum -1.

[13.12.23]

4.2 Determinantenformen

Bemerkung 4.2.1 (Determinante vs. Fläche in $\mathbb{R}^2$)**.** Wir erinnern daran, dass die Determinante bzw. Fläche einer Matrix $A \in \mathbb{R}^{2\times 2}$ definiert sind durch

$$\text{Fläche}(A) := |ad - bc| \quad \text{und} \quad \det(A) := ad - bc, \quad \text{wobei} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In Korollar 2.1.52 haben wir für eine beliebige Matrix $A \in \mathbb{R}^{2\times 2}$ gezeigt, dass

$$A \text{ invertierbar} \iff \text{Fläche}(A) \neq 0 \iff \det(A) \neq 0.$$

Die Fläche von A hat eine eindeutige geometrische Interpretation: Sind v und w die Spalten von A, so ist Fläche(A) der Flächeninhalt des von v und w aufgespannten Parallelogramms. Die Determinante ist demzufolge ein vorzeichenbehafteter Flächeninhalt. Was ist die Bedeutung des Vorzeichens von $\det(A)$?

Es sei α der Winkel, der eingeschlossen wird, wenn man gegen den Uhrzeigersinn vom Strahl durch v zum Strahl durch w läuft. Ist dieser Winkel kleiner als 180^o, so nennen wir v und w *positiv orientiert*, andernfalls *negativ orientiert*. Man kann zeigen, dass gilt

$$\det(A) > 0 \iff (v, w) \text{ positiv orientiert.}$$

Die Determinante kombiniert also Informationen über den Flächeninhalt des von v und w aufgespannten Parallelogramms und Informationen über die Orientierung von (v, w). Man bezeichnet $\det(A)$ daher auch als *orientierten Flächeninhalt* von v und w.

Bemerkung 4.2.2. Für die Frage der Invertierbarkeit reeller Matrizen, spielt es keine Rolle, ob man mit der Determinante oder de Fläche arbeitet. Trotzdem bevorzugen die Mathematiker die Determinante. Dafür gibt es mehrere Gründe:

- Die Determinante lässt sich auf Matrizen über allgemeinen Körpern verallgemeinern, weil die Definition keinen Absolutbetrag erfordert.
- Die Determinanten hat bessere „formale Eigenschaften“ als der Flächeninhalt.

Letzteres wollen wir nun genauer erklären. Aus technischen Gründen ist es besser, anstelle der Determinante die eng verwandte Abbildung

$$\text{Det} : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}, \quad \left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \right) \mapsto ad - bc,$$

zu betrachten, die wir die *Determinantenform* von $\mathbb{R}^2$ nennen. Diese Abbildung trägt genau dieselbe Information wie die Determinante, denn für eine Matrix A mit Spalten v und w gilt nach Definition gerade

$$\det(A) = \text{Det}(v, w).$$

Bemerkung 4.2.3 (Bilinearität)**.** Halten wir einen Vektor $v = \begin{pmatrix} a \\ c \end{pmatrix}$ fest, so ist die Abbildung

$$\mathbb{R}^2 \to \mathbb{R}, \quad w = \begin{pmatrix} b \\ d \end{pmatrix} \mapsto \mathrm{Det}(v,w) = ad - bc$$

linear, und halten wir die zweite Spalte $w = \begin{pmatrix} b \\ d \end{pmatrix}$ fest, so ist die Abbildung

$$\mathbb{R}^2 \to \mathbb{R}, \quad v = \begin{pmatrix} a \\ c \end{pmatrix} \mapsto \mathrm{Det}(v,w) = ad - bc$$

ebenfalls linear. Wir sagen, die Determinantenform ist *bilinear*.

Bemerkung 4.2.4 (Weitere Eigenschaften der Determinante)**.** Neben der Bilinearität hat die Determinantenform noch eine Reihe weiterer offensichtlicher Eigenschaften. Es gilt

$$\mathrm{Det}(e_1,e_2) = 1, \quad \mathrm{Det}(v,v) = 0 \quad \text{und} \quad \mathrm{Det}(v,w) = -\mathrm{Det}(w,v) \quad \text{für alle } v,w \in \mathbb{K}^2 \tag{4.2.1}$$

Es stellt sich heraus, dass diese Eigenschaften die Determinantenform schon eindeutig festlegen:

Proposition 4.2.5 (Eindeutigkeit der Determinantenform)**.** *Die Determinantenform ist die eindeutige bilineare Abbildung* $\mathrm{Det} : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$*, die* (4.2.1) *erfüllt.*

Man könnte Proposition 4.2.5 direkt durch eine Rechnung nachweisen (Übung!). Wir werden später einen konzeptuellen Beweis nachliefern. Was wir uns an dieser Stelle merken sollten ist die Tatsache, dass die Determinantenform sich sehr leicht axiomatisch charakterisieren lässt. (Für den Flächeninhalt ist das nicht so einfach!) Diese axiomatische Charakterisierung ist der Schlüssel zur Verallgemeinerung der Determinante auf höhere Dimensionen.

Definition 4.2.6. Sei V ein $\mathbb{K}$-Vektorraum[2] und $D : V^k \to \mathbb{K}$ eine Abbildung.

(i) D heißt *k-linear*, falls für $1 \le i \le k$ und $v_1,\dots,v_{i-1},v_{i+1},\dots,v_k \in V$ die Abbildung

$$V \to \mathbb{K}, \quad w \mapsto D(v_1,\dots,v_{i-1},w,v_{i+1},\dots,v_k)$$

linear ist.

(ii) D heißt *alternierend*, falls für $1 \le i < j \le k$ und $v_1,\dots,v_k \in V$ gilt

$$v_i = v_j \quad \Longrightarrow \quad D(v_1,\dots,v_i,\dots,v_j,\dots,v_k) = 0.$$

(iii) D heißt *schief-symmetrisch*, falls für $1 \le i < j \le k$ und $v_1,\dots,v_k \in V$ gilt

$$D(v_1,\dots,v_i,\dots,v_j,\dots,v_k) = -D(v_1,\dots,v_j,\dots,v_i,\dots,v_k).$$

(iv) Ist $\dim_{\mathbb{K}} V = k$, so heißt eine alternierende, schief-symmetrische k-lineare Abbildung $D : V^k \to \mathbb{K}$ eine *orientierte Volumenform* auf V, falls $D \neq 0$.

Wir können Proposition 4.2.5 dann auch so formulieren:

[2] Hier und im folgenden sei wieder $\mathbb{K}$ ein Körper oder, wenn Sie wollen, $\mathbb{K} = \mathbb{R}$.

Proposition 4.2.7. *Auf $\mathbb{R}^2$ gibt es genau eine orientierte Volumenform D mit $D(e_1,e_2)=1$.*

Allgemeiner werden wir in Satz 4.2.22 beweisen, dass es auf jedem endlichdimensionalen Vektorraum bis auf Normierung genau eine orientierte Volumenform gibt; dies wird uns dann erlauben, die Determinante zu definieren. Zum Beweis dieser Tatsache holen wir nun ein wenig aus.

Notation 4.2.8 (Kontravariante Tensoren)**.** Wir schreiben im Folgenden

$$(V^*)^{\otimes k} := \{D : V^k \to \mathbb{K} \mid D \text{ } k\text{-linear}\}$$

und nennen Elemente von $(V^*)^{\otimes k}$ heißen *(kontravariante) k-Tensoren*. Beachten Sie, dass $(V^*)^{\otimes 1} = V^*$ gerade der Dualraum von V ist, kontravariante 1-Tensoren sind also gerade Linearformen. Weiter setzen wir

$$\bigwedge^k V^* := \{D \in (V^*)^{\otimes k} \mid D \text{ alternierend}\}$$

Elemente von $\bigwedge^k V^*$ heißen *k-Formen*.

Übung 4.2.9. Zeigen Sie, dass $\bigwedge^k V^* \subseteq (V^*)^{\otimes k} \subseteq \mathrm{Abb}(V^k,\mathbb{K})$ Untervektorräume sind.

Beispiel 4.2.10 (Elementare Tensoren)**.** Es ist leicht, Beispiele für k-Tensoren anzugeben.

(i) Ein 1-Tensor ist einfach ein Element des Dualraums V^*, also eine Linearform.

(ii) Sind $\lambda_1,\dots,\lambda_k \in V^*$ Linearformen, so definiert

$$\lambda_1 \otimes \cdots \otimes \lambda_k : V^k \to \mathbb{K}, \quad (v_1,\dots,v_k) \mapsto \lambda_1(v_1)\lambda_2(v_2)\cdots\lambda_k(v_k)$$

einen k-Tensor. Solche Tensoren heißen *elementare Tensoren*.

(iii) Allgemeiner sind wegen Übung 4.2.9 Linearkombinationen solcher elementarer Tensoren wieder Tensoren.

Proposition 4.2.11. *Ist $\dim V = n$ und $(v_1,\dots,v_n)$ eine geordnete Basis von V mit dualer Basis $(v_1^*,\dots,v_n^*)$, so sind die Tensoren $v_{i_1}^* \otimes \cdots \otimes v_{i_k}^*$ mit $i_1,\dots,i_k \in \{1,\dots,n\}$ linear unabhängig.*

Beweis. Für beliebige Indizes $i_1,\dots,i_k,j_1,\dots,j_k \in \{1,\dots,n\}$ gilt

$$v_{i_1}^* \otimes \cdots \otimes v_{i_k}^*(v_{j_1},\dots,v_{j_k}) = \begin{cases} 1, & \text{falls } i_1 = j_1,\dots,i_k = j_k \\ 0, & \text{sonst.} \end{cases}$$

Sind nun $a_{i_1,\dots,i_k} \in \mathbb{K}$ mit

$$\sum_{i_1=1}^{n} \cdots \sum_{i_k=1}^{n} a_{i_1,\dots,i_k} v_{i_1}^* \otimes \cdots \otimes v_{i_k}^* = \mathbf{0}, \tag{4.2.2}$$

so liefert Einsetzen von $(v_{j_1},\dots,v_{j_k})$ also, dass $a_{j_1,\dots,j_k} = 0$. □

Übung 4.2.12. Zeigen Sie, dass in der Situation von Proposition 4.2.11 die Menge

$$\{v_{i_1}^* \otimes \cdots \otimes v_{i_k}^* \mid i_1,\dots,i_k \in \{1,\dots,n\}\}$$

ein Erzeugendensystem von $(V^*)^{\otimes k}$ ist, und schließen Sie, dass

$$\dim(V^*)^{\otimes k} = n^k.$$

Wie können wir aber nun alternierende oder schief-symmetrische Tensoren finden? Zunächst überlegen wir uns wie die beiden Begriffe zusammenhängen.

Bemerkung 4.2.13 (Alternierend vs. schief-symmetrisch)**.** Jede alternierende k-lineare Abbildung D ist schief-symmetrisch, denn für $1 \le i < j \le k$ und $v_1, \dots, v_k \in V$ gilt

$$\begin{aligned} 0 &= D(v_1, \dots, v_i + v_j, \dots, v_i + v_j, \dots, v_k) \\ &= D(v_1, \dots, v_i, \dots, v_i + v_j, \dots, v_k) + D(v_1, \dots, v_j, \dots, v_i + v_j, \dots, v_k) \\ &= D(v_1, \dots, v_i, \dots, v_i, \dots, v_k) + D(v_1, \dots, v_i, \dots, v_j, \dots, v_k) \\ &\quad + D(v_1, \dots, v_j, \dots, v_i, \dots, v_k) + D(v_1, \dots, v_j, \dots, v_j, \dots, v_k) \\ &= D(v_1, \dots, v_i, \dots, v_j, \dots, v_k) + D(v_1, \dots, v_j, \dots, v_i, \dots, v_k). \end{aligned}$$

Ist umgekehrt D eine schief-symmetrische k-lineare Abbildung und sind $v_1, \dots, v_k \in V$ mit $v_i = v_j$ für $1 \le i < j \le k$, so gilt

$$2 \cdot D(v_1, \dots, v_i, \dots, v_j, \dots, v_k) = D(v_1, \dots, v_i, \dots, v_j, \dots, v_k) + D(v_1, \dots, v_j, \dots, v_i, \dots, v_k) = 0.$$

Wir würden jetzt gerne daraus folgern, dass $D(v_1, \dots, v_i, \dots, v_j, \dots, v_k) = 0$ gilt. Für $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{Q}$ ist das problemlos möglich. Wir werden allerdings später Körper kennenlernen, in denen $2 := 1 + 1 = 0$ gilt, z.B. den Körper mit 2 Elementen. Über solchen Körpern können wir so nicht argumentieren.

Wir halten fest:

Proposition 4.2.14. *Gilt in $\mathbb{K}$ die Ungleichung $1 + 1 \neq 0$, so ist ein k-Tensor $D \in (V^*)^{\otimes k}$ genau dann alternierend (also eine k-Form), wenn er schiefsymmetrisch ist.*

Im Allgemeinen ist alternierend eine stärkere Bedingung als schiefsymmetrisch, weswegen wir meist diese stärkere Bedingung annehmen.

Bemerkung 4.2.15 (k-Formen und Permutationen)**.** Ist $\sigma \in \mathrm{Sym}_k$ eine Permutation, so können wir σ als Produkt von Transpositionen schreiben. Da jede Transposition ein Vorzeichen liefert, gilt dann für $D \in \bigwedge^k V^*$, dass

$$D(v_{\sigma(1)}, \dots, v_{\sigma(k)}) = \mathrm{sgn}(\sigma) \cdot D(v_1, \dots, v_k). \tag{4.2.3}$$

Umgekehrt ist jeder k-Tensor mit dieser Eigenschaft schiefsymmetrisch. Falls in $\mathbb{K}$ die Bedingung $1 + 1 \neq 0$ erfüllt ist, so gilt also

$$\bigwedge^k V^* = \{D \in (V^*)^{\otimes k} \mid \forall\, \sigma \in \mathrm{Sym}_k : D(v_{\sigma(1)}, \dots, v_{\sigma(k)}) = \mathrm{sgn}(\sigma) \cdot D(v_1, \dots, v_k)\}.$$

Wir geben nun eine Konstruktion an, die es uns erlaubt, einen beliebigen Tensor alternierend zu machen:

Proposition 4.2.16. *Sei $D \in (V^*)^{\otimes k}$. Dann ist* $\mathrm{Alt}(D)$ *gegeben durch*

$$\mathrm{Alt}(D)(v_1, \dots, v_k) := \sum_{\sigma \in \mathrm{Sym}_k} \mathrm{sgn}(\sigma) \cdot D(v_{\sigma(1)}, \dots, v_{\sigma(k)}) \quad (v_1, \dots, v_k \in V)$$

alternierend (und daher schiefsymmetrisch).

Beweis. Wir dürfen annehmen, dass $k \geq 2$. Es seien $v_1, \ldots, v_k \in V$ und $1 \leq i < j \leq k$ mit $v_i = v_j$. Wir müssen zeigen, dass dann $\mathrm{Alt}(D)(v_1, \ldots, v_k) = 0$ gilt.

Es sei $\mathrm{Sym}_k^+ := \{\sigma \in \mathrm{Sym}_k \mid \mathrm{sgn}(\sigma) = +1\}$ und $\mathrm{Sym}_k^- := \{\sigma \in \mathrm{Sym}_k \mid \mathrm{sgn}(\sigma) = -1\}$. Ist $\sigma \in \mathrm{Sym}_k$ eine Permutation, so ist auch $\sigma' := (i,j) \circ \sigma$ eine Permutation, und es gilt $\mathrm{sgn}(\sigma') = -\mathrm{sgn}(\sigma)$. Wegen $(i,j) \circ (i,j) = \mathrm{Id}$ definiert die Formel $\sigma \mapsto \sigma'$ also zueinander inverse bijektive Abbildungen

$$\mathrm{Sym}_k^+ \to \mathrm{Sym}_k^- \quad \text{und} \quad \mathrm{Sym}_k^- \to \mathrm{Sym}_k^+.$$

Es gilt daher

$$\mathrm{Sym}_k = \mathrm{Sym}_k^+ \sqcup \mathrm{Sym}_k^- = \bigsqcup_{\sigma \in \mathrm{Sym}_k^+} \{\sigma, \sigma'\},$$

und daher

$$\mathrm{Alt}(D)(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_k) = \sum_{\sigma \in \mathrm{Sym}_k^+} \mathrm{sgn}(\sigma) D(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) + \mathrm{sgn}(\sigma') D(v_{\sigma'(1)}, \ldots, v_{\sigma'(k)}) \quad (4.2.4)$$

Wegen $v_i = v_j$ gilt aber in jedem der Summanden $(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = (v_{\sigma'(1)}, \ldots, v_{\sigma'(k)})$, und andererseits gilt $\mathrm{sgn}(\sigma') = -\mathrm{sgn}(\sigma)$. Daher ist jeder der $n!/2$ Summanden in (4.2.4) gleich 0. □

Notation 4.2.17. Sind $\lambda_1, \ldots, \lambda_k \in V^*$, so schreiben wir

$$\lambda_1 \wedge \cdots \wedge \lambda_k := \mathrm{Alt}(\lambda_1 \otimes \cdots \otimes \lambda_k) \in \bigwedge^k V^*.$$

Lemma 4.2.18. *Es gilt*

$$(\lambda_1 \wedge \cdots \wedge \lambda_k)(v_1, \ldots, v_k) = \sum_{\sigma \in \mathrm{Sym}_k} \mathrm{sgn}(\sigma) \prod_{i=1}^k \lambda_{\sigma(i)}(v_i) = \sum_{\sigma \in \mathrm{Sym}_k} \mathrm{sgn}(\sigma) \prod_{i=1}^k \lambda_i(v_{\sigma(i)}).$$

Beweis. Die erste Formel ist genau die Definition. Da jede Permutation genau eine inverse Permutation hat, kann man in der Summe σ durch σ^{-1} ersetzen. Unter Verwendung von $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$ folgt

$$\sum_{\sigma \in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^k \lambda_{\sigma(i)}(v_i) \right) = \sum_{\sigma^{-1} \in \mathrm{Sym}_n} \mathrm{sgn}(\sigma^{-1}) \left(\prod_{i=1}^k \lambda_{\sigma^{-1}(i)}(v_i) \right) = \sum_{\sigma \in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \left(\prod_{j=1}^k \lambda_j(v_{\sigma(j)}) \right),$$

wobei wir im letzten Schritt $j := \sigma^{-1}(i)$ gesetzt und die Reihenfolge der Faktoren umsortiert haben. □

Wir haben also scheinbar viele Beispiele für k-Formen hingeschrieben. Es stellt sich allerdings heraus, dass fast alle dieser Beispiele $\mathbf{0}$ sind; dies folgt aus der folgenden Beobachtung:

Lemma 4.2.19. *Sind $v_1, \ldots, v_k$ linear abhängig, so gilt $D(v_1, \ldots, v_k) = 0$ für alle $D \in \bigwedge^k V^*$.*

Beweis. Mindestens einer der Vektoren ist redundant. Da D schief-symmetrisch ist, ist die Schlussfolgerung invariant unter Vertauschungen der v_i. Wir dürfen daher annehmen, dass v_k redundant ist. Schreibe also

$$v_k = \sum_{i=1}^{k-1} \alpha_i v_i \quad (\alpha_i \in \mathbb{K}).$$

Indem wir verwenden, dass D linear im letzten Eintrag ist, erhalten wir

$$D(v_1, \ldots, v_k) = \sum_{i=1}^{k-1} \alpha_i D(v_1, \ldots, v_{k-1}, v_i),$$

und da D alternierend ist, sind alle Summanden 0. □

Korollar 4.2.20. *Ist V endlichdimensional und $k > \dim_{\mathbb{K}} V$, so gilt $\bigwedge^k V^* = \{\mathbf{0}\}$.* □

Gibt es überhaupt Formen vom Grad > 1, die nicht = 0 sind?

Beispiel 4.2.21. Ist $(b_1,\dots,b_n)$ eine geordnete Basis von V mit dualer Basis $(b_1^*,\dots,b_n^*)$, so gilt

$$b_1^* \wedge \cdots \wedge b_n^*(b_1,\dots,b_n) = \sum_{\sigma\in \mathrm{Sym}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n b^*_{\sigma(i)}(b_i).$$

Nun ist aber $b^*_{\sigma(i)}(b_i) = 0$, außer wenn $\sigma(i) = i$. Es gibt also überhaupt nur einen Summanden, der nicht 0 ist, und wir erhalten

$$b_1^* \wedge \cdots \wedge b_n^*(b_1,\dots,b_n) = \prod_{i=1}^n b_i^*(b_i) = 1.$$

Insbesondere gilt $b_1^* \wedge \cdots \wedge b_n^* \neq 0$.

Satz 4.2.22 (Eindeutigkeitssatz)**.** *Sei $D \in \bigwedge^n V^*$ und $(b_1,\dots,b_n)$ eine geordnete Basis von V. Dann gilt $b_1^* \wedge \cdots \wedge b_n^* \neq 0$*

$$D = D(b_1,\dots,b_n)\cdot b_1^* \wedge \cdots \wedge b_n^*. \tag{4.2.5}$$

Insbesondere gilt

$$\bigwedge^n V^* = \mathbb{K} b_1^* \wedge \cdots \wedge b_n^* \quad \text{und} \quad \dim_{\mathbb{K}} \bigwedge^n V^* = 1,$$

d.h. es gibt bis auf Multiplikation mit $\lambda \in \mathbb{K}\setminus\{0\}$ genau eine orientierte Volumenform auf V.

Beweis. Die erste Aussage haben wir bereits in Beispiel 4.2.21 gesehen. Nach Definition der dualen Basis gilt

$$D(v_1,\dots,v_n) = D\left(\sum_{i=1}^n b_i^*(v_1)b_i,\dots,\sum_{i=1}^n b_i^*(v_n)b_i\right).$$

Da D multilinear ist, können wir „ausmultiplizieren“: Wir wählen zu jedem $j \in \{1,\dots,n\}$ einen Summanden $\varphi(j)$ und erhalten

$$\begin{aligned} D(v_1,\dots,v_n) &= \sum_{\varphi:\{1,\dots,n\}\to\{1,\dots,n\}} D(b^*_{\varphi(1)}(v_1)b_{\varphi(1)},\dots,b^*_{\varphi(n)}(v_n)b_{\varphi(n)}) \\ &= \sum_{\varphi:\{1,\dots,n\}\to\{1,\dots,n\}} b^*_{\varphi(1)}(v_1)\cdots b^*_{\varphi(n)}(v_n)\cdot D(b_{\varphi(1)},\dots,b_{\varphi(n)}) \end{aligned}$$

Falls die Abbildung φ nicht bijektiv, und daher nicht injektiv ist, so ist $D(b_{\varphi(1)},\dots,b_{\varphi(n)}) = 0$. Wir erhalten also wegen (**??**),

$$\begin{aligned} D(v_1,\dots,v_n) &= \sum_{\sigma\in\mathrm{Sym}_n} b^*_{\sigma(1)}(v_1)\cdots b^*_{\sigma(n)}(v_n)\cdot D(b_{\sigma(1)},\dots,b_{\sigma(n)}) \\ &= \sum_{\sigma\in\mathrm{Sym}_n} b^*_{\sigma(1)}(v_1)\cdots b^*_{\sigma(n)}(v_n)\cdot \operatorname{sgn}(\sigma) D(b_1,\dots,b_n) \\ &= D(b_1,\dots,b_n)\cdot \sum_{\sigma\in\mathrm{Sym}_n} \operatorname{sgn}(\sigma)\left(\prod_{i=1}^n b^*_{\sigma(i)}(v_i)\right). \end{aligned}$$

Die rechte Seite ist aber gerade $D(b_1,\dots,b_n)\cdot(b_1^*\wedge\cdots\wedge b_n^*)(v_1,\dots,v_n)$. □

Indem wir auf $V = \mathbb{R}^2$ spezialisieren erhalten wir nun wie versprochen eine konzeptuellen Beweis von Proposition 4.2.7 (und daher Proposition 4.2.5).

Bemerkung 4.2.23 (Welche orientierte Volumenform?)**.** In einem allgemeinen Vektorraum gibt es keine bevorzugte Wahl einer orientierten Volumenform. Jede Wahl einer geordneten Basis $(b_1,\dots,b_n)$ liefert eine orientierte Volumenform $b_1^* \wedge \cdots \wedge b_n^*$, und verschieden Wahlen liefern im Allgemeinen verschiedene Volumenformen. Da sich diese nur um eine Konstante unterscheiden, spielt die genaue Wahl im folgenden meist keine Rolle, und man kann einfach irgendeine Wahl treffen. Im $\mathbb{K}^n$ gibt es hingegen eine bevorzugte geordnete Basis, die Standardbasis $(e_1,\dots,e_n)$. Wir definieren daher die *Determinantenform* als die orientierte Volumenform des $\mathbb{K}^n$, die durch

$$\mathrm{Det} := e_1^* \wedge \cdots \wedge e_n^*$$

gegeben ist. Dies ist die eindeutig bestimmte orientierte Volumenform mit der Eigenschaft, dass

$$\mathrm{Det}(e_1,\dots,e_n) = 1,$$

d.h. wir haben das orientierte Volumen des Einheitsquaders auf 1 normiert.

Beispiel 4.2.24 (Leibniz-Formel)**.** Seien $v^{(1)},\dots,v^{(n)}$ beliebige Vektoren in $\mathbb{K}^n$; wir schreiben

$$v^{(i)} = \begin{pmatrix} v_1^{(i)} \\ \vdots \\ v_n^{(i)} \end{pmatrix} \in \mathbb{K}^n.$$

Nah Definition von Det gilt dann die sogenannte *Leibniz-Formel*

$$\mathrm{Det}(v^{(1)},\dots,v^{(n)}) = \sum_{\sigma\in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^n v_{\sigma(i)}^{(i)} \right) = \sum_{\sigma\in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^n v_i^{(\sigma(i))} \right),$$

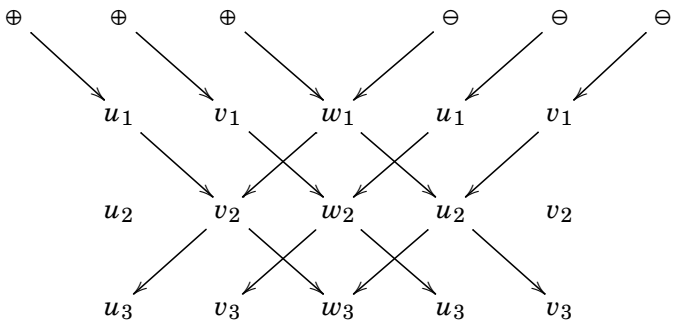
Für $n = 2$ erhalten wir die bekannte Formel

$$\mathrm{Det}\left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \right) = ad - bc.$$

Für $n = 3$ erhalten wir die *Regel von Sarrus* [3]

$$\mathrm{Det}(u,v,w) = u_1v_2w_3 + u_2v_3w_1 + u_3v_1w_2 - u_3v_2w_1 - u_1v_3w_2 - u_2v_1w_3,$$

die man sich wie folgt merken kann („Jägerzaun-Regel“):



Für $n = 4$ hat die Leibniz-Formel bereits 24 Terme, für $n = 5$ bereits 120.
WARNUNG! In Dimensionen ≥ 4 gilt keine Jägerzaunregel!

[3] Pierre Frédéric Sarrus, frz. Mathematiker, 1798-1861

Aus dem Eindeutigkeitssatz folgt unmittelbar:

Korollar 4.2.25 (Basen und orientierte Volumenformen)**.** *Sei D eine orientierte Volumenform auf V und $b_1,\dots,b_n \in V$. Dann gilt:*

$$D(b_1,\dots,b_n) \neq 0 \quad \Longleftrightarrow \quad \{b_1,\dots,b_n\} \text{ ist eine Basis von } V.$$

Beweis. „$\Longrightarrow$“: Wäre $\{b_1,\dots,b_n\}$ keine Basis, so wären $b_1,\dots,b_n$ aus Dimensionsgründen linear abhängig. Dann wäre aber $D(b_1,\dots,b_n) = 0$ nach Lemma 4.2.19.

„$\Longleftarrow$“: Da D und $b_1^* \wedge \cdots \wedge b_n^*$ orientierte Volumenformen sind, sind sie Vielfache voneinander. Wegen $(b_1^* \wedge \cdots \wedge b_n^*)(b_1,\dots,b_n) = 1$ folgt $D(b_1,\dots,b_n) \neq 0$. □

Korollar 4.2.26. *Vektoren $u,v,w \in \mathbb{K}^3$ sind genau dann linear unabhängig, wenn*

$$u_1v_2w_3 + u_2v_3w_1 + u_3v_1w_2 - u_3v_2w_1 - u_1v_3w_2 - u_2v_1w_3 \neq 0.$$

Beispiel 4.2.27.

$$\mathrm{Det}\left(\begin{pmatrix}1\\2\\3\end{pmatrix},\begin{pmatrix}2\\3\\4\end{pmatrix},\begin{pmatrix}3\\4\\5\end{pmatrix}\right) = 15+24+24-27-16-20 = 0 \Longrightarrow \begin{pmatrix}1\\2\\3\end{pmatrix},\begin{pmatrix}2\\3\\4\end{pmatrix},\begin{pmatrix}3\\4\\5\end{pmatrix} \text{ linear abhängig.}$$

[15.12.23]

Bemerkung 4.2.28 (Determinantenform via Spaltenumformungen)**.** Wie kann man die Determinantenform in höheren Dimensionen berechnen? Die Leibniz-Formel ist in diesem Fall zu aufwendig, um diese direkt auszuwerten. Stattdessen kann man mit Spaltenumformungen arbeiten. Dazu beobachtet man, dass die Determinantenform $\mathrm{Det}:(\mathbb{K}^n)^n \to \mathbb{K}$ die folgenden Eigenschaften hat:

(D1) $\mathrm{Det}(v_1,\dots,v_n)=0$, wenn $v_1,\dots,v_n$ linear abhängig sind.

(D2) $\mathrm{Det}(e_1,\dots,e_n)=1$.

(D3) $\mathrm{Det}(v_1,\dots,\lambda v_i,\dots v_n)=\lambda\cdot\mathrm{Det}(v_1,\dots,v_n)$ für $\lambda\in\mathbb{K}$ und $1\le i\le n$.

(D4) $\mathrm{Det}(v_1,\dots,v_i,\dots,v_j,\dots,v_n)=\mathrm{Det}(v_1,\dots,v_i+\lambda v_j,\dots,v_j,\dots v_n)$ für $\lambda\in\mathbb{K}$ und $1\le i<j\le n$.

(D5) Det ist schief-symmetrisch.

Zum Beweis von (D4) verwendet man, dass wegen Linearität in der $i$ten Variable und Alternierheit schon

$$\mathrm{Det}(v_1,\dots,v_i+\lambda v_j,\dots,v_j,\dots v_n)=\mathrm{Det}(v_1,\dots,v_n)+\lambda\mathrm{Det}(v_1,\dots,v_j,\dots,v_j,\dots,v_n)=\mathrm{Det}(v_1,\dots,v_n)$$

gilt. (D1) folgt sofort aus Lemma 4.2.19, (D2) folgt aus Beispiel 4.2.21, (D3) folgt aus der n-Linearität und (D5) aus der Antisymmetrie der Determinantenform.

Mittels der Regeln (D1)–(D5) kann man die Determinanten in konkreten Fällen berechnen.

Beispiel 4.2.29. Es gilt

$$\begin{aligned}
\mathrm{Det}\left(\begin{pmatrix}1\\0\\1\end{pmatrix},\begin{pmatrix}2\\6\\4\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix}\right) &\overset{(D5)}{=} -\mathrm{Det}\left(\begin{pmatrix}1\\0\\1\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix},\begin{pmatrix}2\\6\\4\end{pmatrix}\right) \overset{(D4)}{=} -\mathrm{Det}\left(\begin{pmatrix}1\\0\\1\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix},\begin{pmatrix}2\\0\\4\end{pmatrix}\right)\\
&\overset{(D4)}{=} -\mathrm{Det}\left(\begin{pmatrix}1\\0\\1\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix},\begin{pmatrix}0\\0\\2\end{pmatrix}\right) \overset{(D4)}{=} -\mathrm{Det}\left(\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix},\begin{pmatrix}0\\0\\2\end{pmatrix}\right)\\
&\overset{(D3)}{=} -6\cdot\mathrm{Det}(e_1,e_2,e_3) = -6.
\end{aligned}$$

Bemerkung 4.2.30. Sind $v_1,\dots,v_n$ linear unabhängig, so ist die Matrix A mit Spalten $v_1,\dots,v_n$ invertierbar und lässt sich daher nach Korollar 3.4.6 durch elementare Spaltenumformungen auf die Einheitsmatrix bringen. Das besagt, dass das Berechnungsverfahren aus Beispiel 4.2.29 für linear unabhängige Vektoren $v_1,\dots,v_n$ immer funktioniert[4]. Damit haben wir insbesondere das folgende Korollar bewiesen.

Korollar 4.2.31. *Die Determinantenform* $\mathrm{Det}:(\mathbb{K}^n)^n\to\mathbb{K}$ *ist die eindeutige Abbildung mit den Eigenschaften (D1)–(D5).* □

Als Anwendung interpretieren wir die Determinantenform des $\mathbb{R}^3$ geometrisch:

[4] Das Verfahren ist immer noch sehr langsam; wir werden es im nächsten Abschnitt noch verbessern.

Bemerkung 4.2.32 (Determinantenform und Volumen)**.** Wir haben gesehen, dass die Determinantenform in $\mathbb{R}^2$ als orientierte Fläche eines Parallelogramms gedeutet werden kann. Eine analoge Interpretation gilt auch im $\mathbb{R}^3$. Die drei-dimensionale Verallgemeinerung eines Parallelogramms ist ein sogenanntes Parallelepiped („schiefer Quader"): Drei Vektoren $u,v,w \in \mathbb{R}^3$ definieren das Parallelepiped

$$P(u,v,w) = \{\alpha u + \beta v + \gamma w \mid \alpha,\beta,\gamma \in [0,1]\},$$

und das Volumen dieses Parallelepipeds ist gegeben durch Grundfläche mal Höhe (oder Seitenfläche mal Breite, oder Vorderfläche mal Tiefe). Für Quader ist das klar, und der allgemeine Fall folgt dann aus dem Cavalierischen Prinzip[5]. Für das Volumen eines Parallelepipeds gilt:

(V1) $\mathrm{Vol}(P(v_1,v_2,v_3)) = 0$, wenn v_1,v_2,v_3 in einer Ebene liegen (also linear abhängig sind).

(V2) $\mathrm{Vol}(P(e_1,e_2,e_3)) = 1$, da das Volumen des Einheitswürfels 1 ist.

(V3) $\mathrm{Vol}(P((v_1,\dots,\lambda v_i,\dots v_3)) = |\lambda| \cdot \mathrm{Vol}(P(v_1,\dots,v_3))$ für $\lambda \in \mathbb{R}$ und $1 \le i \le 3$, denn eine Spiegelung ändert das Volumen nicht, und eine Streckung/Stauchung multipliziert das Volumen mit dem entsprechenden Faktor.

(V4) $\mathrm{Vol}(P(v_1,\dots,v_i,\dots,v_j,\dots,v_3)) = \mathrm{Vol}(P(v_1,\dots,v_i+\lambda v_j,\dots,v_j,\dots v_3))$ für $\lambda \in \mathbb{R}$ und $1 \le i < j \le 3$, denn eine Scherung erhält Grundfläche und Höhe.

(V5) $\mathrm{Vol}(P(v_1,v_2,v_3)$ ist symmetrisch, ändert sich also nicht unter Vertauschungen der v_i.

Das entspricht schon fast den Bedingungen (D1)–(D5). Wir definieren nun die *Orientierung* als die Abbildung

$$o : \mathbb{R}^3 \to \{-1,0,1\}, \quad o(v_1,v_2,v_3) := \begin{cases} \frac{\mathrm{Det}(v_1,v_2,v_3)}{|\mathrm{Det}(v_1,v_2,v_3)|}, & \text{falls } \mathrm{Det}(v_1,v_2,v_3) \neq 0, \\ 0, & \text{sonst.} \end{cases}$$

Nach Definition haben Daumen, Zeigefinger und Mittelfinger der rechten bzw. linken Hand die Orientierung $+1$ bzw. -1. Diese Abbildung hat die folgenden Eigenschaften: Es gilt $o(e_1,e_2,e_3) = 1$ und $o(v_1,v_2,v_3) = 0$, wenn v_1,v_2,v_3 linear abhängig sind. Wie wir noch sehen werden (vgl. Übung 4.3.18) ist o außerdem invariant unter Streckungen/Stauchungen und Scherungen und kehrt ihr Vorzeichen unter Spiegelungen um. Aus diesen Eigenschaften und (V1)–(V5) folgt nun, dass die Abbildung $(v_1,v_2,v_3) \mapsto o(v_1,v_2,v_3) \cdot \mathrm{Vol}(P(v_1,v_2,v_3))$ die Eigenschaften (D1)–(D5) hat. Das beweist aber gerade, dass

$$\mathrm{Det}(v_1,v_2,v_3) = o(v_1,v_2,v_3) \cdot \mathrm{Vol}(P(v_1,v_2,v_3)), \quad \text{insbesondere} \quad \mathrm{Vol}(P(u,v,w)) = |\mathrm{Det}(u,v,w)|.$$

Wir können die Determinantenform im $\mathbb{R}^3$ also als orientiertes Volumen auffassen. Andere orientierte Volumenformungen liefern auch einen orientierte Volumenbegriff, der sich nur in der Normalisierung (also dem Volumen, das man dem Einheitswürfel zuweist) unterscheiden.

[5] Dieses Prinzip der Euklidischen Geometrie besagt, dass zwei Körper derselben Höhe dasselbe Volumen haben, wenn alle ihre Schnittflächen mit horizontalen Ebenen denselben Flächeninhalt haben. Es geht auf Bonaventura Francesco Cavalieri (ital. Mathematiker, 1598-1647) zurück.

Zusammenfassung von Abschnitt 4.2

(1) Tensoren sind Abbildungen $V^k \to \mathbb{K}$, die in jeder Komponente linear („multilinear“) sind.

(2) Formen sind alternierende Tensoren, die also verschwinden, wenn man zweimal dasselbe Element einsetzt. Falls $2 \neq 0$, so ist dies gleichbedeutend damit, dass sie schief-symmetrisch sind, also unter Transpositionen das Vorzeichen wechseln.

(3) Auf einem n-dimensionalen Vektorraum gibt es bis auf Vielfache genau eine von 0 verschiedene n-Form. Eine solche heißt orientierte Volumenform.

(4) Orientierte Volumenformen detektieren lineare Unabhängigkeit.

(5) Die orientierte Volumenform des $\mathbb{K}^n$, die auf der Standardbasis den Wert 1 annimmt, heißt Determinantenform. Es gibt eine geschlossene Formel (Leibniz-Formel), die jedoch zum praktischen Rechnen in Dimensionen > 3 unbrauchbar ist.

4.3 Die Determinante eines Endomorphismus

Eine wichtige Konstruktion in der multilinearen Algebra ist die folgende:

Übung 4.3.1 (Rückzug)**.** Seien V und W Vektorräume über einem Körper $\mathbb{K}$, $\Phi \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ und $k \in \mathbb{N}$.

(i) Ist $D \in \bigwedge^k W^*$, so ist die Abbildung

$$\Phi^* D : V^k \to \mathbb{K}, \quad (v_1,\dots,v_k) \mapsto D(\Phi(v_1),\dots,\Phi(v_k))$$

eine k-Form auf V.

(ii) Die Abbildung

$$\Phi^* : \bigwedge^k W^* \to \bigwedge^k V^*, \quad D \mapsto \Phi^* D$$

ist linear.

$\Phi^* D$ heißt der *Rückzug* von D entlang Φ. (Für $k = 1$ ist Φ^* einfach die duale Abbildung.)

Beachte, dass die Abbildung Φ^* in die „andere Richtung“ geht als die Abbildung Φ. Wie bei der dualen Abbildung gilt

$$(\Psi \circ \Phi)^* = \Phi^* \circ \Psi^*$$

für lineare Abbildungen zwischen geeigneten Vektorräumen.

Im Folgenden sei wieder V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$ und es sei $n := \dim_{\mathbb{K}}(V)$. Wir untersuchen, was mit einer orientierten Volumenform passiert, wenn man sie mit einem Endomorphismus von V zurückzieht.

Proposition 4.3.2. *Für jedes* $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *existiert ein eindeutig besimmtes Element* $\det(\Phi) \in \mathbb{K}$, *so dass*

$$\Phi^* D = \det(\Phi) \cdot D \text{ für alle } D \in \bigwedge^n V^*. \tag{4.3.1}$$

Beweis. Wir fixieren zunächst eine orientierte Volumenform D_0 auf V. Dann gilt

$$\Phi^* D_0 \in \bigwedge^n V^* = \mathbb{K} \cdot D_0,$$

also existiert ein $\lambda \in \mathbb{K}$ mit

$$\Phi^* D_0 = \lambda \cdot D_0.$$

Ist nun $D \in \bigwedge^n V^*$ beliebig, so existiert ein $\mu \in \mathbb{K}$ mit $D = \mu D_0$, und daher ist

$$\Phi^* D' = \Phi^*(\mu D) = \mu \Phi^* D = \mu\lambda D = \lambda\mu D = \lambda D'.$$

Wir können also $\det(\Phi) := \lambda$ wählen. □

Definition 4.3.3. $\det(\Phi)$ heißt die *Determinante* von Φ.

Was ist nun die geometrische Bedeutung dieser Determinante?

Bemerkung 4.3.4 (Determinante und Volumenverzerrung in $\mathbb{R}^3$)**.** Seien $v_1, v_2, v_3 \in \mathbb{R}^3$ linear unabhängig und sei

$$P = P(v_1, v_2, v_3) = \left\{ \sum_{i=1}^{3} \lambda_i v_i \mid \lambda_1, \lambda_2, \lambda_3 \in [0,1] \right\}$$

das zugehörige Parallelepiped. Gemäß Bemerkung 4.2.32 ist das Volumen von P dann

$$\mathrm{Vol}(P) = |\mathrm{Det}(v_1, v_2, v_3)|.$$

Sei nun $\Phi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^3)$. Was ist das Volumen von $\Phi(P)$? Da Φ linear ist, bildet es Parallelepipede auf Parallelepipede ab. Wir erhalten also

$$\begin{aligned} \mathrm{Vol}(\Phi(P)) &= \mathrm{Vol}(P(\Phi(v_1), \Phi(v_2), \Phi(v_3)) = |\mathrm{Det}(\Phi(v_1), \Phi(v_2), \Phi(v_3))| \\ &= |\Phi^* \mathrm{Det}(v_1, v_2, v_3)| = |\det(\Phi) \cdot \mathrm{Det}(v_1, v_2, v_3)|, \end{aligned}$$

und daher

$$|\det(\Phi)| = \frac{\mathrm{Vol}(\Phi(P))}{\mathrm{Vol}(P)},$$

d.h. der Betrag der Determinante ist gerade die *Volumenverzerrung* von P unter Φ. Es ist eine zentrale Eigenschaft von Endomorphismen, dass diese Volumenverzerrung *universell* ist, also nicht von P abhängt. Analog zeigt das Vorzeichen von $\det(\Phi)$, ob Φ die Orientierung erhält ($\det(\Phi) > 0$) oder umkehrt ($\det(\Phi) < 0$).

Unmittelbar aus der Definition erhalten wir nun die folgenden zentralen Eigenschaften der Determinante:

Satz 4.3.5 (Hauptsatz über Determinanten)**.** *Seien* $\Phi, \Psi \in \mathrm{End}_{\mathbb{K}}(V)$.

(i) $\det(\mathrm{Id}) = 1$ *und* $\det(\Phi \circ \Psi) = \det(\Phi)\det(\Psi)$.

(ii) Φ *ist invertierbar genau dann, wenn* $\det(\Phi) \neq 0$*, und in diesem Fall ist* $\det(\Phi^{-1}) = \det(\Phi)^{-1}$.

Beweis. (i) Die Aussage über die Identität folgt sofort aus $\mathrm{Id}^* = \mathrm{Id}$. Sei nun D eine orientierte Volumenform. Dann gilt:

$$(\Phi \circ \Psi)^* D = \Psi^*(\Phi^* D) = \det(\Psi) \cdot \Phi^* D = \det(\Psi)\det(\Phi) D,$$

und folglich $\det(\Phi \circ \Psi) = \det(\Psi)\det(\Phi) = \det(\Phi)\det(\Psi)$.

(ii) Sei D eine orientierte Volumenform und $(b_1,\dots,b_n)$ eine geordnete Basis. Da eine orientierte Volumenform genau dann 0 ist, wenn sie auf einer beliebigen geordneten Basis verschwindet, gelten dann die folgenden Äquivalenzen:

$$\begin{aligned}\det(\Phi)=0 &\iff \Phi^*D=0 \overset{(4.2.5)}{\iff} \Phi^*D(b_1,\dots,b_n)=0\\ &\iff D(\Phi(b_1),\dots,\Phi(b_n))=0 \overset{\text{Korollar 4 2 25}}{\iff} \{\Phi(b_1),\dots,\Phi(b_n)\}\text{ keine Basis}\\ &\iff \Phi\text{ nicht invertierbar,}\end{aligned}$$

wobei die letzte Äquivalenz aus Proposition 3.3.1 folgt. Dies zeigt die erste Aussage, und die zweite Aussage folgt dann aus (i). □

Die geometrische Interpretation im $\mathbb{R}^3$ ist wie folgt: Volumenverzerrung ist multiplikativ, und ein Endomorphismus ist genau dann invertierbar, wenn er kein Parallelepiped ausarten lässt.

Wir wenden uns nun der Frage zu, wie man Determinanten von Endomorphismen berechnen kann. Wir betrachten zunächst einen Spezialfall:

Bemerkung 4.3.6 (Determinante einer Matrix)**.** Sei $A\in\mathbb{K}^{n\times n}$ eine quadratische Matrix mit Spalten $s_1,\dots,s_n$ und $\Phi_A:\mathbb{K}^n\to\mathbb{K}^n$, $v\mapsto Av$. Wir definieren die *Determinante von A* durch

$$|A|:=\det(A):=\det(\Phi_A).$$

Dann gilt speziell für die Determinantenform $\mathrm{Det}=e_1^*\wedge\cdots\wedge e_n^*$, dass

$$\det(A)\cdot\mathrm{Det}=\Phi_A^*\mathrm{Det}.$$

Einsetzen von $e_1,\dots,e_n$ liefert

$$\begin{aligned}\det(A) &= \det(A)\cdot\mathrm{Det}(e_1,\dots,e_n) &&= \Phi_A^*\mathrm{Det}(e_1,\dots,e_n)\\ &= \mathrm{Det}(\Phi_A(e_1),\dots,\Phi_A(e_n)) &&= \mathrm{Det}(s_1,\dots,s_n).\end{aligned}$$

Wir erhalten also die Determinante von A durch Auswerten der Determinantenform auf den Spalten von A. Die Leibniz-Formel aus Beispiel 4.2.24 liefert daher

$$\det(A)=\sum_{\sigma\in\mathrm{Sym}_n}\mathrm{sgn}(\sigma)\cdot\prod_{i=1}^n a_{i\sigma(i)}=\sum_{\sigma\in\mathrm{Sym}_n}\mathrm{sgn}(\sigma)\cdot\prod_{j=1}^n a_{\sigma(j)j}. \tag{4.3.2}$$

Wir nennen diese Formel auch die *Leibniz-Formel für Matrizen*.

Beispiel 4.3.7 (Niedrige Dimensionen)**.** Für (2×2)- bzw. (3×3)-Matrizen erhalten wir die „Jägerzaunformeln“

$$\begin{aligned}\begin{vmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{vmatrix} &= a_{11}a_{22}-a_{12}a_{21},\\ \begin{vmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{vmatrix} &= a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32}-a_{13}a_{22}a_{31}-a_{11}a_{23}a_{32}-a_{12}a_{21}a_{33}.\end{aligned}$$

Die entsprechenden Matrizen sind also genau dann invertierbar, wenn das Ergebnis der jeweiligen Jägerzaunformel nicht 0 ist.

Beispiel 4.3.8 (Determinanten von Dreiecksmatrizen)**.** Es sei $A = (a_{ij}) \in \mathbb{K}^{n\times n}$ eine untere Dreiecksmatrix, d.h. es gilt $a_{ij} = 0$ für alle $i < j$. Nach der Leibnizformel gilt

$$|A| = \sum_{\sigma\in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i\sigma(i)}$$

Ist $\sigma(1) > 1$, so ist $a_{1\sigma(1)} = 0$, also liefern nur die Summanden mit $\sigma(1) = 1$ einen Beitrag. Sei also $\sigma(1) = 1$. Ist $\sigma(2) > 2$, so ist $a_{2\sigma(2)} = 0$, also liefern nur die Summanden mit $\sigma(1) = 1$ und $\sigma(2) = 2$ einen Beitrag usw. Mit Induktion sieht man, dass überhaupt nur ein Summand einen Beitrag liefert, nämlich die Identität. Wir erhalten also

$$|A| = \prod_{i=1}^{n} a_{ii}.$$

Dieselbe Formel gilt auch für obere Dreiecksmatrizen (Beweis analog oder mittels (4.3.3)).

Bemerkung 4.3.9 (Determinante und Spaltenumformungen)**.** Aus Korollar 4.2.31 folgt, dass die Determinante einer Matrix die folgenden Eigenschaften hat, und durch diese eindeutig festgelegt ist:

(d1) Die Determinante einer nicht-invertierbaren Matrix ist 0.

(d2) Die Determinante der Einheitsmatrix ist 1.

(d3) Die Determinante wird mit λ multipliziert, wenn man eine Spalte mit λ multipliziert.

(d4) Die Determinante ändert sich nicht, wenn man das Vielfache einer Spalte zu einer anderen Spalte addiert.

(d5) Die Determinante wird mit (-1) multipliziert, wenn man zwei Spalten vertauscht.

WARNUNG! Für $A \in \mathbb{K}^{n\times n}$ und $\lambda \in \mathbb{K}$ besagt (d3) NICHT, dass $\det(\lambda \cdot A) = \lambda \cdot \det(A)$, sondern dass $\det(\lambda \cdot A) = \lambda^n \cdot A$. Man muss nämlich (d3) auf jede der Spalten von A anwenden!

Wir können also die Determinanten einer Matrix mittels Spaltenumformungen bestimmen, analog zu Beispiel 4.2.29. Es kommt aber noch besser:

Bemerkung 4.3.10 (Determinante und Zeilenumformungen)**.** Aus der Leibniz-Formel für Matrizen folgt unmittelbar, dass

$$\det(A) = \det(A^\top) \quad \text{für alle } A \in \mathbb{K}^{n\times n}. \tag{4.3.3}$$

Das bedeutet in der Praxis, dass wir Determinanten auch durch Zeilenumformungen, bzw. sogar durch Zeilen- **und** Spaltenumformungen berechnen können! Wir müssen unsere Matrix auch nicht durch Zeilen- und Spaltenumformungen auf die Einheitsmatrix bringen, sondern lediglich auf eine (obere oder untere) Dreiecksmatrix, denn dann können wir die Determinante nach Beispiel 4.3.8 direkt ablesen.

Beispiel 4.3.11 (Ein Zahlenbeispiel)**.** Mittels Elementarumformungen rechnet man

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & 4 & 1 & 4 \\ 1 & 8 & -1 & -8 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & -2 & -3 \\ 0 & 3 & 0 & 3 \\ 0 & 7 & -2 & -9 \end{vmatrix} = -\begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 1 & -3 \\ 0 & 0 & 3 & 3 \\ 0 & -2 & 7 & -9 \end{vmatrix}$$
$$= -\begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 1 & -3 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 6 & -6 \end{vmatrix} = -\begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 1 & -3 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & -12 \end{vmatrix} = -72,$$

wobei wir im letzten Schritt Beispiel 4.3.8 verwendet haben. Insbesondere ist diese Matrix invertierbar.

In der Regel ist das Berechnen von Determinanten mittels Elementarumformungen (und Beispiel 4.3.8) schneller als das Anwenden der Leibniz-Regel.

Beispiel 4.3.12 (Signum als Determinante)**.** Für Permutationsmatrizen kann man die Determinante direkt aus der Definition bestimmen: Ist $A = S_{ij} \in \mathbb{K}^{n\times n}$ eine Transpositionsmatrix mit $1 \le i < j \le n$, so gilt

$$\det(A) = \mathrm{Det}(e_1,\dots,e_j,\dots,e_i,\dots,e_n) = -\mathrm{Det}(e_1,\dots,e_i,\dots,e_j,\dots,e_n) = -1,$$

da die Determinantenform schief-symmetrisch ist. Ist allgemeiner A eine Permutationsmatrix mit Spalten $e_{\sigma(1)},\dots,e_{\sigma(n))}$, so gilt

$$\det(A) = \mathrm{Det}e_{\sigma(1)},\dots,e_{\sigma(n))}) = \mathrm{sgn}(\sigma)\mathrm{Det}(e_1,\dots,e_i,\dots,e_j,\dots,e_n) = \mathrm{sgn}(\sigma).$$

Das Signum einer Permutation kann also als Determinante der zugehörigen Permutationsmatrix interpretiert werden.

Damit kennen wir nun die Determinanten aller Elementarmatrizen:

Bemerkung 4.3.13 (Determinanten von Elementarmatrizen)**.** Sei $A \in \mathbb{K}^{n\times n}$ eine Elementarmatrix.

(i) Ist A eine Permutationsmatrix mit Spalten $e_{\sigma(1)},\dots,e_{\sigma(n))}$, so ist $\det(A) = \mathrm{sgn}(\sigma)$ nach Beispiel 4.3.12

(ii) Ist A eine unipotente Elementarmatrix, so gilt nach Beispiel 4.3.8, dass $\det(A) = 1$.

(iii) Ist $A = \mathrm{diag}(\lambda_1,\dots,\lambda_n)$ eine Diagonalmatrix, so gilt nach Beispiel 4.3.8, dass $\det(A) = \lambda_1\cdots\lambda_n$.

Aus Satz 4.3.5 folgt andererseits:

Korollar 4.3.14. *Für quadratische Matrizen $A,B \in \mathbb{K}^{n\times n}$ gelten die Rechenregeln*

$$\det(\mathbf{1}) = 1 \quad \text{und} \quad \det(AB) = \det(A)\det(B).$$

A ist invertierbar genau dann, wenn $\det(A) \neq 0$, und in diesem Fall gilt

$$\det(A^{-1}) = \det(A)^{-1}$$

Damit ist zum Thema Determinantenberechnung von Matrizen fast alles gesagt. Es gibt noch ein weiteres rekursives Berechnungsverfahren, das wir im nächsten Abschnitt vorstellen. Wir überlegen uns nun zum Abschluss noch, wie man die allgemeine Berechnungen von Determinanten von Endomorphismen auf den Matrizenfall zurückführen kann.

Satz 4.3.15 (Berechnung von Determinanten via darstellende Matrizen)**.** *Sei* $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *und* $A := D_{\mathscr{B}}(\Phi)$ *für eine geordnete Basis* $\mathscr{B} = (b_1, \dots b_n)$ *von* V*. Dann gilt*

$$\det(\Phi) = \det(A).$$

Beweis. Es sei $\Psi := (-)_{\mathscr{B}} : V \to \mathbb{K}^n$ der Koordinatenisomorphismus zu $\mathscr{B}$. Dieser bildet $\mathscr{B}$ auf die Standardbasis $\mathscr{B}_0$ ab, es gilt also nach der Basiswechselformel

$$D_{\mathscr{B}_0,\mathscr{B}_0}(\Psi \circ \Phi \circ \Psi^{-1}) = D_{\mathscr{B}_0,\mathscr{B}}(\Psi) D_{\mathscr{B},\mathscr{B}}(\Phi) D_{\mathscr{B}_0,\mathscr{B}}(\Psi)^{-1} = \mathbf{1} \cdot A \cdot \mathbf{1}^{-1} = A,$$

und daher $\Phi_A = \Psi \circ \Phi \circ \Psi^{-1}$. Da $\Psi^* \mathrm{Det}$ eine orientierte Volumenform ist, gilt nach Definition von $\det(A)$, dass

$$\begin{aligned} \det(A) \cdot \mathrm{Det} &= \Phi_A^* \mathrm{Det} = (\Psi \circ \Phi \circ \Psi^{-1})^* (\mathrm{Det}) \\ &= (\Psi^{-1})^* (\Phi^* (\Psi^* (\mathrm{Det})) = (\Psi^{-1})^* (\det(\Phi) \cdot \Psi^* (\mathrm{Det})) \\ &= \det(\Phi) \cdot ((\Psi^{-1})^* \circ \Psi^* (\mathrm{Det})) = \det(\Phi) \cdot \mathrm{Det}. \end{aligned}$$

Einsetzen der Standardbasis liefert dann $\det(A) = \det(\Phi)$. □

Wir erhalten also die Determinante von Φ als Determinante einer beliebigen darstellenden Matrix (bzgl. zweimal derselben geordneten Basis) von Φ.

Bemerkung 4.3.16. Wie überall in der linearen Algebra muss man auch im Hinblick auf Determinanten zwischen dem abstrakten Konzept und dem konkreten Modell zur Berechnung unterscheiden. Schematisch haben wir:

abstraktes Konzept	konkretes Modell
Vektorraum	$\mathbb{K}^n$
Basis	Standardbasis
Endomorphimus	darstellende Matrix
orientierte Volumenform	Determinantenform
Determinante eines Endomorphismus	Determinante einer Matrix

Wichtig ist auch, zwischen der abstrakten Definition der Determinante und den konkreten Berechnungsmethoden zu unterscheiden.

Aussagen über Determinanten von Endomorphismen und Matrizen kann man häufig auf sehr viele verschiedene Arten interpretieren; wir geben ein Beispiel:

Korollar 4.3.17. *Es sei* V *ein* n*-dimensionaler* $\mathbb{K}$*-Vektorraum mit geordneter Basis* $\mathscr{B}$ *und* $A = D_{\mathscr{B}}(\Phi) \in \mathbb{K}^{n \times n}$ *die darstellende Matrix von* Φ *bzgl.* $\mathscr{B}$ *mit Spalten* $s_1, \dots, s_n$ *und* $z_1, \dots, z_n$*. Dann sind die folgenden Bedingungen äquivalent.*

(i) $\det(\Phi) \neq 0$.

(ii) $\det(A) \neq 0$.

(iii) Φ *ist ein Automorphismus.*

(iv) A *ist invertierbar.*

(v) A *besitzt eine Linksinverse (oder Rechtsinverse).*

(vi) $\mathrm{rk}(\Phi) = n$ *(oder* $\mathrm{def}(\Phi) = 0$*).*

(vii) $\ker(\Phi) = \{\mathbf{0}\}$.

(viii) $\ker(A) = \{\mathbf{0}\}$.

(ix) Der Spaltenrang (oder Zeilenrang) von A *ist* n.

(x) $s_1, \ldots, s_n$ *sind linear unabhängig.*

(xi) $z_1, \ldots, z_n$ *sind linear unabhängig.*

(xii) $s_1, \ldots, s_n$ *erzeugen* $\mathbb{R}^n$.

(xiii) $z_1, \ldots, z_n$ *erzeugen* $\mathbb{R}^{1\times n}$.

(xiv) Das LGS $Ax = y$ *hat für jedes* $y \in \mathbb{R}^n$ *mindestens eine Lösung.*

(xv) Das LGS $Ax = y$ *hat für jedes* $y \in \mathbb{R}^n$ *genau eine Lösung.*

(xvi) Das LGS $Ax = y$ *hat für mindestens ein* $y \in \mathbb{R}^n$ *genau eine Lösung.*

(xvii) Φ *bildet lineare unabhängige Vektoren auf lineare unabhängige Vektoren ab.*

(xviii) Φ *bildet Erzeugendensysteme auf Erzeugendensysteme ab.*

(xix) A ist ein Produkt invertierbare Elementarmatrizen.

(xx) A lässt sich durch elementare Zeilenumformungen (oder Spaltenumformungen) in $\mathbf{1}$ *transformieren.*

(xxi) $\det(A^\top) \neq 0$.

(xxii) $A^\top$ *ist invertierbar.*

(xxiii) $\Phi^* : V^* \to V^*$ *ist ein Automorphismus des Dualraums.*

Als eine Anwendung dieses Abschnitts komplettieren wir nun noch den Beweis von Bemerkung 4.2.32:

Übung 4.3.18. Wir betrachten die Abbildung

$$o : \mathbb{R}^3 \to \{-1,0,1\}, \quad o(v_1,v_2,v_3) := \begin{cases} \frac{\mathrm{Det}(v_1,v_2,v_3)}{|\mathrm{Det}(v_1,v_2,v_3)|}, & \text{falls } \mathrm{Det}(v_1,v_2,v_3) \neq 0, \\ 0, & \text{sonst.} \end{cases}$$

Zeigen Sie:

(i) $o(e_1,e_2,e_3) = 1$ und $o(v_1,v_2,v_3) = 0$, wenn v_1,v_2,v_3 linear abhängig sind.

(ii) o ist invariant unter Streckungen/Stauchungen und Scherungen und kehrt ihr Vorzeichen unter Spiegelungen um.

(iii) o ist durch (i) und (ii) eindeutig festgelegt. [Hinweis: Jede Basis lässt sich durch Streckungen/Stauchungen, Scherungen und Spiegelungen auf die Einheitsbasis bringen. Warum?]

Zusammenfassung von Abschnitt 4.3

(1) Rückzug einer orientierten Volumenform entlang eines Endomorphismus Φ multipliziert diese mit einer Konstanten, der Determinante von Φ. Geometrisch ist die Determinante eine orientierte Volumenverzerrung.

(2) Die Determinante ist multiplikativ und genau im Fall von Automorphismen von 0 verschieden.

(3) Ist Φ ein Endomorphismus und $A = D_{\mathscr{B}}(\Phi)$ eine darstellende Matrix von Φ, so berechnet man $\det(\Phi)$ durch Anwenden der Determinantenform auf die Spalten von A.

(4) Determinanten von Matrizen kann man mittels Elementarumformungen berechnen. In speziellen Fällen kann man auch die Leibniz-Formel direkt auswerten, im Allgemeinen ist dies aber nicht effizient.

[20.12.23]

4.4 Laplace-Entwicklung und die Cramersche Regel

In diesem Abschnitt beweisen wir eine Rekursionsformel für Determinanten und geben eine überraschende Anwendung: Eine explizite Formel für das Inverse einer invertierbaren Matrix in Termen von sogenannten Minoren.

Notation 4.4.1. Es sei $A = (a_{ij}) \in \mathbb{K}^{p\times q}$ eine Matrix. Sind $I = \{i_1, \dots, i_n\}$ und $J = \{j_1, \dots, j_n\}$ mit $1 \le i_1 < \cdots < i_n \le p$ und $1 \le j_1 < \cdots < j_n \le q$, so definieren wir ein $(n \times n)$-Untermatrix von A durch

$$A_{IJ} := (a_{i_k, j_l})_{k,l\in\{1,\dots,n\}} \in \mathbb{K}^{n\times n}.$$

Die Determinante $\det_{IJ}(A) := \det(A_{IJ})$ heißt dann eine *n-Minore* von A.

Beispiel 4.4.2. Wir betrachten die Matrix $A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$. Diese hat die 1-Minoren 1,2,3,4,5,6 und die 2-Minoren

$$\left|\begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix}\right| = -3, \quad \left|\begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}\right| = -6 \quad \text{und} \quad \left|\begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}\right| = -3.$$

Zwischen den Minoren einer Matrix gibt es eine Reihe interessanter Relationen. Wir überlegen uns zunächst, dass man die Determinante einer $(n \times n)$-Matrix, durch die $(n-1)$-Minoren der Matrix ausdrücken kann. (Durch wiederholtes Anwenden kann man sie dann auch durch kleinere Minoren ausdrücken.)

Notation 4.4.3. Ist $A \in \mathbb{K}^{n\times n}$ und sind $i, j \in \{1, \dots, n\}$, so schreiben wir kurz

$$A_{ij} := A_{\{1,\dots,n\}\setminus\{i\},\{1,\dots,n\}\setminus\{j\}}.$$

Die $(n-1)$-Minoren von A sind dann gerade die Minoren $\det(A_{ij})$ mit $i, j \in \{1, \dots, n\}$

Wir benötigen die folgende Verallgemeinerung von Beispiel 4.3.8:

Lemma 4.4.4 (Determinante von Blockmatrizen)**.** *Es seien $a, c \in \mathbb{N}$. Dann gilt für alle $A \in \mathbb{K}^{a\times a}$, $B \in \mathbb{K}^{a\times c}$ und $C \in \mathbb{K}^{c\times c}$*

$$\det\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A) \cdot \det(C).$$

Beweis. Es seien $A = (a_{ij})$, $C = (c_{ij})$ und $D = (d_{ij})$ gegeben durch $D := \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$. Nach 4.3.2 gilt

$$\det(D) = \sum_{\sigma\in \mathrm{Sym}_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} d_{\sigma(i)i}$$

Falls $i \in \{1, \dots, a\}$ und $\sigma(i) > a$, so ist $d_{\sigma(i)i} = 0$. Es tragen also nur Permutationen σ zur Summe bei, die die Menge $\{1, \dots, a\}$ (und daher auch die Menge $\{a+1, \dots, a+c\}$) auf sich selbst abbilden.

Es gilt daher

$$\begin{aligned}
\det(D) &= \sum_{\sigma_1\in S_a}\sum_{\sigma_2\in S_c}\operatorname{sgn}(\sigma_1\circ\sigma_2)\prod_{i=1}^{a} d_{\sigma(i),i}\prod_{j=1}^{c} d_{a+\sigma_2(j),a+j}\\
&= \sum_{\sigma_1\in S_a}\sum_{\sigma_2\in S_c}\operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)\prod_{i=1}^{a} a_{\sigma(i),i}\prod_{j=1}^{c} c_{\sigma_2(j),j}\\
&= \sum_{\sigma_1\in S_a}\operatorname{sgn}(\sigma_1)\prod_{i=1}^{a} a_{\sigma(i),i}\sum_{\sigma_2\in S_c}\operatorname{sgn}(\sigma_2)\prod_{j=1}^{c} c_{\sigma_2(j),j}\\
&= \det(A)\cdot\det(C).
\end{aligned}$$

Damit ist die Formel bewiesen. □

Übung 4.4.5. Gilt für jede Blockmatrix der Form $\begin{pmatrix} A & B\\ C & D\end{pmatrix}$ die Formel

$$\det(A)\cdot\det(D)-\det(B)\cdot\det(C)?$$

[Wir müssen natürlich voraussetzen, dass B und C quadratisch sind, damit alle Determinanten definiert sind.]

Bemerkung 4.4.6 (Entwickeln nach der ersten Spalte)**.** Es sei $A=(a_{ij})\in\mathbb{K}^{n\times n}$ eine Matrix mit Spalten $s_1,\dots,s_n$. Es gilt dann wegen Multilinearität der Determinantenform, dass

$$\begin{aligned}
\det(A) &= \operatorname{Det}(s_1,\dots,s_n) = \operatorname{Det}(a_{11}e_1+\cdots+a_{n1}e_n,s_2,\dots,s_n)\\
&= \sum_{i=1}^{n} a_{i1}\operatorname{Det}(e_i,s_2,\dots,s_n).
\end{aligned}$$

Nun ist $\operatorname{Det}(e_i,s_2,\dots,s_n)$ gerade die Determinante der Matrix mit Spalten $e_i,s_2,\dots,s_n$. Wir vertauschen nun in dieser Matrix die Zeilen mittels der Permutation $\tau=(1,2,\dots,i)$, so erhalten wir Matrix

$$\begin{pmatrix} 1 & a_{i2} & \dots & a_{in}\\ 0 & & & \\ & & A_{i1} & \\ 0 & & & \end{pmatrix},$$

Nach Lemma 4.4.4 hat diese Matrix Determinante $\det(A_{i1})$, und mit $\operatorname{sgn}(\tau)=(-1)^{i+1}$ folgt

$$\operatorname{Det}(a_{i1}\cdot e_i,s_2,\dots,s_n)=(-1)^{i+1}\det(A_{i1}).$$

Damit haben wir gezeigt, dass

$$\det(A)=\sum_{i=1}^{n}(-1)^{i+1}a_{i1}\det(A_{i1}) \tag{4.4.1}$$

Man nennt diese Formel die *Laplace*[6]*-Entwicklung* von A nach der ersten Spalte.

Beispiel 4.4.7.

$$\begin{vmatrix} 1 & 2 & 3\\ 2 & 3 & 4\\ 0 & 4 & 5\end{vmatrix} = 1\cdot\begin{vmatrix} 3 & 4\\ 4 & 5\end{vmatrix} - 2\cdot\begin{vmatrix} 2 & 3\\ 4 & 5\end{vmatrix} = 1\cdot(-1)-2\cdot(-2)=3.$$

[6] PIERRE-SIMON LAPLACE, frz. Universalgelehrter, 1749-1827

Analog kann man auch nach einer beliebigen anderen Spalte entwickeln: Um nach der j-ten Spalte zu entwickeln, permutiert man die Spalten mittels des Zykels $(1,2,\dots,j)$ (was ein zusätzliches Vorzeichen $(-1)^{1+j}$ liefert) und entwickelt dann nach der ersten Spalte. Daraus folgt nun:

Satz 4.4.8 (Laplace-Entwicklung, Spaltenform)**.** *Für $A=(a_{ij})\in\mathbb{K}^{n\times n}$ und $k\in\{1,\dots,n\}$ gilt*

$$\det(A)=\sum_{i=1}^{n}(-1)^{k+i}a_{ik}\cdot\det(A_{ik}).$$ □

Da die Determinanten invariant unter Tranposition ist, kann man analog auch nach einer beliebigen Zeile entwickeln. Hierbei verwendet man, dass $\det(A)=\det(A^\top)$ und $\det((A^\top)_{ik})=\det((A_{ki})^\top)=\det(A_{ki})$. Man erhält dann:

Satz 4.4.9 (Laplace-Entwicklung, Zeilenform)**.** *Für $A=(a_{ij})\in\mathbb{K}^{n\times n}$ und $k\in\{1,\dots,n\}$ gilt*

$$\det(A)=\sum_{j=1}^{n}(-1)^{j+k}a_{kj}\cdot\det(A_{kj}).$$ □

Bemerkung 4.4.10 (Wozu ist das gut?)**.** Mittels Laplace-Entwicklung können wir die Determinanten einer $(n\times n)$-Matrix durch n Determinanten von $(n-1)\times(n-1)$-Matrizen ausdrücken. Man kann dieses Spiel nun noch weiter treiben, und jede dieser Determinanten wieder durch $(n-1)$-Determinanten von $(n-2)\times(n-2)$-Matrizen ausdrücken. Treibt man die Sache auf die Spitze, so erhält man am Ende einen Ausdruck für die Determinanten, der aus $n!$ Determinanten von (1×1)-Matrizen (also Matrixeinträgen) besteht – nämlich die Leibnizformel, die zum Berechnen bekanntermaßen ineffizient ist. Für das praktische Rechnen empfiehlt sich Entwicklung nach einer Spalte oder Zeile nur, wenn in dieser Spalte oder Zeile viele 0en vorhanden sind.

Die Laplace-Entwicklung hat aber mehrere wichtige theoretische Zwecke. Zum einen wird sie in der Kombinatorik häufig eingesetzt, um Rekursionsformeln zu beweisen; zum anderen liefert sie eine geschlossene Formel für das Inverse einer invertierbaren Matrix.

Beispiel 4.4.11. Für beliebige $n\geq 2$ und $x_1,\dots,x_n\in\mathbb{K}$ ist die Vandermondsche[7] Determinante $V(x_1,\dots,x_n)$ definiert als

$$V(x_1,\dots,x_n)=\left|\begin{pmatrix}1 & 1 & \dots & 1\\ x_1 & x_2 & \dots & x_n\\ x_1^2 & x_2^2 & \dots & x_n^2\\ \vdots & \vdots & & \vdots\\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1}\end{pmatrix}\right|.$$

Für $n=2$ gilt

$$V(x_1,x_2)=\left|\begin{pmatrix}1 & 1\\ x_1 & x_2\end{pmatrix}\right|=1\cdot x_2-x_1\cdot 1=(x_2-x_1).$$

Für $n\geq 3$ ziehen wir von jeder Zeile das x_1-fache der vorigen Zeile ab, wobei wir von oben nach unten vorgehen. Wir erhalten dann durch Entwickeln nach der ersten Spalte und unter

[7] ALEXANDRE-THÉOPHILE VANDERMONDE, frz. Geiger und (später) Mathematiker, 1735-1796

Verwendung der Multilinearität,

$$\begin{aligned}
V(x_1,\dots,x_n) &= \left|\begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix}\right| = \left|\begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & x_2-x_1 & \dots & x_n-x_1 \\ 0 & x_2^2-x_1x_2 & \dots & x_n^2-x_1x_n \\ \vdots & \vdots & & \vdots \\ 0 & x_2^{n-1}-x_1x_2^{n-2} & \dots & x_n^{n-1}-x_1x_n^{n-2} \end{pmatrix}\right| \\
&= \left|\begin{pmatrix} x_2-x_1 & \dots & x_n-x_1 \\ x_2^2-x_1x_2 & \dots & x_n^2-x_1x_n \\ \vdots & & \vdots \\ x_2^{n-1}-x_1x_2^{n-2} & \dots & x_n^{n-1}-x_1x_n^{n-2} \end{pmatrix}\right| = \left|\begin{pmatrix} (x_2-x_1) & \dots & (x_n-x_1) \\ (x_2-x_1)x_2 & \dots & (x_n-x_1)x_n \\ \vdots & & \vdots \\ (x_2-x_1)x_2^{n-2} & \dots & (x_n-x_1)x_n^{n-2} \end{pmatrix}\right| \\
&= (x_2-x_1)\cdots(x_n-x_1)\cdot V(x_2,\dots,x_n).
\end{aligned}$$

Wir erhalten also

$$V(x_1,x_2,x_3) = (x_2-x_1)(x_3-x_1)V(x_2,x_3) = (x_2-x_1)(x_3-x_1)(x_3-x_2),$$

und allgemein für beliebige $n \geq 2$ die Formel

$$V(x_1,\dots,x_n) = \prod_{1\leq i<j\leq n} (x_j - x_i).$$

Formal beweist man diese Formel mit vollständiger Induktion.

Es ist eine interessante Tatsache, dass die Anzahl, der $(n-1)$-Minoren einer $(n\times n)$-Matrix genau n^2 ist, und man daher die $(n-1)$-Minoren wieder zu einer quadratischen Matrix anordnen kann.

Definition 4.4.12. Ist $A = (a_{ij}) \in \mathbb{K}^{n\times n}$, so defineren wir die *adjunkte Matrix* $A^\sharp$ von A als

$$A^\sharp := (\alpha_{ij}) \in \mathbb{K}^{n\times n} \text{ durch } \alpha_{ij} := (-1)^{i+j}\det(A_{ji}).$$

WARNUNG! Man beachte die Vorzeichen und die Verdrehung der Indizes in der Definition von α_{ij}!

Beispiel 4.4.13. Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Dann gilt $A_{12} = (c)$, und daher $\alpha_{21} = (-1)^{2+1}\det(A_{12}) = -c$. Analog rechnet man $\alpha_{11} = d$, $\alpha_{12} = -b$ und $\alpha_{22} = a$, also

$$A^\sharp = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Ist A invertierbar, so haben wir andererseits in Satz 2.1.47 gesehen, dass

$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{\det(A)}\cdot A^\sharp.$$

Das gilt ganz allgemein:

Satz 4.4.14 (Cramersche[8] Regel)**.** *Ist $A \in \mathbb{K}^{n\times n}$, so gilt*

$$A \cdot A^\sharp = \det(A) \cdot \mathbf{1}.$$

Ist speziell A invertierbar, so gilt

$$A^{-1} = \frac{1}{\det(A)} \cdot A^\sharp.$$

Beweis. Wir betrachten die Matrizen $A = (a_{ij})$, $A^\sharp = (\alpha_{ij})$ und $B := AA^\sharp = (b_{ij})$.
1. FALL: Wir berechnen die Diagonaleinträge b_{ii} für $1 \le i \le n$. Nach Satz 4.4.9 gilt

$$b_{ii} = \sum_{j=1}^{n} a_{ij}\alpha_{ji} = \sum_{j=1}^{n} a_{ij}(-1)^{i+j}\det(A_{ij}) = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij}) = \det(A).$$

2. FALL: Wir berechnen den Eintrag b_{ik} im Fall $1 \le i < k \le n$. Nach Definition ist

$$b_{ik} = \sum_{j=1}^{n} a_{ij}\alpha_{jk} = \sum_{j=1}^{n}(-1)^{j+k}a_{ij}\det(A_{kj});$$

Nach Satz 4.4.9 ist dies aber gerade die Determinante der Matrix, die aus A ensteht, indem man die k-te Spalte durch die i-te Spalte ersetzt. Diese Matrix hat aber zwei gleiche Spalten, also ist die ihre Determinante 0. Dies zeigt $b_{ik} = 0$.
3. FALL: Wir berechnen den Eintrag b_{ik} im Fall $1 \le k < i \le n$. Die Rechnung ist analog zum 2. Fall und liefert $b_{ik} = 0$. □

Bemerkung 4.4.15. Diese Regel ist aufgrund des Rechenaufwands in keiner Weise für die praktische Bestimmung der Inversen geeignet - außer für $n = 2$. Sie ist aber von großer theoretischer Bedeutung, weil sie besagt, dass die Einträge der inversen Matrix in polynomieller Weise (und im reellen Fall insbesondere stetig differenzierbar) von den Einträgen der ursprünglichen Matrix abhängen. Die Konsequenzen dieser Tatsache werden wir in der Vorlesung LINEARE ALGEBRA II genauer untersuchen. Wir geben hier zunächst eine sehr einfache, aber wichtige Anwendung.

Beispiel 4.4.16. Aufgaben vom folgenden Typ sind aus dem Arithmetischen Handbuch von Chang Ch'iu-chien (um 475 n. Chr.) überliefert: *Ein Hahn kostet* 3 *Sapek und eine Henne* 2 *Sapek. Wenn wir nun für* 100 *Sapek* 40 *dieser Tiere einkaufen, wieviele Hähne kaufen wir?* Dieses Problem führt auf das ganzzahlige LGS

$$\begin{pmatrix}1 & 1\\ 3 & 2\end{pmatrix} x = \begin{pmatrix}40\\ 100\end{pmatrix},$$

wobei x_1 die Anzahl der Hähne und x_2 die Anzahl der Hennen bezeichnet. Trotz gutem Zuredens lässt sich der Tierhändler nicht darauf ein, halbe Tiere zu verkaufen. Man interessiert sich also in diesem Fall nur für *ganzzahlige* Lösungen des Systems. Systematisch lernen Sie die Lösungstheorie solcher ganzzahliger Systeme in der Vorlesung EINFÜHRUNG IN ALGEBRA UND ZAHLENTHEORIE im 4. Semester kennen. In diesem Fall können wir die Lösung direkt angeben: Es gilt

$$\begin{pmatrix}1 & 1\\ 3 & 2\end{pmatrix}^{-1} = \frac{1}{(-1)} \cdot \begin{pmatrix}2 & -1\\ -3 & 1\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 3 & -1\end{pmatrix} \Longrightarrow x = \begin{pmatrix}-2 & 1\\ 3 & -1\end{pmatrix}\begin{pmatrix}40\\ 100\end{pmatrix} = \begin{pmatrix}20\\ 20\end{pmatrix}$$

Wir kaufen also 20 Hähne.

[8] Gabriel Cramer, Schweizer Mathematiker, 1704-1752

In diesem Fall hatten wir zufällig Glück, weil die inverse Matrix selbst wieder ganzzahlig war. Das is aber nicht bei jeder ganzzahligen Matrix der Fall, so gilt etwa $\mathrm{diag}(1,3)^{-1} = \mathrm{diag}(1,1/3)$.

Bemerkung 4.4.17 (Ganzzahlige Inverse)**.** Es sei $A = (a_{ij}) \in \mathbb{Q}^{n\times n}$ eine $(n \times n)$-Matrix mit ganzzahligen Einträgen (a_{ij}). Wann hat die inverse Matrix A^{-1} selbst wieder ganzzahlige Einträge? Wir beobachten zunächst, dass die Determinanten einer Matrix mit ganzzahligen Einträgen wieder eine ganze Zahl ist, weil in die Definition der Determinanten nur die Matrixeinträge sowie Addition, Multiplikation und Vorzeichen eingehen. Analog sieht man, dass die Minoren einer ganzzahligen Matrix ganze Zahlen sind.

Hat die ganzzahlige Matrix A eine ganzzahlige Inverse A^{-1}, so muss gelten

$$1 = \det(\mathbf{1}) = \det(AA^{-1}) = \det(A)\det(A^{-1}),$$

wobei $\det(A)$ und $\det(A^{-1})$ ganze Zahlen sind. Das ist aber nur möglich, wenn $\det(A)$ ein Teiler von 1 also 1 oder -1, ist.

Wir behaupten nun, dass auch die Umkehrung gilt: Es sei also A ganzzahlig mit $\det(A) \in \{-1,1\}$, also $\det(A)^{-1} = \det(A)$ Nach der Cramerschen Regel gilt dann

$$A^{-1} = \frac{1}{\det(A)} \cdot A^\sharp = \det(A) \cdot A^\sharp,$$

und da die Einträge von $A^\sharp$ bis auf Vorzeichen Minoren von A sind, ist diese Matriz ganzzahlig!

Wir fassen zusammen:

Korollar 4.4.18. *Eine ganzzahlige Matrix A hat genau dann eine ganzzahlige Inverse, wenn ihre Determinante* 1 *oder* -1 *ist.* □

Zusammenfassung von Abschnitt 4.4

(1) Determinanten lassen sich rekursiv durch Entwickeln nach einer Zeile oder Spalte bestimmen. Für das praktische Rechnen ist das allerdings nur in Ausnahmefällen nützlich.

(2) Die Cramersche Regel gibt eine geschlossene Formel für die Inverse einer invertierbaren Matrix. Diese ist z.B. nützlich um zu entscheiden, ob die Inverse einer ganzzahligen Matrix ganzzahlig ist.

4.5 Eigenwerte und Eigenvektoren

Als eine weitere Anwendung von Determinanten riskieren wir einen ersten Blick auf das Normalformenproblem für Endomorphismen (Problem 3.1.20.(ii)). Dieses fragt für einen gegebenen Endomorphismus $\Phi : V \to V$ eines endlichdimensionalen $\mathbb{K}$-Vektorraums V nach einer geordneten Basis $\mathscr{B}$ von V, so dass die darstellende Matrix $D_{\mathscr{B}}(\Phi)$ „möglichst einfach“ ist. Eine mögliche Klasse von sehr einfachen Matrizen sind Diagonalmatrizen; wir führen daher den folgenden Begriff ein:

Definition 4.5.1. $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ heißt *diagonalisierbar*, falls eine geordnete Basis $\mathscr{B}$ von V existiert, so dass $D_{\mathscr{B}}(\Phi)$ eine Diagonalmatrix ist. Man sagt dann auch, dass $\mathscr{B}$ den Endomorphismus Φ *diagonalisiert*.

Beispiel 4.5.2 (Spiegelungen)**.** Wir haben bereits in Beispiel 3.1.19 gesehen, dass jede Geradenspiegelung Φ im $\mathbb{R}^2$ an einer Ursprungsgeraden diagonalisierbar sind: Ist v_1 ein Vektor auf der Spiegelachse von Φ_1 und v_2 ein dazu senkrechter Vektor mit $v_1 \neq 0 \neq v_2$, so ist $\mathrm{B} = (v_1, v_2)$ eine geordnete Basis des $\mathbb{R}^2$ mit $D_{\mathscr{B}}(\Phi) = \mathrm{diag}(1,-1)$.

Bemerkung 4.5.3. Nehmen wir an, dass $\mathscr{B} = (v_1, \ldots, v_n)$ den Endomorphismus Φ diagonalisiert. Nach Definition existieren dann $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$, so dass

$$D_{\mathscr{B}}(\Phi) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$$

gilt. Dies bedeutet aber gerade, dass $v_1^*(\Phi(v_1)) = \lambda_1$, $v_2^*(\Phi(v_1)) = 0, \ldots, v_n^*(\Phi(v_1)) = 0$, also $\Phi(v_1) = \lambda_1 v_1$. Analog überlegt man sich, dass

$$\Phi(v_1) = \lambda_1 v_1, \quad \Phi(v_2) = \lambda_2 v_2, \quad \ldots, \quad \Phi(v_n) = \lambda_n v_n. \tag{4.5.1}$$

Gilt umgekehrt (4.5.1) für eine geordnete Basis $\mathscr{B} = (v_1, \ldots, v_n)$, so ist $D_{\mathscr{B}}(\Phi) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$.

Definition 4.5.4. Sind $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$, $\lambda \in \mathbb{K}$ und $v \in V$ mit

$$\Phi(v) = \lambda v \quad \text{und} \quad v \neq 0,$$

so heißt v ein *Eigenvektor* von Φ und λ ein *Eigenwert* von Φ. Wir sagen dann auch, v ist ein Eigenvektor von Φ zum Eigenwert λ.

Mit dieser Terminologie können wir Bemerkung 4.5.3 wie folgt formulieren:

Proposition 4.5.5 (1. Diagonalisierbarkeitskriterium)**.** *$\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ ist genau dann diagonalisierbar, wenn V eine geordnete Basis aus Eigenvektoren von Φ besitzt, und in diesem Fall diagonalisiert jede solche geordnete Basis Φ.* □

Bemerkung 4.5.6 (Charakterisierung von Eigenwerten)**.** Es sei v ein Eigenvektor von Φ zum Eigenwert λ. Dann gilt

$$\Phi(v) = \lambda v \iff (\lambda \cdot \mathrm{Id} - \Phi)v = \mathbf{0} \iff v \in \ker(\lambda \cdot \mathrm{Id} - \Phi) \implies \ker(\lambda \cdot \mathrm{Id} - \Phi) \neq \{\mathbf{0}\}$$

Mit Korollar 4.3.17 folgt dann, dass für jeden Eigenwert λ die Gleichung

$$\det(\lambda \cdot \mathrm{Id} - \Phi) = 0. \tag{4.5.2}$$

gelten muss. Gilt umgekehrt (4.5.2) für ein $\lambda \in \mathbb{K}$, so existiert nach Korollar 4.3.17 eine nichttriviale Lösung v des LGS $(\lambda \cdot \mathrm{Id} - \Phi)v = \mathbf{0}$. Dann ist aber v nach Definition gerade ein Eigenvektor von Φ zum Eigenwert λ. Damit haben wir den folgenden Satz bewiesen.

Satz 4.5.7 (Eigenwertgleichung)**.** *Die Eigenwerte von Φ sind genau die Nullstellen der Funktion*

$$\chi_\Phi : \mathbb{K} \to \mathbb{K}, \quad x \mapsto \det(x \cdot \mathrm{Id} - \Phi).$$ □

Die Funktion χ_Φ ist eine sogenannte Polynomfunktion und heißt die *charakteristische Polynomfunktion* von Φ. Wir werden solche Polynomfunktionen im nächsten Kapitel systematisch untersuchen und unter anderem zeigen, dass solche Funktionen nur endlich viele Nullstellen haben. Dies wird insbesondere zeigen, dass Endomorphismen endlichdimensionaler Vektorräume nur endlich viele Eigenwerte haben.

[22.12.23]

Bemerkung 4.5.8 (Eigengeraden und Eigenräume)**.** Ist v ein Eigenvektor von Φ zum Eigenwert λ, so nennen wir $\mathbb{K}v$ eine *Eigengerade* zum Eigenwert λ. Eigengeraden sind gerade diejenigen Ursprungsgeraden, die von Φ wieder auf sich selbst abgebildet werden (und dabei gestreckt oder gestaucht und ggf. gespiegelt werden). Eigenvektoren sind gerade die Basisvektoren solcher Eigengeraden.

Ist λ ein Eigenwert von Φ, so nennen wir $V_\lambda(\Phi) := \ker(\lambda \cdot \mathrm{Id} - \Phi) = \{v \in V \mid \Phi(v) = \lambda v\}$ den *Eigenraum* von Φ zum Eigenwert λ. Dieser enthält alle Eigenvektoren und alle Eigengeraden von Φ zum Eigenwert λ und wird unter Φ ebenfalls auf sich selber abgebildet (und dabei gestreckt oder gestaucht und ggf. gespiegelt).

Beispiel 4.5.9 (Geometrische Beispiele)**.** Wir betrachten spezielle Endomorphismen Φ von $\mathbb{R}^2$:

(i) Ist Φ die Spiegelung an einer Ursprungsgeraden, so besitzt Φ genau zwei Eigengeraden: Die Spiegelungsachse (mit Eigenwert 1) und die dazu senkrechte Ursprungsgerade (mit Eigenwert -1).

(ii) Ist Φ die Punktspiegelung am Ursprung, so ist $V_{-1}(\Phi) = \mathbb{R}^2$. Jede Ursprungsgerade ist daher eine Eigengerade zum Eigenwert -1.

(iii) Ist Φ eine Drehung um den Ursprung um einen Winkel, der kein ganzzahliges Vielfaches von π ist, dann besitzt Φ offensichtlich keine Eigengeraden (und daher auch keine Eigenwerte oder Eigenvektoren).

In Beispiel 4.5.9 konnten wir die Eigenwerte, Eigenvektoren, Eigengeraden und Eigenräume direkt mittels unserer geometrischen Anschauung bestimmen. Bei komplizierteren Beispielen wird das nicht mehr so einfach sein. Mittels Satz 4.5.7 können wir aber die Eigenwerte stets rechnerisch bestimmen – zumindest wenn es uns gelingt die Nullstellen der charakteristischen Polynomfunktion zu bestimmen. Im Allgemeinen ist es ein schwieriges algorithmisches Problem, Nullstellen von Polynomfunktionen zu bestimmen - wir werden darauf noch zurückkommen - aber dies soll uns nicht aufhalten. Wir überlegen uns zunächst, wie man die charakteristische Polynomfunktion praktisch berechnet:

Bemerkung 4.5.10. Ist A die darstellende Matrix von Φ zu einer beliebigen geordneten Basis $\mathscr{B}$, so gilt

$$D_{\mathscr{B}}(x \cdot \mathrm{Id} - \Phi) = x \cdot D_{\mathscr{B}}(\mathrm{Id}) - D_{\mathscr{B}}(\Phi) = x \cdot \mathbf{1} - A.$$

Die charakterische Polynomfunktion von Φ ist dann also durch

$$\chi_\Phi(x) = \chi_A(x) := \det(x \cdot \mathbf{1} - A)$$

gegeben. Man nennt χ_A auch die *charakteristische Polynomfunktion der Matrix* A.

Damit können wir nun die geometrischen Einsichten aus Beispiel 4.5.9 rechnerisch untermauern:

Beispiel 4.5.11. Es sei $\Phi = \Phi_A \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ die Spiegelung mit darstellender Matrix

$$A := \begin{pmatrix} \cos(2t) & \sin(2t) \\ \sin(2t) & -\cos(2t) \end{pmatrix}.$$

Die charakteristische Polynomfunktion von Φ ist

$$\chi_\Phi(x) = \chi_A(x) = \left|\begin{pmatrix} x-\cos(2t) & -\sin(2t) \\ -\sin(2t) & x+\cos(2t) \end{pmatrix}\right| = (x^2-\cos^2(2t)) - \sin^2(2t) = x^2 - 1 = (x-1)(x+1),$$

die Eigenwerte von Φ sind also (wie wir bereits wissen) -1 und 1.

Beispiel 4.5.12. Es sei $\Phi = \Phi_A \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ die Drehung mit darstellender Matrix

$$A := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},$$

wobei $\theta \in \mathbb{R}$ kein ganzzahliges Vielfaches von π sei. Die charakteristische Polynomfunktion von Φ ist

$$\begin{aligned} \chi_\Phi(x) &= \chi_A(x) = \left|\begin{pmatrix} x-\cos(\theta) & \sin(\theta) \\ -\sin(\theta) & x-\cos(\theta) \end{pmatrix}\right| = (x-\cos(\theta))^2 + \sin^2(\theta) \\ &= x^2 - 2\cos(\theta)x + \cos^2(\theta) + \sin^2(\theta) = x^2 - 2\cos(\theta)x + 1. \end{aligned}$$

Aus der Schule wissen Sie vielleicht, dass die Funktion $p : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax^2 + bx + c$ genau dann eine reelle Nullstelle hat, wenn die Diskriminante $D(p) = b^2 - 4ac$ nicht-negativ ist. (Das ist Teil der Aussage der sogenannten Mitternachtsformel.) In unserem Fall gilt aber

$$D(\chi_\Phi) = (-2\cos(\theta))^2 - 4 \cdot 1 \cdot 1 = 4(\cos^2(\theta) - 1) = -4\sin^2(\theta).$$

Da θ kein ganzzahliges Vielfaches von π ist, ist also $D(\chi_\Phi) < 0$. Daher hat Φ keine Eigenwerte.

Übung 4.5.13. Was passiert im letzten Beispiel, wenn θ ein Vielfaches von π ist?

Sieht man von dem Problem ab, das wir bislang keine Methode kennen, um systematisch Nullstellen von Polynomfunktionen zu bestimmen, so können wir mit dem bisher Gelernten einen Algorithmus zur Diagonalisierung diagonalisierbare Endomorphismen angeben.

Bemerkung 4.5.14 (Diagonalisierungsalgorithmus)**.** Es sei Φ ein Endomorphismus eines endlichdimensionalen Vektorraums V. Zum Diagonalisieren von V können wir wie folgt vorgehen.

1. Wähle eine beliebige Basis und stelle die entsprechende darstellende Matrix A von Φ auf.
2. Bestimme die charakteristische Polynomfunktion χ_A von A.
3. Bestimme die Nullstellen von χ_A. Diese sind die Eigenwerte von Φ.
4. Für jeden Eigenwert λ von Φ bestimme den zugehörigen Eigenraums $V_\lambda(\Phi)$.
5. Falls die Eigenräume nicht ganz V aufspannen, so ist Φ nicht diagonalisierbar.
6. Andernfalls wähle eine geordnete Basis aus Eigenvektoren. Bzgl. dieser Basis nimmt die darstellende Matrix von Φ Diagonalgestalt an.

Dieser Algorithmus verwendet viele Algorithmen, die wir schon von früher kennen: 1. benötigt das Aufstellen einer darstellenden Matrix. 2. benötigt das Berechnen einer Determinante. 4. benötigt das Lösen eines linearen Gleichungssystems. Für 3. fehlt uns derzeit noch ein Algorithmus, aber in konkreten Beispielen lassen sich die Nullstellen häufig bestimmen.

Beispiel 4.5.15. Wir diagonalisieren die Spiegelung $\Phi = \Phi_A$ aus Beispiel 4.5.11 mittels des obigen Algorithmus, wobei wir der Einfachheit halber annehmen, dass t kein ganzzahliges Vielfaches von $\frac{\pi}{2}$ ist. Schritte 1.-3. des Algorithmus haben wir bereits durchgeführt und wissen daher, dass die Eigenwerte 1 und -1 ist. Der Eigenraum zum Eigenwert 1 ist

$$V_1(\Phi) = \ker(\mathbf{1} - A) = \ker\begin{pmatrix} 1-\cos(2t) & -\sin(2t) \\ -\sin(2t) & 1+\cos(2t) \end{pmatrix}.$$

Mutliplizieren wir die erste Zeile der Matrix mit $\sin(2t)$ und die untere Zeile mit $\cos(2t)$ und subtrahieren dann die zweite Zeile von der ersten, so erhalten wir

$$\begin{pmatrix} \sin(2t)-\sin(2t)\cos(2t) & -\sin^2(2t) \\ -\sin(2t)\cos(2t) & \cos(2t)+\cos^2(2t) \end{pmatrix} \rightsquigarrow \begin{pmatrix} \sin(2t) & -\cos(2t)-1 \\ -\sin(2t)\cos(2t) & \cos(2t)+\cos^2(2t) \end{pmatrix}$$

Multiplizieren wir jetzt die erste Zeile mit $\cos(2t)$ und addieren wir diese zur zweiten, so erhalten wir die Matrix

$$B := \begin{pmatrix} \sin(2t) & -\cos(2t)-1 \\ 0 & 0 \end{pmatrix} \quad \text{mit} \quad V_1(\Phi) = \ker(B) = \left\langle \begin{pmatrix} \frac{\cos(2t)+1}{\sin(2t)} \\ 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} \cot(2t)+\csc(2t) \\ 1 \end{pmatrix} \right\rangle$$

Analog rechnet man nach, dass

$$V_{-1}(\Phi) = \left\langle \begin{pmatrix} \cot(2t)-\csc(2t) \\ 1 \end{pmatrix} \right\rangle.$$

Setzen wir $\mathscr{B} := \left(\begin{pmatrix} \cot(2t)+\csc(2t) \\ 1 \end{pmatrix}, \begin{pmatrix} \cot(2t)-\csc(2t) \\ 1 \end{pmatrix} \right)$, so erhalten wir $D_{\mathscr{B}}(\Phi) = \operatorname{diag}(1,-1)$.

Übung 4.5.16. Was ändert sich, wenn t ein ganzzahliges Vielfaches von $\pi/2$ ist?

Definition 4.5.17. Eine Matrix $A \in \mathbb{K}^{n\times n}$ heißt *diagonalisierbar*, falls die zugehörige lineare Abbildung $\Phi_A : \mathbb{K}^n \to \mathbb{K}^n$ ist. In diesem Fall heißen die Eigenwerte und Eigenvektoren von Φ_A auch die *Eigenwerte* und *Eigenvektoren* von A.

Bemerkung 4.5.18 (Diagonalisierungsformel für Matrizen)**.** Es sei $A \in \mathbb{K}^{n\times n}$ diagonalisierbar und $\mathscr{B} = (v_1, \ldots, v_n)$ eine Basis, die Φ_A diagonalisiert, so gilt nach Definition gerade

$$D_{\mathscr{B}}(\Phi_A) = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

Nach der Basiswechselformel gilt aber

$$A = D_{\mathscr{B}_0}(\Phi_A) = D_{\mathscr{B}_0,\mathscr{B}}(\mathrm{Id}) \cdot D_{\mathscr{B}}(\Phi_A) \cdot D_{\mathscr{B}_0,\mathscr{B}}(\mathrm{Id})^{-1},$$

wobei $\mathscr{B}_0 = (e_1, \ldots, e_n)$ die Standardbasis ist. Die Matrix $S := D_{\mathscr{B}_0,\mathscr{B}}(\mathrm{Id})$ ist aber gerade die Matrix, deren Spalten die Eigenvektoren $v_1, \ldots, v_n$ bilden, und wir bezeichnen diese Matrix (etwas unsauber) auch kurz mit $S = (v_1, \ldots, v_n)$. Es gilt dann also

$$A = (v_1, \ldots, v_n) \cdot \operatorname{diag}(\lambda_1, \ldots, \lambda_n) \cdot (v_1, \ldots, v_n)^{-1}. \tag{4.5.3}$$

Beispiel 4.5.19. Aus Beispiel 4.5.15 folgt mit (4.5.3), dass

$$\begin{pmatrix} \cos(2t) & \sin(2t) \\ \sin(2t) & -\cos(2t) \end{pmatrix} = S \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} S^{-1} \quad \text{mit} \quad S := \begin{pmatrix} \cot(2t)+\csc(2t) & \cot(2t)-\csc(2t) \\ 1 & 1 \end{pmatrix}. \tag{4.5.4}$$

Bemerkung 4.5.20 (Potenzen diagonalisierbarer Matrizen)**.** Ist $A = S\mathrm{diag}(\lambda_1,\dots,\lambda_n)S^{-1}$ wie in (4.5.3), so gilt

$$\begin{aligned} A^2 &= S\mathrm{diag}(\lambda_1,\dots,\lambda_n)S^{-1}S\mathrm{diag}(\lambda_1,\dots,\lambda_n)S^{-1} = S\mathrm{diag}(\lambda_1,\dots,\lambda_n)\mathrm{diag}(\lambda_1,\dots,\lambda_n)S^{-1} \\ &= S\mathrm{diag}(\lambda_1^2,\dots,\lambda_n^2)S^{-1}. \end{aligned}$$

Allgemeiner gilt für alle $k \in \mathbb{N}$ die Formel

$$A^k = S\mathrm{diag}(\lambda_1^k,\dots,\lambda_n^k)S^{-1}. \tag{4.5.5}$$

Mittels Diagonalisierung kann man also eine geschlossene Formel für die Potenzen einer beliebigen diagonalisierbaren Matrix angeben!

Für Spiegelungsmatrizen A folgt aus (4.5.4) und (4.5.5) gerade, dass $A^2 = \mathbf{1}$, was geometrisch klar ist. Es gibt aber wesentlich interessantere Beispiele.

Beispiel 4.5.21. Wir berechnen die Potenzen der Matrix

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

Die charakteristische Polynomfunktion von A ist

$$\chi_A(x) = \left|\begin{pmatrix} x-1 & -1 \\ -1 & x \end{pmatrix}\right| = (x-1)\cdot x - 1\cdot 1 = x^2 - x - 1.$$

Diese Matrix hat keine rationalen Nullstellen, ist also als Element von $\mathbb{Q}^{2\times 2}$ nicht diagonalisierbar. Wir können A aber als reelle Matrix auffassen, und dann können wir mittels pq-Formel zwei reelle Nullstellen λ_1, λ_2 von $\chi_A(x)$ finden:

$$\lambda_{1,2} = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1 \pm \sqrt{5}}{2}.$$

$\lambda_1 = \varphi := \frac{1+\sqrt{5}}{2}$ ist der goldene Schnitt, und wir bezeichnen die andere Nullstelle λ_2 mit φ^*. Es gilt dann also

$$x^2 - x - 1 = (x-\varphi)(x-\varphi^*).$$

Daraus ergeben sich die Rechenregeln

$$\varphi^2 = \varphi + 1, \quad (\varphi^*)^2 = \varphi^* + 1 \quad \text{und} \quad \varphi\varphi^* = \varphi^*\varphi = -1. \tag{4.5.6}$$

Letzteres besagt, dass $\varphi^* = -\varphi^{-1}$. Mittels dieser Rechenregeln bestimmt man nun leicht die Eigenräume von A: Der Eigenraum zu $\lambda_1 = \varphi$ ist gegeben als Kern der Matrizen

$$\begin{pmatrix} \varphi-1 & -1 \\ -1 & \varphi \end{pmatrix} \sim \begin{pmatrix} \varphi^2-\varphi & -\varphi \\ -1 & \varphi \end{pmatrix} = \begin{pmatrix} 1 & -\varphi \\ -1 & \varphi \end{pmatrix} \sim \begin{pmatrix} 1 & -\varphi \\ 0 & 0 \end{pmatrix},$$

der durch den Vektor $\begin{pmatrix} \varphi \\ 1 \end{pmatrix}$ aufgespannt wird. Analog ist der Eigenraum zu $\lambda_2 = \varphi^*$ gegeben als Kern der Matrizen

$$\begin{pmatrix} \varphi^*-1 & -1 \\ -1 & \varphi^* \end{pmatrix} \sim \begin{pmatrix} (\varphi^*)^2-\varphi^* & -\varphi^* \\ -1 & \varphi^* \end{pmatrix} = \begin{pmatrix} 1 & -\varphi^* \\ -1 & \varphi^* \end{pmatrix} \sim \begin{pmatrix} 1 & -\varphi^* \\ 0 & 0 \end{pmatrix},$$

der durch den Vektor $\begin{pmatrix}\varphi^*\\1\end{pmatrix}$ aufgespannt wird. Wir erhalten also

$$A = \begin{pmatrix}\varphi & \varphi^*\\1 & 1\end{pmatrix}\begin{pmatrix}\varphi & 0\\0 & \varphi^*\end{pmatrix}\begin{pmatrix}\varphi & \varphi^*\\1 & 1\end{pmatrix}^{-1}.$$

Weiter gilt

$$\left|\begin{pmatrix}\varphi & \varphi^*\\1 & 1\end{pmatrix}\right| = \varphi - \varphi^* = \sqrt{5} \quad\Longrightarrow\quad \begin{pmatrix}\varphi & \varphi^*\\1 & 1\end{pmatrix}^{-1} = \frac{1}{\sqrt{5}}\begin{pmatrix}1 & -\varphi^*\\-1 & \varphi\end{pmatrix}.$$

Wir erhalten also

$$\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}^n = \frac{1}{\sqrt{5}}\begin{pmatrix}\varphi & \varphi^*\\1 & 1\end{pmatrix}\begin{pmatrix}\varphi^n & 0\\0 & (\varphi^*)^n\end{pmatrix}\begin{pmatrix}1 & -\varphi^*\\-1 & \varphi\end{pmatrix}. \tag{4.5.7}$$

Bemerkung 4.5.22. In Beispiel 3.1.24 haben wir gesehen, dass sich die Rekursionsformel der Fibonacci-Folge (f_n) schreiben lässt als

$$\begin{pmatrix}f_{n+2}\\f_{n+1}\end{pmatrix} = \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}f_{n+1}\\f_n\end{pmatrix}.$$

Es gilt also

$$\begin{pmatrix}f_{n+1}\\f_n\end{pmatrix} = \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}^{n-1}\begin{pmatrix}f_2\\f_1\end{pmatrix} = \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}^{n-1}\begin{pmatrix}1\\1\end{pmatrix}.$$

Aus (4.5.7) folgt nun, dass

$$\begin{aligned}\begin{pmatrix}f_{n+1}\\f_n\end{pmatrix} &= \frac{1}{\sqrt{5}}\begin{pmatrix}\varphi & \varphi^*\\1 & 1\end{pmatrix}\begin{pmatrix}\varphi^{n-1} & 0\\0 & (\varphi^*)^{n-1}\end{pmatrix}\begin{pmatrix}1 & -\varphi^*\\-1 & \varphi\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}\\ &= \frac{1}{\sqrt{5}}\begin{pmatrix}\varphi^{n+1}-(\varphi^*)^{n+1}\\ \varphi^n-(\varphi^*)^n\end{pmatrix}\end{aligned}$$

Dies ist genau die Formel von de Moivre-Binet! (Sie haben also in Übung 3.1.25 ohne es zu merken eine Matrix diagonalisiert.)

Bemerkung 4.5.23 (Lineare Rekursionsgleichungen)**.** Die Fibonacci-Folge ist ein Beispiel für eine rekursiv definierte Folge. Solche Folgen spielen in der Informatik und Kombinatorik eine zentrale Rolle. Allgemeiner betrachtet man Folgen $(a_n) \in \mathbb{K}^{\mathbb{N}}$, die durch eine *lineare Rekursionsgleichung* der Form

$$a_{n+k} = \alpha_1 a_{n+k-1} + \cdots + \alpha_k a_n \quad (\alpha_1,\ldots,\alpha_k \in \mathbb{K})$$

und *Anfangswerte* $a_1 := w_1, \ldots, a_k := w_k$ gegeben sind. Setzt man

$$v_n := \begin{pmatrix}a_{n+k-1}\\\vdots\\a_n\end{pmatrix} \quad\text{und}\quad A := \begin{pmatrix}\alpha_1 & \ldots & \alpha_{k-1} & \alpha_k\\1 & & 0 & 0\\ & \ddots & & \vdots\\0 & & 1 & 0\end{pmatrix},$$

so gilt $v_{n+1} = Av_n$, und daher

$$\begin{pmatrix}a_{n+k-1}\\\vdots\\a_n\end{pmatrix} = A^{n-1}\begin{pmatrix}w_k\\\vdots\\w_1\end{pmatrix}.$$

Falls A diagonalisierbar ist, so kann man daraus wie im Fall der Fibonacci-Folge eine geschlossene Formel für a_n herleiten.

Beispiel 4.5.24 (Eine Markov-Kette)**.** Sheldon isst in der Mensa immer entweder bei der Linie 1 oder bei der Linie 2. Er mag Abwechslung, bevorzugt die Linie 1, möchte aber auch die Linie 2 nicht missen. Um nicht jeden Tag neu darüber nachdenken zu müssen, an welcher Linie er sich anstellt, hat er sich den folgenden ausgeklügelten Algorithmus ausgedacht. Nach jeder Mahlzeit würfelt er mit einem fairen sechsseitigen Würfel und legt dadurch fest, bei welcher Linie er beim nächsten Mal isst:

- Am ersten Tag stellt er sich an der Linie 1 an.
- Hat er gerade an der Linie 1 gegessen, so isst er morgen auch in der Linie 1, falls er eine 1,2 oder 3 würfelt, sonst wechselt er zur Linie 2.
- Hat er gerade an der Linie 2 gegessen, so isst er morgen auch in der Linie 2, falls er eine 1 oder 2 würfelt, sonst wechselt er zur Linie 1.

An welcher Linie wird er wohl seine 100. Mahlzeit einnehmen? Es sei $p_1(n)$ die Wahrscheinlichkeit, dass Sheldon seine $n$te Mahlzeit in der Linie 1 einnimmt und $p_2(n)$ die Wahrscheinlichkeit, dass Sheldon seine $n$te Mahlzeit in der Linie 2 einnimmt. Es gilt dann $p_1(1) = 1$, $p_2(1) = 0$, sowie

$$p_1(n+1) = \frac{1}{2}p_1(n) + \frac{2}{3}p_2(n) \quad \text{und} \quad p_2(n+1) = \frac{1}{2}p_1(n) + \frac{1}{3}p_2(n).$$

Wir können dies In Matrix-Vektor-Schreibweise schreiben:

$$\begin{pmatrix} p_1(n+1) \\ p_2(n+1) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{2}{3} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} p_1(n) \\ p_2(n) \end{pmatrix}.$$

Daraus erhalten wir

$$\begin{pmatrix} p_1(n) \\ p_2(n) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{2}{3} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix}^{n-1} \begin{pmatrix} p_1(1) \\ p_2(1) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{2}{3} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Um die Wahrscheinlichkeiten $p_1(n)$ und $p_2(n)$ für beliebige n zu berechnen, müssen wir die Matrix

$$A := \begin{pmatrix} \frac{1}{2} & \frac{2}{3} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix} = \frac{1}{6}\begin{pmatrix} 3 & 4 \\ 3 & 2 \end{pmatrix}$$

diagonalisieren. Die charakteristische Polynomfunktion zu A lautet

$$\begin{aligned} \chi_A(x) &= \left| \frac{1}{6}\begin{pmatrix} 6x-3 & -4 \\ -3 & 6x-2 \end{pmatrix} \right| = \frac{1}{36}((6x-3)(6x-2)-12) = \frac{1}{36}(36x^2 - 30x + 6 - 12) \\ &= \frac{1}{6}(6x^2 - 5x - 1) = \frac{1}{6}(x-1)(6x+1). \end{aligned}$$

Die Eigenwerte sind also $\lambda_1 = 1$ und $\lambda_2 = -\frac{1}{6}$. Der Eigenraum V_1 zu λ_1 ist der Kern der Matrizen

$$\frac{1}{6}\begin{pmatrix} 3 & -4 \\ -3 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & -4 \\ -3 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & -4 \\ 0 & 0 \end{pmatrix}.$$

Ein möglicher Eigenvektor ist also $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$. Der Eigenraum $V_{-\frac{1}{6}}$ zu λ_2 ist der Kern der Matrizen

$$\frac{1}{6}\begin{pmatrix} -4 & -4 \\ -3 & -3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -4 & -4 \\ -3 & -3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Ein möglicher Eigenvektor ist also $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Wir erhalten damit

$$A = \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -\frac{1}{6} \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix}^{-1}.$$

Nach der Cramerschen Regel gilt

$$\begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix}^{-1} = \frac{1}{7} \begin{pmatrix} 1 & 1 \\ 3 & -4 \end{pmatrix},$$

also

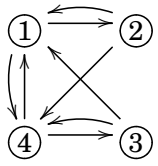
$$A^n = \frac{1}{7} \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-\frac{1}{6})^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 3 & -4 \end{pmatrix}.$$

Damit gilt insbesondere

$$\begin{aligned} \begin{pmatrix} p_1(n) \\ p_2(n) \end{pmatrix} &= \frac{1}{7} \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-\frac{1}{6})^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 3 & -4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{7} \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-\frac{1}{6})^n \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 4 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \cdot (-\frac{1}{6})^n \end{pmatrix} \\ &= \begin{pmatrix} \frac{4}{7} + \frac{3}{7}(-\frac{1}{6})^n \\ \frac{3}{7} - \frac{3}{7}(-\frac{1}{6})^n \end{pmatrix} \xrightarrow{n \to \infty} \begin{pmatrix} \frac{4}{7} \\ \frac{3}{7}, \end{pmatrix} \end{aligned}$$

wobei die Konvergenz sehr schnell (exponentiell!) ist. Langfristig gesehen wird Sheldon also in etwa 4 von 7 Tagen an der Linie 1 anstehen.

Beispiel 4.5.25 (Pfadproblem)**.** Wir kehren abschließend noch einmal zum Pfadproblem des Graphen



aus Beispiel 3.1.23 zurück. Wir wissen bereits: Bezeichnet $a_{ij}^{(n)}$ die Menge der Pfade der Länge n von der $i$ten zur $j$ten Ecke, so gilt $(a_{ij}^{(n)}) = A^n$, wobei A die Adjazenzmatrix

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

ist. Um das Pfadproblem zu lösen, diagonalisieren wir die Matrix A. Das charakteristische

Polynom ist

$$\begin{aligned}
\chi_A(X) &= \left|\begin{pmatrix} X & -1 & 0 & -1 \\ -1 & X & 0 & -1 \\ -1 & 0 & X & -1 \\ -1 & 0 & -1 & X \end{pmatrix}\right| = \left|\begin{pmatrix} -1 & 0 & -1 \\ -1 & X & -1 \\ -1 & -1 & X \end{pmatrix}\right| + X \cdot \left|\begin{pmatrix} X & 0 & -1 \\ -1 & X & -1 \\ -1 & -1 & X \end{pmatrix}\right| \\
&= \left|\begin{pmatrix} -1 & 0 & 0 \\ -1 & X & 0 \\ -1 & -1 & X+1 \end{pmatrix}\right| + X \cdot (X^3 + 0 + (-1) - X - X - 0) \\
&= X \cdot (-X-1) + X \cdot (X^3 - 2X - 1) = X \cdot (X^3 - 3X - 2) \\
&= X(X-2)(X+1)^2.
\end{aligned}$$

Die Eigenwerte sind also $\lambda_1 = -1$, $\lambda_2 = 0$ und $\lambda_3 = 2$. Der Eigenraum zu $\lambda_1 = -1$ ist der Kern der Matrizen

$$\begin{pmatrix} -1 & -1 & 0 & -1 \\ -1 & -1 & 0 & -1 \\ -1 & 0 & -1 & -1 \\ -1 & 0 & -1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

also

$$V_{\lambda_1} = \left\langle \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

Analog rechnet man

$$V_{\lambda_2} = \left\langle \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix} \right\rangle \quad \text{und} \quad V_{\lambda_3} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle.$$

Wir erhalten also

$$A = S \cdot \operatorname{diag}(-1,-1,0,2) \cdot S^{-1}, \quad \text{mit } S := \begin{pmatrix} -1 & -1 & -1 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Invertieren liefert

$$S^{-1} = \frac{1}{6} \begin{pmatrix} -2 & 2 & -4 & 4 \\ -2 & 2 & 2 & -2 \\ 0 & -3 & 3 & 0 \\ 2 & 1 & 1 & 2 \end{pmatrix}.$$

Wir erhalten daher

$$A^n = S \cdot \operatorname{diag}((-1)^n,(-1)^n,0,2^n) \cdot S^{-1} = \frac{1}{6} \begin{pmatrix} -(-1)^n & -(-1)^n & 0 & 2^n \\ 0 & (-1)^n & 0 & 2^n \\ 0 & (-1)^n & 0 & 2^n \\ (-1)^n & 0 & 0 & 2^n \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 & -4 & 4 \\ -2 & 2 & 2 & -2 \\ 0 & -3 & 3 & 0 \\ 2 & 1 & 1 & 2 \end{pmatrix}.$$

Die Anzahl Pfade der Länge n vom 2ten zum 3ten Knoten ist also

$$a_{23}^{(n)} = \frac{1}{6}(2 \cdot (-1)^n + 2^n).$$

Lassen wir n variieren, so erhalten wir

$$0,1,1,3,5,11,36,43\ldots,$$

und von da an steigt die Anzahl der Pfade rapide an, denn $\frac{a_{23}^{(n)}}{2^n} \to \frac{1}{6}$.

Das Diagonalisieren von Matrizen ist in vielen weiteren Zusammenhängen nützlich. In der Analysis werden Sie z.B. eine Anwendung im Zusammenhang mit linearen gewöhlichen Differentialgleichungen mit konstanten Koeffizienten sehen.

Zusammenfassung von Abschnitt 4.5

(1) Ein Endomorphismus Φ eines endlich-dimensionalen Vektorraums V ist genau dann diagonalisierbar, wenn V eine Basis aus Eigenvektoren von Φ besetzt.

(2) Die Eigenwerte eines Endomorphismus sind genau die Nullstellen der charakteristischen Polynomfunktion. Die Eigenvektoren zu einem gegebenen Eigenwert lassen sich durch Lösen eines LGS bestimmen. Dies liefert einen praktischen Algorithmus zur Diagonalisierung diagonalisierbarer Endomorphismen.

(3) Der Diagonalisierungsalgorithmus hat vielfältige Anwendungen, u.a. zum Bestimmen der Potenzen einer Matrix und daher bei der Lösung des Pfadproblems in Graphen, dem Berechnen von Markov-Ketten und der Lösung linearer Rekursionsgleichungen.

Weihnachtspause!

5 Algebraische Strukturen

[10.01.24]

5.1 Universelle Algebra

Bemerkung 5.1.1 (Historische Bemerkung)**.** Das Wort „Algebra“ ist eine Latinisierung des arabischen Worts „Al-Jabr“ (dt. ungefähr „Zusammenfügen gebrochener Teile“). Im mathematischen Kontext taucht das Wort erstmals um 825 n. Chr. im Titel des Buches „Al-Kitab al-muhtasar fi hisab al-jabr wa-muqabala“ (dt. ungefähr „Das kurz gefasste Buch über die Rechenverfahren durch Ergänzen und Ausgleichen“) von al-Chwarizmi[1], dessen latinisierter Name Algorismi noch heute synonym für Rechenverfahren steht. Zu Beginn der Neuzeit war „Algebra“ also quasi ein Synonym für die Anwendung systematischer („algorithmischer“) Rechenverfahren zur Lösung von Gleichungen. Wenn man die heutige Algebra betrachtet, so ist davon auf den ersten Blick scheinbar nicht viel übrig geblieben.

Unsere heutige Vorstellung von dem, was Algebra ist, wurde maßgeblich geprägt durch van der Waerdens[2] Lehrbuch „Moderne Algebra“ aus dem Jahr 1930, in dem er, basierend auf Vorlesungen seiner Lehrer Emil Artin[3] und Emmy Noether[4] in Göttingen quasi einen modernen Kanon der Algebra (auf Basis der Linearen Algebra und der damals neuen abstrakten Mengenlehre) erstellte. Vereinfacht ausgedrückt[5] ist für van der Waerden Algebra das Studium algebraischer Strukturen wie „Gruppen“, „Ringe“, „Körper“, „Vektorräume“ und eben „Algebren“.

Wenn man van der Waerdens Algebra-Buch aufschlägt, dann findet man dort in den ersten Kapiteln kaum etwas, was an die ursprünglichen „algorithmischen“ Wurzeln der Algebra erinnert, und überhaupt schweigt sich der Autor lange darüber aus, *warum* man abstrakte algebraische Strukturen studieren sollte. Das ist z.T. dem Zeitgeist geschuldet (der heutzutage wieder mehr in die algorithmische Richtung weht), aber es hat auch seine Berechtigung: Einerseits wurde es im Laufe des 19. Jahrhunderts in der Beschäftigung mit konkreten geometrischen und zahlentheoretischen Problemen wie dem notorischen Fermat-Problem immer klarer, dass ohne ein tiefes Verständnis algebraischer Strukturen keine weiteren Fortschritte möglich waren. Andererseits erlaubte die abstraktere Sichtweise, klassische Resultate auf neue Situtationen zu verallgemeinern.

[1] Muhammad ibn Musa al-Chwarizmi (ca. 780-850), arabischer Universalgelehrter, dem wir u.a. das moderne Dezimalsystem und die Zahl 0 zu verdanken hatten, die dieser aus älteren indischen Quellen übernahm und durch seine Bücher dem Rest der Welt zugänglich machte

[2] Bartel Leendert van der Waerden (1903-1996), niederl. Mathematiker und Professor in Leipzig

[3] Emil Artin (1898 –1962), österreichischer Mathematiker und bedeutender Algebraiker, der auf der Flucht vor den Nazis in die USA emigrierte

[4] Emmy Noether (1882-1935), dt. Mathematikerin, die sich trotz doppelter Diskriminierung als Frau und Jüdin internationale Anerkennung als die wichtigste Vertreterin der modernen abstrakten Algebra erlangte, bevor sie kurz nach ihrer erzwungenen Emigration in die USA verstarb

[5] Van der Waerden war sich der Probleme seines Zugangs durchaus bewusst, ich tue ihm mit dieser Vereinfachung also wohl ein Unrecht.

Van der Waerden sieht den Wandel der modernen Algebra weg von den Algorithmen zu den abstrakten Strukturen als eine notwenige Antwort auf eine Stagnationskrise der Mathematik; im Vorwort seines Buches schreibt er: *„Die „abstrakte“ „formale“ oder „axiomatische“ Richtung, der die Algebra ihren erneuten Aufschwung verdankt, hat [...] zu einer Reihe von neuartigen Begriffsbildungen, zur Einsicht in neue Zusammenhänge und zu weitreichenden Resultaten geführt.“*

In der Linearen Algebra brauchen wir abstrakte Algebra aus zwei Gründen: Einerseits, um gewisse schwierige Probleme, wie etwa das Normalformenproblem für Endomorphismen behandeln zu können, und andererseits um neue Anwendungsbeispiele für unsere bisherigen Ergebnisse zu finden.

Was ist nun eine algebraische Struktur? Dazu schauen wir uns zunächst einige Beispiele an:

Beispiel 5.1.2 (Reelle Zahlen)**.** Auf der Menge $\mathbb{R}$ der reellen Zahlen sind eine Addition und eine Multiplikation

$$A : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (x,y) \mapsto x+y \quad \text{und} \quad M : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (x,y) \mapsto xy$$

definiert. Diese erfüllen gewisse Rechengesetze (Assoziativgesetze, Kommutativgesetze, Distributivgesetze). Daneben gibt es zwei ausgezeichnete Elemente 0 und 1, und es gibt Abbildungen

$$\mathbb{R} \to \mathbb{R},\ x \mapsto -x \quad \text{und} \quad \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\},\ x \mapsto x^{-1},$$

die wiederum gewissen Gesetzen (z.B. $xx^{-1} = 1$) genügen.

Beispiel 5.1.3 (Boolesche Algebra über einer Menge)**.** Ist M eine beliebige Menge, so können wir auf der Potenzmenge $\mathscr{P}(M)$ den Schnitt und die Vereinigung

$$\cap : \mathscr{P}(M) \times \mathscr{P}(M) \to \mathscr{P}(M),\ (A,B) \mapsto A \cap B \quad \cup : \mathscr{P}(M) \times \mathscr{P}(M) \to \mathscr{P}(M),\ (A,B) \mapsto A \cup B$$

definieren. Wieder gelten Assoziativgesetze, Kommutativgesetze und Distributivgesetze. Wir haben zwei ausgezeichnete Elemente $\emptyset$ und M und eine Abbildung

$$\mathscr{P}(M) \to \mathscr{P}(M),\ A \mapsto A^c := M \setminus A,$$

die wiederum gewissen Gesetzen genügen (z.B. $A \cap A^c = \emptyset$ und $A \cup A^c = M$).

Beispiel 5.1.4 (Symmetriegruppe des n-Ecks)**.** Es sei D_{2n} die Menge der Drehungen und Spiegelungen der Ebene (inklusive der identischen Abbildung), die ein regelmäßiges n-Eck auf sich selbst abbilden. Für $n = 4$ sind das genau die vier Spiegelungen an den beiden Mittelsenkrechten der Seiten und den beiden Diagonalen und die vier Drehungen um Vielfache von $\pi/2$. Diese 8-elementige Menge D_8 ist abgeschlossen unter Verkettung von Abbildungen, wir erhalten also eine Verknüpfung

$$D_8 \times D_8 \to D_8, \quad (\Phi, \Psi) \mapsto \Phi \circ \Psi.$$

Diese ist assoziativ, aber nicht kommutativ. Es gibt ein ausgezeichnetes Element (die Identität Id), und eine Abbildung $D_8 \to D_8$, $\Phi \mapsto \Phi^{-1}$, wobei wieder $\Phi \circ \Phi^{-1} = \mathrm{Id}$ gilt.

Definition 5.1.5. Seien M, N Mengen, $\Phi : M \to N$ eine Abbildung und $k \in \mathbb{N}$.

(i) Eine *k-stellige Verknüpfung* auf M ist eine Abbildung

$$M^k := \underbrace{M \times \cdots \times M}_{k \text{ Faktoren}} \to M$$

(ii) Eine 0-*stellige Verknüpfung* ist nach Definition eine Abbildung $M^0 := \{\emptyset\} \to M$. Wir können eine solche Verknüpfung mit einem Element von M (dem Bild von $\emptyset$) identifizieren.

(iii) $(M, V_1, \ldots, V_n)$ heißt eine *abstrakte Algebra vom Typ* $(\tau_1, \ldots, \tau_n)$, falls V_j eine τ_j-stellige Verknüpfung ist.

(iv) Sind $\mathscr{M} = (M, V_1, \ldots, V_n)$ und $\mathscr{N} = (N, W_1, \ldots, W_n)$ zwei abstrakte Algebren vom selben Typ $(\tau_1, \ldots, \tau_n)$, so heißt Φ ein *Morphismus* von $\mathscr{M}$ nach $\mathscr{N}$, falls

$$\Phi(V_j(m_1, \ldots, m_{\tau_j})) = W_j(\Phi(m_1), \ldots, \Phi(m_{\tau_j})) \quad \text{für alle } j \in \{1, \ldots, n\}, m_1, \ldots, m_{\tau_j} \in M$$

gilt. Ist Φ injektiv (bzw. surjektiv, bijektiv), so heißt Φ ein *Monomorphismus* (bzw. *Epimorphismus, Isomorphismus*). Ist $\mathscr{M} = \mathscr{N}$ (und Φ bijektiv), so heißt Φ ein *Endomorphismus* (bzw. *Automorphismus*).

(v) Zwei abstrakte Algebren heißen *isomorph*[6], wenn sie vom gleichen Typ sind und es einen Isomorphismus zwischen ihnen gibt.

Beispiel 5.1.6. Die rellen Zahlen sind eine abstrakte Algebra vom Typ (2,2,1,1,0,0) (wenn man die Abbildung $x \mapsto x^{-1}$ durch $0 \mapsto 0$ auf ganz $\mathbb{R}$ fortsetzt), die Boolesche Algebra über M sit eine abstrakte Algebra vom Typ (2,2,1,0,0) und die Symmetriegruppe des n-Ecks ist eine abstrakte Algebra vom Type (2,1,0).

Bemerkung 5.1.7 (Algebren über Algebren)**.** $\mathbb{R}$-Vektorräume sind keine abstrakten Algebren, weil wir nicht nur eine Abbildung $V \times V \to V$, sondern auch eine Abbildung $\mathbb{R} \times V \to V$ als Teil der Struktur haben. Man muss also die obigen Definitionen noch etwas verallgemeinern: Sind K und M Mengen, so nennen wir eine Abbildung $K \times M \to M$ eine *Wirkung* von K auf M. Allgemeiner kann man Abbildungen der Form

$$K \times \cdots \times K \times M \times \cdots \times M \to M,$$

sogenannte *äußere Verknüpfungen* über K, betrachten. Ist $\mathscr{K} = (K, V_1, \ldots, V_m)$ eine abstrakte Algebra, so nennen wir eine Menge M zusammen mit Verknüpfungen und äusseren Verknüpfungen über K, eine *abstrakte $\mathscr{K}$-Algebra*. Ein $\mathbb{R}$-Vektorraum ist dann eine abstrakte $\mathbb{R}$-Algebra. Morphismen und Isomorphie kann man dann in der offensichtlichen Weise definieren.

Bemerkung 5.1.8 (Welche Axiomensysteme?)**.** Nach van der Waerden ist die Algebra das Studium abstrakter Algebren (ggf. über anderen Algebren) und ihrer Morphismen. Natürlich betrachtet man nicht beliebige abstrakte Algebren, sondern solche, die ein System sinnvoller Axiome (wie z.B. Assoziativgesetze) erfüllen. Nicht für jedes Axiomensystem gibt es Beispiele, die dieses System erfüllen, und selbst wenn es Beispiele gibt, müssen diese noch lange nicht von Interesse sein. Historisch hat es viele hundert Jahre gedauert, bis man z.B. ein gutes Axiomensystem gefunden hat, das Symmetriegruppen beschreibt. Aus Zeitgründen überspringen wir diese Jahrhunderte und geben Ihnen einfach einige der Axiomensysteme an, für die sich heutige Mathematiker am meisten interessieren. Sie sollten sich aber klar machen, dass diese Axiomensysteme nicht vom Himmel gefallen sind, sondern das Ergebnis eines langen Abstraktionsprozesses, der immer von konkreten Beispielen ausgeht.

[6] Dies ist ein Spezialfall von Definition 1.5.2, da abstrakte Algebren von festem Typ und ihre Morphismen eine Kategorie bilden.

Zusammenfassung von Abschnitt 5.1

(1) Die Algebra ist ursprünglich aus der algorithmischen Behandlung von Gleichungen entstanden.

(2) Die moderne Algebra studiert abstrakte algebraische Strukturen und strukturerhaltende Abbildungen (Morphismen) zwischen solchen Strukturen.

(3) Typische algebraische Strukturen sind Mengen mit Verknüpfungen (sogenannte abstrakte Algebren), die gewisse Axiome (z.B. Assoziativität) erfüllen.

5.2 Gruppen und ihre Wirkungen

In diesem Abschnitt betrachten wir Axiomensystem für abstrakte Algebren mit einer einzigen 2-stelligen Verknüpfung. Ziel ist der Begriff der Gruppe, eine Abstraktion des Symmetriebegriffs. Wir beginnen allerdings mit einigen schwächeren Axiomensystemen.

Definition 5.2.1. Sei G eine Menge und $\mu : G \times G \to G$, $(x,y) \mapsto x * y$ eine Verknüpfung.

(i) (G,μ) heißt *Halbgruppe*, falls das Assoziativgesetz gilt: $\forall\, x,y,z \in G : (x*y)*z = x*(y*z)$.

(ii) Eine Halbgruppe heißt *abelsch*[7] (oder *kommutativ*), falls $\forall\, x,y \in G : xy = yx$.

Das Verknüpfungssymbol $*$ wird häufig durch ein anderes Symbol ersetzt, z.B. $\cdot$, $\times$, $\otimes$, $+$, $\barwedge$, $\wedge$, $\vee$, $\cap$, $\cup$. Manchmal lässt man das Symbol auch ganz weg und schreibt einfach xy statt $x*y$. Wenn mehrere Halbgruppen im Spiel sind, dann sollte man die Verknüpfungen eigentlich klar unterscheiden, also z.B. $x *_G y$ und $x' *_H y'$ für die Multiplikation in den Halbgruppen G und H schreiben. In der Praxis ist man aber häufig faul und schreibt einfach xy und $x'y'$ und überlässt dem Leser die Deutung. Ab jetzt sei (G,μ) eine Halbgruppe.

Definition 5.2.2. Ein Element $e \in G$ heißt *linksneutral* (bzw. *rechtsneutral*), falls $ex = x$ (bzw. $xe = x$) für alle $x \in G$ gilt. Es heißt *neutral*, falls e sowohl linksneutral als auch rechtsneutral ist.

Ist $e \in G$ neutral, so heißt die abstrakte Algebra (G,μ,e) vom Typ (2,0) ein *Monoid*.

Bemerkung 5.2.3 (Eindeutigkeit)**.** Eine Halbgruppe kann beliebig viele linksneutrale[8] oder rechtsneutrale Elemente besitzen, aber sie besitzt immer höchstens ein neutrales Element. Allgemeiner gilt nämlich, ist e_1 linksneutral und e_2 rechtsneutral, so gilt $e_1 = e_1 e_2 = e_2$. Das Monoid (G,μ,e) ist also durch die Halbgruppe (G,μ) schon eindeutig bestimmt.

Beispiel 5.2.4 (Monoide)**.** Wir haben in dieser Vorlesung schon einen reichen Vorrat an Beispielen für Monoide gesehen:

(i) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ sind abelsche Monoide mit neutralem Element 0, und $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$ sind abelsche Monoide mit neutralem Element 1. Ist V ein Vektorraum, so ist $(V,+)$ ein abelsches Monoid.

[7] nach Niels Henrik Abel (1802-1829), einem norwegischen Mathematiker und Mitbegründer der modernen Gruppentheorie, der mit nur 26 Jahren an Tuberkulose starb

[8] Es sei M die Menge der Funktionen $f : \mathbb{N} \to \mathbb{N}$, mit $1 \notin \mathrm{Bild}(f)$. Diese bilden eine Halbgruppe unter Verkettung, und jede Funktion f mit $f|_{\{2,3,\ldots\}} = \mathrm{Id}_{\{2,3,\ldots\}}$ ist ein linksneutrales Element.

(ii) Es sei M eine Menge und $\mathrm{Abb}(M,M)$ die Menge der Abbildungen von M nach M. Dann ist $(\mathrm{Abb}(M,M),\circ,\mathrm{Id}_M)$ ein Monoid. Ist $|M|\geq 2$, so ist dieses Monoid nicht-abelsch.

(iii) Ist V ein $\mathbb{R}$-Vektorraum, so ist $(\mathrm{End}_{\mathbb{R}}(V),\circ,\mathrm{Id}_V)$ ein (meist nicht-abelscher) Monoid. Analog ist $(\mathbb{R}^{p\times p},\cdot,\mathbf{1})$ ein Monoid, und ist $\mathscr{B}$ eine endliche geordnete Basis von V mit $|\mathscr{B}|=p$, so ist die Abbildung

$$\mathrm{End}_{\mathbb{R}}(V)\to\mathbb{R}^{p\times p},\quad \Phi\mapsto D_{\mathscr{B}}(\Phi)$$

ein Isomorphismus von Monoiden.

(iv) Allgemeiner bilden die Endomorphismen einer abstrakten Algebra ein Monoid bzgl. Verkettung.

Der Begriff eines Monoids ist sehr allgemein. Gruppen sind spezielle Monoide, die Symmetrien modellieren sollen. Eine Symmetrie ist grob gesagt eine Abbildung eines Objekts in sich, die alle relevante Struktur erhält, und keine vorhandene Struktur zerstört. Letzteres bedeutet insbesondere, dass solche Symmetrien umkehrbar sein sollen. Dies wird durch die Forderung nach einem Inversen modelliert.

Definition 5.2.5. Sei (G,μ,e) ein Monoid. Sind $x,y\in G$ mit $xy=e$, so heißt x ein *Linksinverses* zu y und y ein *Rechtsinverses* zu x. Ein Links- und Rechtsinverses heißt ein *Inverses*.

Ist (G,μ,e) ein Monoid und $\iota:G\to G$, so dass $\iota(g)$ ein Inverses zu g ist, so heißt (G,μ,ι,e) eine *Gruppe*.

Statt *„(G,μ,ι,e) ist eine Gruppe."* sagen wir oft auch schlampig *„G ist eine Gruppe."* Das ist kürzer, kann allerdings manchmal zu Verwechslungen führen, insbesondere wenn auf einer Menge mehrere Verknüpfungen definiert sind.

Bemerkung 5.2.6 (Eindeutigkeit von Inversen)**.** Jedes Element x eines Monoids hat höchstens ein Inverses. Allgemeiner gilt: Ist y ein Linksinverses von x und z ein Rechtsinverses von x, so ist

$$y=ye=y(xz)=(yx)z=ez=z.$$

Eine Gruppe (G,μ,ι,e) ist also durch die Halbgruppe (G,μ) (die sogenannte *zugrundeliegende Halbgruppe*) schon eindeutig bestimmt.

Man bezeichnet das eindeutige Inverse eines Elements x in einem Monoid - wenn es denn existiert - häufig[9] mit x^{-1}. In einer Gruppe ist jedes Linksinverse automatisch ein Rechtsinverses und daher das eindeutige Inverses, denn ist $xy=e$, so gilt

$$x=x(yy^{-1})=(xy)y^{-1}=y^{-1}.$$

Übung 5.2.7. Zeigen Sie: Eine Halbgruppe (G,μ) ist genau dann die unterliegende Halbgruppe einer Gruppe, wenn G ein linksneutrales Element e besitzt und jedes Element von G ein Linksinverses bzgl. e besitzt. Gilt dies auch, wenn man in diesem Satz Linksinverses durch Rechtsinverses ersetzt?

Um Beispiele für Gruppen zu geben, können wir wie folgt vorgehen:

[9] In $(\mathbb{Z},+,e)$ schreibt man aber natürlich weiterhin $-n$ für das Inverse von n...

Konstruktion 5.2.8 (Einheitengruppen)**.** Sei (M, μ, e) ein Monoid; wir definieren

$$M^\times := \{x \in M \mid x \text{ hat ein Inverses}\}.$$

Sind $x, y \in M^\times$, so gilt

$$(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = y^{-1}y = e \implies xy \in M^\times.$$

Ausserdem gilt $xx^{-1} = e$, also ist $x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$. Folglich ist $(M^\times, \mu|_{M^\times \times M^\times}, (-)^{-1}, e)$ eine Gruppe. Diese heißt die *Einheitengruppe* von M.

Beispiel 5.2.9. Wir bestimmen die Einheitengruppen der Monoide aus Beispiel 5.2.4

(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(V, +)$ (für einen Vektorraum V) sind schon selbst abelsche Gruppen. $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ sind dagegen lediglich (abelsche) Monoide, und die zugehörigen Einheitengruppen sind

$$\mathbb{Z}^\times := \{-1, 1\}, \quad \mathbb{Q}^\times := \mathbb{Q} \setminus \{0\} \quad \text{und} \quad \mathbb{R}^\times := \mathbb{R} \setminus \{0\}.$$

(ii) Für jede Menge M ist die Einheitengruppe von $(\mathrm{Abb}(M, M), \circ)$ gegeben durch

$$\mathrm{Sym}(M) := \{f : M \to M \mid f \text{ bijektiv}\},$$

denn eine Funktion hat genau dann eine Umkehrfunktion, wenn sie bijektiv ist. Die Elemente von $\mathrm{Sym}(M)$ heißen *Permutationen* oder *Symmetrien* von M, und $(\mathrm{Sym}(M), \circ, (-)^{-1}, \mathrm{Id})$ heißt die *symmetrische Gruppe* über M.

(iii) Ist V ein $\mathbb{R}$-Vektorraum, so heißt die Einheitengruppe von $\mathrm{End}_\mathbb{R}(V)$ die *allgemeine lineare Gruppe*[10] von V und ist gegeben durch

$$\mathrm{GL}_\mathbb{R}(V) := \{\Phi \in \mathrm{End}_\mathbb{R}(V) \mid \Phi \text{ bijektiv}\}.$$

Für $p \in \mathbb{N}$ heißt analog die Einheitengruppe

$$\mathrm{GL}_p(\mathbb{R}) := \{A \in \mathbb{R}^{p \times p} \mid A \text{ invertierbar}\}$$

von $\mathbb{R}^{p \times p}$ die *p-te allgemeine lineare Gruppe über* $\mathbb{R}$. Ist $\dim_\mathbb{R} V = p$ endlich und ist $\mathrm{End}_\mathbb{R}(V) \to \mathbb{R}^{p \times p}$ ein beliebiger Isomorphismus, so schränkt sich dieser zu einem Gruppenisomorphismus $\mathrm{GL}_\mathbb{R}(V) \to \mathrm{GL}_p(\mathbb{R})$ ein.

(iv) Allgemeiner bilden die Automorphismen einer abstrakten Algebra die Einheitengruppe des Monoids der Endomorphismen. Das ist der Grund dafür, warum Gruppen in der Algebra allgegenwärtig sind: Egal, welche Strukturen man betrachtet, die Automorphismen bilden immer eine Gruppe.

Damit haben wir schon einen gewissen Vorrat an Beispielen. Wir wollen diesen nun noch etwas erweitern.

[10] engl. „general linear group“

Bemerkung 5.2.10 (Untergruppen)**.** Es sei (G,μ,ι,e) eine Gruppe und $A \subseteq G$ eine Teilmenge. Wir nennen A eine *Untergruppe* von G und schreiben $A \leq G$, falls für alle $x,y \in A$ gilt:

$$e \in A, \quad xy \in A \quad \text{und} \quad x^{-1} \in A.$$

In diesem Fall ist $(A,\mu|_{A\times A},\iota|_A,e)$ selbst wieder eine Gruppe. Nach Definition gilt stets $\{e\} \leq G$ und $G \leq G$. Diese heißen die *trivialen Untergruppen*, alle anderen Untergruppen heißen *nicht-trivial*.

Um konkrete Beispiele anzugeben, kann man Gruppenhomomorphismen verwenden:

Bemerkung 5.2.11 (Gruppenhomomorphismen)**.** Seien (G,μ,ι,e) und (H,μ',ι',e') Gruppen. Nach Definition ist eine Abbildung $\Phi : G \to H$ genau dann ein Morphismus, wenn die folgenden Bedingungen erfüllt sind:

(G1) $\Phi(g_1 *_G g_2) = \Phi(g_1) *_H \Phi(g_2)$ für alle $g_1,g_2 \in G$.

(G2) $\Phi(g^{-1}) = \Phi(g)^{-1}$ für alle $g \in G$.

(G3) $\Phi(e) = e'$.

Es stellt sich allerdings heraus, dass (G2) und (G3) schon aus (G1) folgen. Für (G3) rechnet man nach, dass

$$\Phi(e) = \Phi(e *_G e) = \Phi(e) *_H \Phi(e) \implies e' = \Phi(e)^{-1} *_H \Phi(e) = \Phi(e)^{-1} *_H \Phi(e) *_H \Phi(e) = \Phi(e).$$

Ist nun $g \in G$, so folgt aus (G1) und (G3), dass

$$e' = \Phi(e) = \Phi(g^{-1} *_G g) = \Phi(g^{-1})\Phi(g) \implies \Phi(g^{-1}) = \Phi(g)^{-1}.$$

Im Folgenden schreiben wir

$$\mathrm{Hom}(G,H) := \{\Phi : G \to H \mid \forall\, g_1,g_2 \in G :\ \Phi(g_1g_2) = \Phi(g_1)\Phi(g_2)\}$$

und nennen Elemente von $\mathrm{Hom}(G,H)$ *Gruppenhomomorphismen*. Man kann solche Morphismen verketten: Ist $\Phi \in \mathrm{Hom}(G,H)$ und $\Psi \in \mathrm{Hom}(H,K)$, so gilt $\Psi \circ \Phi \in \mathrm{Hom}(G,K)$. Ist Φ bijektiv, so ist auch $\Phi^{-1} \in \mathrm{Hom}(H,G)$ bijektiv. Die Beweise sind wie im Vektorraum-Fall.

Die folgenden Eigenschaften von Gruppenhomomorphismen und Untergruppen sind ganz analog zu den entsprechenden Eigenschaften von linearen Abbildungen und Untervektorräumen, und lassen sich auch genau so beweisen:

Proposition 5.2.12 (Kern und Bild)**.** *Seien G,H Gruppen, $\Phi \in \mathrm{Hom}(G,H)$ und $G' \leq G$ und $H' \leq H$.*

(i) $\Phi[G'] \leq H$ *ist eine Untergruppe. Speziell ist* $\mathrm{Bild}(\Phi) := \Phi[G] \leq H$ *eine Untergruppe.*

(ii) $\Phi^{-1}(H') \leq G$ *ist eine Untergruppe. Speziell ist* $\ker(\Phi) := \Phi^{-1}[e]$ *eine Untergruppe.*

(iii) Φ *ist genau dann injektiv, wenn* $\ker(\Phi) = \{e\}$ *gilt.*

Übung 5.2.13. Beweisen Sie Proposition 5.2.12

Beispiel 5.2.14. Wir geben einige Beispiele für Gruppenhomomorphismen und Untergruppen.

(i) Nach Proposition 4.1.16 ist die Abbildung $\operatorname{sgn} : (\operatorname{Sym}_n, \circ) \to (\{-1,1\}, \cdot)$ für alle $n \geq 2$ ein Epimorphismus. Ihr Kern ist die *alternierende Gruppe*

$$\operatorname{Alt}_n := \{\sigma \in \operatorname{Sym}_n \mid \operatorname{sgn}(\sigma) = 1\} \leq \operatorname{Sym}_n.$$

(ii) Nach Satz 4.3.5 ist die Determinante $\det : (\mathrm{GL}_n(\mathbb{R}), \circ) \to (\mathbb{R}^\times, \cdot)$ ein Epimorphismus. Ihr Kern ist die *spezielle lineare Gruppe* (englisch „special linear group“)

$$\mathrm{SL}_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n} \mid \det(A) = 1\} \leq \mathrm{GL}_n(\mathbb{R}).$$

(iii) Für $n \in \mathbb{N} \cup \{0\}$ ist die Abbildung $\mu_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $k \mapsto nk$ ein Gruppenhomomorphismus; wegen des Distrivbutivgesetzes gilt nämlich

$$\mu_n(k+l) = n(k+l) = nk + nl = \mu_n(k) + \mu_n(l) \quad (k, l \in \mathbb{Z}).$$

Das Bild von μ_n is die Untergruppe $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\} \leq \mathbb{Z}$ der *Vielfachen* von n.

Die in Beispiel 5.2.14 gefundenen Untergruppen von $\mathbb{Z}$ sind bereits *alle* Untergruppen. Zum Beweis benötigen wir das folgende Hilfsmittel:

Bemerkung 5.2.15 (Division mit Rest)**.** Sind $m, n \in \mathbb{Z}$ mit $n \neq 0$, so können wir m durch n mit Rest dividieren: Es existieren $q, r \in \mathbb{Z}$ mit

$$m = q \cdot n + r \quad \text{und} \quad |r| < |n|.$$

Wir können stets $r \geq 0$ wählen; dann ist $r \in \{0, \ldots, n-1\}$ der eindeutige *nicht-negative Rest* von m bei Division durch n.

Lemma 5.2.16. *Jede Untergruppe H von $\mathbb{Z}$ ist von der Form $H = n\mathbb{Z}$ für ein $n \in \mathbb{N} \cup \{0\}$.*

Beweis. Sei $H < \mathbb{Z}$. Ist $H = \{0\} = 0\mathbb{Z}$, so sind wir fertig. Andernfalls sei $h \in H \setminus \{0\}$. Dann ist entweder h oder $-h$ positiv, also $H \cap \mathbb{N} \neq \emptyset$. Sei $n := \min(H \cap \mathbb{N})$ das kleinste positive Element von H; wegen $n \in H$ gilt $n + \cdots + n \in H$, also $kn \in H$ für alle $k > 0$. Da H eine Gruppe ist, gilt dann auch $-kn \in H$ für alle $k > 0$, also $n\mathbb{Z} \subseteq H$. Ist umgekehrt $h \in H$ und ist $r \in \{0, \ldots, n-1\}$ der nicht-negative Rest von h bei Division durch n, so gilt

$$h = kn + r \implies r = h - kn \in H.$$

Es ist also $r \in (H \cap \mathbb{N}) \cup \{0\}$ und $r < n$. Nach Minimalität von n muss daher $r = 0$ gelten. Folglich ist $h = kn \in n\mathbb{Z}$, und daher $H \subseteq n\mathbb{Z}$. □

Nach Beispiel 5.2.9 und Bemerkung 5.2.10 ist jede Untergruppe einer symmetrischen Gruppe eine Gruppe. Wir überlegen nun, wie wir uns solche Gruppen anschaulich vorstellen können.

Bemerkung 5.2.17 (Gruppenwirkung)**.** Es sei G eine Gruppe, M eine Menge und $\operatorname{Sym}(M)$ die zugehörige symmetrische Gruppe. Ist $\rho : G \to \operatorname{Sym}(M)$ ein Gruppenhomomorphismus, so nennen wir das Tripel (G, ρ, M) eine *Permutationsgruppe*. Ist ρ injektiv, so ist G isomorph zur Untergruppe $\rho[G]$ von $\operatorname{Sym}(M)$.

Ist (G, ρ, M) eine Permutationsgruppe, so definieren wir die zugehörige *Permutationswirkung* von G auf M als die Abbildung

$$w_\rho : G \times M \to M, \quad (g, m) \mapsto g.m := \rho(g)(m).$$

Wir stellen uns vor, dass die Elemente von G die Elemente von M „bewegen“: Das Elemente $m \in M$ wird von $g \in G$ auf das Element $g.m \in M$ bewegt. Da ρ ein Gruppenhomomorphismus ist, hat die Abbildung w_ρ die folgenden Eigenschaften:

(W1) $e.m = m$ für alle $m \in M$. (Dies folgt aus $\rho(e) = \mathrm{Id}$ und besagt, dass das Einselement nichts bewegt.)

(W2) $(gh).m = g.(h.m)$. (Dies folgt aus $\rho(gh) = \rho(g)\rho(h)$ und besagt, dass wir das Bild von m unter gh erhalten, indem wir m erst mit h und dann mit g bewegen.)

Man nennt eine Abbildung $w : G \times M \to M$, $(g,m) \mapsto g.m$ mit diesen beiden Eigenschaften eine *Gruppenwirkung* von G auf M. Aus (W1) und (W2), folgt sofort, dass

$$g^{-1}.(g.m) = (g^{-1}g).m = e.m = m,$$

d.h. g^{-1} bewegt $g.m$ auf m zurück.

Permutationsgruppen und Gruppenwirkungen sind äquivalente Konzepte: Ist $w : G \times M \to M$ eine Gruppenwirkung von G auf M, so erhalten wir eine Permutationsgruppe (G, ρ, M), indem wir $\rho(g) \in \mathrm{Sym}(M)$ durch

$$\rho(g)(m) := g.m = w(g,m)$$

definieren, und dann ist w gerade die zu ρ gehörige Permutationswirkung. Rein logisch betrachtet macht es daher keinerlei Unterschied, ob wir über Permutationsgruppen oder über Gruppenwirkungen reden. Psychologisch ist aber die Vorstellung einer „wirkenden“ Gruppe oft besser als die Vorstellung eines abstrakten Gruppenhomomorphismus in eine symmetrische Gruppe.

Beispiel 5.2.18 (Symmetriegruppe des n-Ecks)**.** Die Gruppe D_{2n} aus Beispiel 5.1.4 wirkt auf der Menge M der Ecken des regelmäßigen n-Ecks durch $\Phi.x := \Phi(x)$. In diesem Beispiel können wir uns gut anschaulich vorstellen, wie die Elemente von D_{2n} die Ecken hin und her bewegen.

Beispiel 5.2.19. Jede Gruppe besitzt mindestens eine interessante[11] Gruppenwirkung, nämlich die sogenannte *Linksmultiplikationswirkung*. Die zugrundeliegende Menge ist $M := G$ und wir setzen $g.h := gh$. (W1) gilt dann nach Definition des neutralen Elements und (W2) gilt wegen der Assoziativität der Multiplikation. Wir erhalten daraus einen Gruppenhomomorphismus $\rho : G \to \mathrm{Sym}(G)$ mit $\rho(g)(h) = gh$. Dieser ist injektiv, denn ist $g \in \ker(\rho)$, so ist $gh = h$ für alle $h \in G$ und daher $g = e$. Damit haben wir den folgenden Satz bewiesen.

Satz 5.2.20 (Satz von Cayley [12])**.** *Jede Gruppe G ist isomorph zu einer Untergruppe von* $\mathrm{Sym}(G)$. *Insbesondere ist jede endliche Gruppe isomorph zu einer Untergruppe von* Sym_n *für ein* $n \in \mathbb{N}$. □

Bis auf Isomorphie sind abstrakte, axiomatisch definierte (endliche) Gruppen also nichts anderes als Permutationsgruppen, die die Punkte einer (endlichen) Menge M hin und her bewegen.

[11] Natürlich wirkt jede Gruppe G auf $M := \{\emptyset\}$ durch $g.\emptyset := \emptyset$ für alle $g \in G$, aber das ist nicht interessant.

[12] Arthur Cayley, 1821-1895, englischer Mathematiker und einer der Väter des abstrakten Gruppenbegriffs; den obigen Satz bewies er, um seine Kollegen davon zu überzeugen, dass die von ihm axiomatisch definierten abstrakten (endlichen) Gruppen nicht schlimmer sind als die schon zuvor von Galois, Abel und anderen untersuchten (endlichen) Permutationsgruppen.

[12.01.24]

Beispiel 5.2.21. Es gibt noch weitere interessante Wirkungen einer Gruppe G auf der Menge $M := G$, nämlich die *Rechtsmultiplikationswirkung* und die *Konjugationswirkung*, gegeben durch

$$g.h := hg^{-1} \quad \text{bzw.} \quad g.h := ghg^{-1}.$$

Letztere wird uns im Folgenden noch öfters begegnen. Die Inversen sind hier nötig, damit (W2) gilt.

Bemerkung 5.2.22 (Quotientenmenge)**.** Eine wichtige Konstruktion in der Linearen Algebra sind Quotientenvektorräume. Gibt es eine analoge Konstruktion auch für Gruppen?

Sei dazu G eine Gruppe und $H \leq G$ eine Untergruppe. Für ein beliebiges $g \in G$ definieren wir

$$gH := \{gh \mid h \in H\} \subseteq G.$$

Die Menge gH heißt die *Linksnebenklasse* von g modulo H. Die Menge

$$G/H := \{gH \mid g \in G\}$$

heißt die *Quotientenmenge* von G modulo H. Wie im Fall von Vektorräumen zeigt man, dass diese Menge eine Partition von G mit zugrundeliegender Äquivalenzrelation

$$g_1 \sim_H g_2 \iff g_1H = g_2H \iff g_1^{-1}g_2 \in H \iff g_2^{-1}g_1 \in H$$

ist. Nun würden wir gerne auf G/H eine Multiplikation definieren durch

$$g_1Hg_2H = g_1g_2H.$$

Leider ist dies aber im Allgemeinen nicht wohldefiniert. Um zu verstehen, wo das Problem liegt, seien $g_1', g_2' \in G$ mit $g_1'H = g_1H$ und $g_2'H = g_2H$. Es existieren dann $h_1, h_2 \in H$ mit $g_1' = g_1h_1$ und $g_2' = g_2h_2$, und daher gilt

$$g_1'g_2' = g_1h_1g_2h_2. \tag{5.2.1}$$

Falls G abelsch ist (wie im Vektorraumfall), so erhalten wir

$$g_1'g_2' = g_1g_2h_1h_2 \implies g_1'g_2'H = g_1g_2H.$$

Im Allgemeinen können wir aber g_2 nicht an h_1 vorbeiziehen.

Definition 5.2.23. Eine Untergruppe $H \leq G$ heißt ein *Normalteiler*, geschrieben $H \trianglelefteq G$, wenn

$$\forall\, g \in G, h \in H : ghg^{-1} \in H.$$

Wir sagen dann, H sei *normal* in G.

Bemerkung 5.2.24 (Quotientengruppe)**.** Ist $H \trianglelefteq G$ ein Normalteiler, so können wir dir rechte Seite von (5.2.1) umschreiben als

$$g_1'g_2' = g_1h_1g_2h_2 = g_1g_2(\underbrace{g_2^{-1}h_1(g_2^{-1})^{-1}}_{\in H})h_2 \implies g_1'g_2'H = g_1g_2H.$$

In diesem Fall (und nur in diesem Fall!) erhalten wir auf G/H also eine wohldefinierte Multiplikation $\mu : G/H \times G/H \to G/H$ mittels

$$g_1H * g_2H := g_1g_2H,$$

und man rechnet leicht nach, dass dann $(G/H, \mu)$ die zugrundeliegende Halbgruppe einer Gruppe $(G/H, \mu, \iota, eH)$ mit $\iota(gH) = g^{-1}H$ ist. Wir nennen $(G/H, \mu)$ die *Quotientengruppe* von G modulo H. Die Abbildung $\pi : G \to G/H$, $g \mapsto gH$ definiert dann einen Epimorphismus auf diese Quotientengruppe, genannt die *kanonische Projektion* modulo H.

Ist G abelsch, so ist jede Untergruppe ein Normalteiler, und wir können stets die Quotientegruppe bilden. Davon haben wir im Fall von Vektorräumen schon reichlich Gebrauch gemacht. Hier ist ein anderes wichtiges Beispiel:

Beispiel 5.2.25 (Addition modulo n)**.** Sei $G := (\mathbb{Z}, +)$, $n \in \mathbb{N}_0$ und $H := n\mathbb{Z}$ die Menge der Vielfachen von n. Für $n = 0$ ist $G/H \cong \mathbb{Z}$. Sei also $n \neq 0$; für $m \in \{0, \dots, n-1\}$ gilt dann

$$[m] := m + n\mathbb{Z} = \{\dots, m-2n, m-n, m, m+n, m+2n, \dots\}.$$

dies sind also genau die ganzen Zahlen, die bei Division durch n den nicht-negativen Rest m lassen. Es gilt dann

$$\mathbb{Z}/n\mathbb{Z} = \{[0], \dots, [n-1]\}$$

und $[m_1] + [m_2] = [r]$, wobei r der nicht-negative Rest von $m_1 + m_2$ bei Division durch n ist. Für $n = 12$ erhalten wir die übliche Addition an der Analoguhr, für $n = 24$ die übliche Addition an der Digitaluhr.

In nicht-abelschen Gruppen sind im Allgemeinen[13] nicht alle Untergruppen normal – z.B. ist die Untergruppe $\{e, (12)\}$ von Sym_3 nicht normal, da

$$(123)(12)(123)^{-1} = (23)$$

gilt. Normalteiler lassen sich in diesem Fall wie folgt charakterisieren:

Proposition 5.2.26. *Für eine Untergruppe $H \leq G$ sind die folgenden Aussagen äquivalent:*

(i) $H \trianglelefteq G$ *ist ein Normalteiler.*

(ii) $H = \ker(\pi)$ *für eine Gruppe K und einen Morphismus $\pi : G \to K$.*

Beweis. (i) $\Longrightarrow$ (ii): Wähle $K := G/H$ und π als die kanonische Projektion.

(ii) $\Longrightarrow$ (i): Nach Proposition 5.2.12 ist $\ker(\pi)$ eine Untergruppe von G. Ist nun $h \in \ker(\pi)$ und $g \in G$, so gilt

$$\pi(ghg^{-1}) = \pi(g)\pi(h)\pi(g^{-1}) = \pi(g)e\pi(g)^{-1} = e \implies ghg^{-1} \in \ker(\pi),$$

also ist $\ker(\pi)$ normal. □

Beispiel 5.2.27. $\mathrm{Alt}_n \leq \mathrm{Sym}_n$ und $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$ sind nach Beispiel 5.2.14 normal.

[13] Es gibt nicht-abelsche Gruppen, für die alle Untergruppen normal sind, sogenannte *Dedekind-Gruppen*, vgl. `https://en.wikipedia.org/wiki/Dedekind_group`

Bemerkung 5.2.28. Ist G eine Gruppe und $H \leq G$, so sind alle Linksnebenklassen xH mit $x \in G$ „gleich groß“[14]: Für $x, y \in G$ ist

$$t_{x,y} : xH \to yH, \quad g \mapsto yx^{-1}g$$

eine wohldefinierte Abbildung (denn ist $g = xh \in xH$, so ist $t_{x,y}(g) = yh \in yH$), und die Abbildungen $t_{x,y}$ und $t_{y,x}$ sind invers zueinander. Ist insbesondere H endlich, so haben gilt

$$|gH| = |H| \quad \text{für alle } g \in G. \tag{5.2.2}$$

Bemerkung 5.2.29 (Kanonische Zerlegung)**.** Sei $\Phi : G \to H$ ein Gruppenhomomorphismus. Für alle $x, y \in G$ gilt

$$\Phi(x) = \Phi(y) \implies \Phi(x^{-1}y) = \Phi(x)^{-1}\Phi(y) = e \implies y \in x\ker(\Phi) \implies \Phi(x) = \Phi(y),$$

also

$$\Phi(x) = \Phi(y) \iff y \in x\ker(\Phi) \iff y\ker(\Phi) = x\ker(\Phi).$$

Die nichtleeren Fasern von Φ sind daher genau die Linksnebenklassen von $\ker(\Phi)$, insbesondere sind sie stets gleich groß im obigen Sinne. Die kanonische Zerlegung von Φ ist dann gegeben durch

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\ker(\Phi) & \xrightarrow[\overline{\Phi}]{} & \mathrm{Bild}(\Phi), \end{array}$$

wobei π die kanonische Projektion ist und $\overline{\Phi}(x\ker(\Phi)) = \Phi(x)$ gilt. Da $\ker(\Phi)$ ein Normalteiler ist, trägt $G/\ker(\Phi)$ (genau wie $\mathrm{Bild}(\Phi)$) eine Gruppenstruktur, und man rechnet sofort nach, dass π, $\overline{\Phi}$ und ι Morphismen sind. Jeder Gruppenhomomorphismus zerlegt sich also in einen Epimorphismus, Isomorphismus und Monomorphismus.

Als Spezialfall erhalten wir:

Satz 5.2.30 (Homomorphiesatz)**.** *Ist $\Phi : G \to H$ ein Gruppenhomomorphismus, so ist*

$$\mathrm{Bild}(\Phi) \cong G/\ker(\Phi). \qquad \square$$

Beispiel 5.2.31. Für $n \geq 2$ ist der Signum-Homomorphismus $\mathrm{sgn} : \mathrm{Sym}_n/\mathrm{Alt}_n$ surjektiv, und nach dem Homomorphiesatz gilt daher

$$\mathrm{Sym}_n/\mathrm{Alt}_n \cong (\{-1, 1\}, \cdot).$$

Bemerkung 5.2.32 (Erzeugte Untergruppe)**.** Ist G eine Gruppe und $\mathfrak{U}$ eine Menge von Untergruppen von G, so ist $\bigcap\mathfrak{U}$ wieder eine Untergruppe von G. Daher existiert zu jeder Teilmenge $S \subseteq G$ eine eindeutig bestimmte kleinste Untergruppe $\langle S\rangle \leq G$, die S enthält, nämlich

$$\langle S\rangle = \bigcap \mathfrak{U}_S, \quad \text{wobei} \quad \mathfrak{U}_S := \{H \leq G \mid S \subseteq H\}.$$

Diese heißt die von S *erzeugte Untergruppe*. Diese abstrakte Beschreibung gibt uns allerdings keine Vorstellung davon, wie Elemente von $\langle S\rangle$ konkret aussehen.

[14] im Sinne von: gleichmächtig

Proposition 5.2.33. *Sei G eine Gruppe, $S \subseteq G$ und $S^{-1} := \{s^{-1} \mid s \in S\}$. Dann gilt*

$$\langle S \rangle = R := \{g \in G \mid \exists g_1, \dots, g_m \in S \cup S^{-1} : g = g_1 \cdots g_m\} \cup \{e\}.$$

Beweis. Wir zeigen, dass R eine Untergruppe von G und daher ein Element von $\mathfrak{U}_S$ ist:

(i) $e \in R$.

(ii) Sind $x, y \in R \setminus \{e\}$, so existieren $g_1, \dots, g_m, h_1, \dots, h_n \in S \cup S^{-1}$ mit $x = g_1 \cdots g_m$ und $y = h_1 \cdots h_n$, also $xy = g_1 \cdots g_m h_1 \cdots h_n \in R$; für $x = e$ oder $y = e$ ist das ohnehin klar.

(iii) ist $x \in R \setminus \{e\}$, so existieren $g_1, \dots, g_m \in S \cup S^{-1}$ mit $x = g_1 \cdots g_m$, also $x^{-1} = g_m^{-1} \cdots g_1^{-1} \in R$. Ist $x = e$, so ist dies ohnehin klar.

Insbesondere gilt dann $\langle S \rangle \subseteq R$. Ist umgekehrt $H \in \mathfrak{U}_S$, so gilt $g_1, \dots, g_m \in H$ und daher $g_1 \cdots g_m \in H$ für alle $g_1, \dots, g_m \in S \cup S^{-1}$. Dies zeigt $R \subseteq H$ für alle $H \in \mathfrak{U}_S$, und daher $R \subseteq \langle S \rangle$. □

Definition 5.2.34. Ist G eine Gruppe so heißt $S \subseteq G$ *Erzeugendenmenge* von G, falls $\langle S \rangle = G$

Beispiel 5.2.35. Wir haben bereits die folgenden interessanten Beispiele gesehen:

(i) Nach Korollar 3.4.6 bilden die invertierbaren Elementarmatrizen ein Erzeugendensystem von $\mathrm{GL}_n(\mathbb{R})$ für alle $n \geq 1$.

(ii) Nach Bemerkung 4.1.12 bilden die Transpositionen eine Erzeugendenmenge von Sym_n für alle $n \geq 2$.

Definition 5.2.36. Eine Gruppe G heißt *zyklisch*, falls $G = \langle g \rangle := \langle \{g\} \rangle$ für ein $g \in G$ gilt.

Beispiel 5.2.37. Die Gruppen $\mathbb{Z}/n\mathbb{Z} = \{[0], \dots, [n-1]\}$ sind zyklisch mit $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$, denn für alle $k \in \{0, \dots, n-1\}$ gilt

$$[k] = [1] \oplus \cdots \oplus [1].$$

Bemerkung 5.2.38 (Zyklische Untergruppen)**.** Ist G eine Gruppe und $g \in G$ und $n \in \mathbb{N}$, so schreiben wir

$$g^n := \underbrace{g \cdots g}_{n \text{ Faktoren}}$$

Weiter definieren wir $g^{-n} := (g^{-1})^n = (g^n)^{-1}$ und $g^0 := e$. Es gelten dann die üblichen Exponentialgesetze $g^m g^n = g^{m+n}$. Dies besagt gerade, dass die Abbildung

$$\Phi_g : (\mathbb{Z}, +) \to G, \quad n \mapsto g^n$$

ein Gruppenhomomorphismus ist. Nach Proposition 5.2.33 und Satz 5.2.30 gilt dann

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \mathrm{Bild}(\Phi_g) \cong \mathbb{Z}/\ker(\Phi_g). \tag{5.2.3}$$

Satz 5.2.39 (Klassifikation zyklischer Untergruppen)**.** *Sei G eine Gruppe, $g \in G$ und $H = \langle g \rangle < G$ eine zyklisch Untergruppe. Dann tritt genau einer der beiden folgenden Fälle ein:*

(a) H ist unendlich; in diesem Fall ist $H \cong (\mathbb{Z}, +)$ und die Potenzen von g sind paarweise verschieden. Insbesondere gilt $g^n \neq e$ für alle $n \neq 0$.

(b) H ist endlich; in diesem Fall existiert ein $n \in \mathbb{N}$ mit $H \cong (\mathbb{Z}/n\mathbb{Z}, \oplus)$ und n ist die kleinste natürliche Zahl mit $g^n = e$. Außerdem gilt $H = \{e, g, g^2, \ldots, g^{n-1}\}$, und diese n Elemente sind verschieden.

Insbesondere ist jede zyklische Gruppe abelsch und isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N} \cup \{0\}$.

Beweis. Nach (5.2.3) gilt $H \cong \mathbb{Z}/\ker(\Phi_g)$, und wegen Lemma 5.2.16 ist entweder $\ker(\Phi_g) = \{0\}$ und wir sind in Fall a), oder $\ker(\varphi_g) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ und wir sind in Fall b). □

Definition 5.2.40. Ist G eine Gruppe und $H \leq G$, so heißt $|H|$ die *Ordnung* von H. Speziell heißt $\operatorname{ord}(g) := |\langle g \rangle|$ die *Ordnung* von g. Weiter heißt $[G : H] := |G/H|$ der *Index* von H in G.

Ist $\operatorname{ord}(g) = n < \infty$, so ist n nach Satz 5.2.39 die kleinste natürliche Zahl mit $g^n = e$. Ist G eine endliche Gruppe, so kann diese Ordnung nur sehr spezielle Werte annehmen:

Satz 5.2.41 (Indexformel)**.** *Ist G eine endliche Gruppe und $H \leq G$, so ist*

$$|G| = |H|[G : H].$$

Insbesondere sind H und $[G : H]$ Teiler von $|G|$.

Beweis. Da die Linksnebenklassen eine Partition von G bilden, gilt

$$G = \bigsqcup_{xH \in G/H} xH \quad \Longrightarrow \quad |G| = \sum_{xH \in G/H} |xH|$$

Nach (5.2.2) gilt nun $|xH| = |H|$ für alle $x \in G$ und daher

$$|G| = \sum_{xH \in G/H} |xH| = \sum_{xH \in G/H} |H| = |G/H| \cdot |H|.$$ □

Korollar 5.2.42 (Satz von Lagrange)**.** *Ist G eine endliche Gruppe und $g \in G$, so ist* $\operatorname{ord}(g)$ *ein Teiler von $|G|$.* □

Hier ist eine überraschende Anwendung, bei der man aus der Anzahl der Elemente einer endlichen Gruppe auf ihre algebraische Struktur schließen kann:

Korollar 5.2.43. *Sei G eine endliche Gruppe und $|G| = p$ eine Primzahl. Dann ist $G \cong \mathbb{Z}/p\mathbb{Z}$. Insbesondere ist G zyklisch, und daher abelsch.*

Beweis. Da $p > 1$ ist, gibt es ein $g \in G$ mit $g \neq e$, also $\operatorname{ord}(g) \neq 1$. Da $\operatorname{ord}(g)$ ein Teiler von $|G| = p$ sein muss, gilt dann

$$|\langle g \rangle| = \operatorname{ord}(g) = p = |G|,$$

also $\langle g \rangle = G$. Folglich ist G zyklisch von Ordnung p, also $G \cong \mathbb{Z}/p\mathbb{Z}$. □

Es gibt also bis auf Isomorphie nur je eine Gruppe der Ordnung 2, 3 und 5. Dagegen gibt es mindestens zwei nicht-isomorphe Gruppen der Ordnung 6, nämlich

$$\mathbb{Z}/6\mathbb{Z} \quad \text{und} \quad \mathrm{Sym}_3 \cong D_6.$$

(Erstere ist zyklisch, also abelsch, letztere ist nicht abelsch.) Wie sieht es nun für Gruppen der Ordnung 4 aus?

Proposition 5.2.44. *Es gibt bis auf Isomorphie genau zwei Gruppen der Ordnung* 4*, und beide sind abelsch.*

Beweis. Sei $|G| = 4$. Existiert $g \in G$ mit $\mathrm{ord}(g) = 4$, so ist $G = \langle g \rangle$ zyklisch, also isomorph zu $\mathbb{Z}/4\mathbb{Z}$. Andernfalls gilt nach dem Satz von Lagrange $G = \{e, a, b, c\}$ mit $\mathrm{ord}(a) = \mathrm{ord}(b) = \mathrm{ord}(c) = 2$, also insbesondere $a^2 = b^2 = c^2 = e$. Was ist ab? Wir probieren alle Möglichkeiten durch:

- $ab = e$ würde bedeuten, dass $b = a^{-1}$, aber wegen $a^2 = e$ ist $a^{-1} = a$, Widerspruch.
- Wäre $ab = a$, so wäre $e = a^{-1}a = a^{-1}ab = b$. Widerspruch.
- Wäre $ab = b$, so wäre $e = bb^{-1} = abb^{-1} = a$. Widerspruch.
- Es bleibt also nur die Möglichkeit $ab = c$.

Analog zeigt man $ba = c$ und $ac = ca = b$ bzw. $bc = cb = a$. Damit ist aber die Multiplikation von G eindeutig bestimmt. □

Die eindeutige nicht-zyklische (abelsche) Gruppe der Ordnung 4 heißt die *Kleinsche*[15] *Vierergruppe*. Sie kann als das direkte Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mit komponentenweiser Addition realisiert werden.

Zum Abschluss dieses Abschnitts beweisen wir noch eine Formel, die in der Kombinatorik zahlreiche Anwendungen hat.

Bemerkung 5.2.45 (Bahnen)**.** Wirkt eine Gruppe G auf einer Menge M und ist $m \in M$, so heißt die Abbildung

$$b_m : G \to M, \quad g \mapsto g.m$$

die zugehörge *Bahnabbildung*, und ihr Bild $G.m := \{g.m \mid g \in G\}$ heißt die *Bahn* von m unter G.

Die Bahnen einer Wirkung bilden eine Partition von M, genannt die *Bahnzerlegung*; zum Beweis zeigt man, das die Relation

$$m \sim m' :\iff \exists g \in G : \, g.m = m'$$

eine Äquivalenzrelation ist: Sind $m, m', m'' \in M$, so gilt $m = e.m$ und aus $m' = g.m$ für ein $g \in G$ folgt $m = e.m = (g^{-1}g).m = g^{-1}.(g.m) = g^{-1}.m'$. Ist schließlich $m' = g.m$ und $m'' = h.m'$ für $g, h \in G$, so gilt $m'' = h.(g.m) = (hg).m$.

Ist $b_m : G \to M$ die Bahnabbildung zu einem fest gewählten $m \in M$, so gelten für $g, h \in G$ die Äquivalenzen

$$b_m(gh) = b_m(g) \iff gh.m = g.m \iff h.m = m \iff h \in \mathrm{Stab}_G(m) := \{h \in G \mid h.m = m\}. \quad (5.2.4)$$

Die Teilmenge $\mathrm{Stab}_G(m)$ heißt der *Stabilisator* von m und ist eine Untergruppe von G, denn es gilt $e \in \mathrm{Stab}_G(m)$ und gilt $g.m = m$ und $h.m = m$, so ist $(gh).m = g.(h.m) = g.m = m$ und $g^{-1}.m = g^{-1}.(g.m) = m$. Wegen (5.2.4) erhalten wir eine wohldefinierte injektive Abbildung

$$\overline{b}_m : G/\mathrm{Stab}_G(m) \to M, \quad g\mathrm{Stab}_G(m) \mapsto g.m.$$

Das Bild dieser Abbildung ist gerade die Bahn $G.m$ von M, insbesondere gilt

$$|G.m| = [G : \mathrm{Stab}_G(m)]. \quad (5.2.5)$$

[15] Felix Klein (1849-1925), dt. Mathematiker, der in seinem Erlanger Programm 1872 die Grundlagen der Geometrie neu sortierte, und darin die zentrale Bedeutung des Gruppenbegriffs für die Geometrie in den Mittelpunkt stellte.

Die Bahnzerlegung ist besonders nützlich, wenn M in endlich viele Bahnen zerfällt, z.B. weil M selbst endlich ist. In diesem Fall gilt:

Satz 5.2.46 (Bahnbilanzformel)**.** *Wirkt eine Gruppe G auf einer endlichen Menge M mit Bahnen $G.m_1,\dots,G.m_n$, so gilt*

$$|M| \quad = \quad \sum_{i=1}^{n} [G : \mathrm{Stab}_G(m_i)]. \tag{5.2.6}$$

Beweis. Da die Bahnen eine Partition von M bilden, gilt

$$|M| = \sum_{i=1}^{n} |G.m_i|.$$

Die Behauptung folgt dann aus (5.2.5). □

Beispiel 5.2.47 (Drehungen des Würfels)**.** Wir betrachten die Gruppe G der Drehungen des $\mathbb{R}^3$, die einen Würfel W auf sich selbst abbilden. Beachte, dass jede solche Drehung den Mittelpunkt des Würfels festhält. Wir dürfen annehmen, dass dieser Mittelpunkt als Koordinatenursprung gewählt ist; dann sind alle Elemente von G lineare Abbildungen und sind daher durch die Bilder von drei linear unabhängigen Punkten (z.B. drei Ecken) eindeutig bestimmt.

Wir bezeichnen mit V, E und F die Mengen der[16] Ecken, Kanten und Seitenflächen von W. Dann wirt G auf $V \subseteq \mathbb{R}^3$ durch $g.v := g(v)$ und auf $E, F \subseteq \mathscr{P}(\mathbb{R}^3)$ durch $g.A := g[A]$. Wir studieren die Bahnen und Stabilisatoren dieser Wirkungen.

Wir bestimmen zunächst den Stabilisator $\mathrm{Stab}_G(f)$ einer Seitenfläche $f \in F$. Ist $g \in \mathrm{Stab}_G(f)$, so gilt $g[f] = f$ und daher muss g die eindeutige affine Ebene A durch f auf sich selbst abbilden. Das ist nur möglich, wenn $g|_A$ eine Drehung (um den Mittelpunkt von f) ist, die die vier Ecken von f permutiert. Nummerieren wir die Ecken von f gegen den Uhrzeigersinn von v_1 bis v_4 durch, so erhalten wir eine Gruppenhomomorphismus

$$\iota : \mathrm{Stab}_G(f) \to \mathrm{Sym}_4, \quad \text{so dass } g(v_j) = v_{\iota(g)(j)} \text{ für alle } j \in \{1,\dots,4\}.$$

Da eine Drehung durch die Bilder von drei Ecken eindeutig festgelegt ist, ist ι injektiv. Jede Drehung in A, die die Menge $\{v_1,\dots,v_4\}$ festhält, muss benachbarte Ecken auf benachbarte Ecken abbilden und die Orientierung erhalten, und der Drehwinkel muss ein Vielfaches von $\pi/2$ sein; folglich gilt

$$\mathrm{Stab}_G(f) \cong \mathrm{Bild}(\iota) = \langle (1234) \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Teilt f eine Kante e mit $f' \in F$, so können wir f durch Drehung um die affine Gerade durch e um $\pi/4$ auf f' abbilden. Durch Verkettung solcher Drehungen können wir f daher auf jede andere Seitenfläche abbilden. Es gilt also $G.f = F$ und daher

$$|G| = |\mathrm{Stab}_G(f)||G.f| = |\mathrm{Stab}_G(f)||F| = 4 \cdot 6 = 24.$$

Das obige Element zeigt auch noch, dass wir jede Ecke von f durch ein Element von $\mathrm{Stab}_G(f)$ auf jede andere Ecke von f abbilden können. Sind v und v' zwei beliebige Ecken, so finden wir Ecken $v_1,\dots,v_k$ mit $v = v_1$ und $v' = v_k$, so dass v_j und v_{j+1} in einer gemeinsamen Fläche liegen. v_j und v_{j+1} liegen dann in derselben G-Bahn, also gilt insbesondere $G.v = V$. Wir erhalten daher

$$24 = |G| = |\mathrm{Stab}_G(v)||G.v| = |\mathrm{Stab}_G(v)||V| = 8|\mathrm{Stab}_G(v)| \implies |\mathrm{Stab}_G(v)| = 3.$$

[16] von engl. „vertices“, „edges“, „faces“

Da 3 eine Primzahl ist, folgt $\mathrm{Stab}_G(v) \cong \mathbb{Z}/3\mathbb{Z}$. Analog überlegt man sich, dass $\mathrm{Stab}_G(f)$ je zwei Kanten in f aufeinander abbildet und folgert daraus, dass $G.e = E$ für jede Kante $e \in E$. Folglich ist

$$24 = |G| = |\mathrm{Stab}_G(e)||G.e| = |\mathrm{Stab}_G(e)||E| = 12|\mathrm{Stab}_G(v)| \implies |\mathrm{Stab}_G(v)| = 2.$$

Da 3 eine Primzahl ist, folgt $\mathrm{Stab}_G(v) \cong \mathbb{Z}/2\mathbb{Z}$. Wir können unsere Überlegungen wie folgt zusammenfassen:

Die Drehgruppe des Wüfels besteht aus 24 *Drehungen (inklusive der Identität). Die Ecken-, Kanten- und Seitenflächstenstabilisatoren sind allesamt zyklisch und von Ordnung* 3 *bzw.* 2 *bzw.* 4. *Es gibt also in G Drehungen mit Drehwinkel* $2\pi/3$*,* π*, und* $\pi/2$.

Wie sehen die 24 Drehungen des Würfels konkret aus? Um jede Gerade durch gegenüberliegende Seitenmittelpunkte können wir um Vielfache von $\pi/2$ drehen (Seitenflächsenstabilisatoren!). Das liefert neben der Identität $3 \cdot 3 = 9$ Drehungen. Um die Geraden durch die Mittelpunkte zweier gegenüberliegenden Seiten kann man um Vielfache von π drehen (Kantenstabilisatoren!), das liefert weitere 6 nicht-triviale Drehungen. Um zwei gegenüberliegende Ecken kann man um Vielfache von $2\pi/3$ drehen (Eckenstabilisatoren!), das liefert weitere $2 \cdot 4 = 8$ nicht-triviale Drehungen. Wegen $1 + 9 + 6 + 8 = 24$ haben wir damit alle Elemente von G gefunden. Insgesamthat der Würfel also $3 + 6 + 4 = 13$ Drehachsen.

Übung 5.2.48. Untersuchen Sie analog die Drehgruppen der anderen vier platonischen Körper, vgl. `https://de.wikipedia.org/wiki/Platonischer_K%C3%B6rper`

Zusammenfassung von Abschnitt 5.2

(1) Abstrakte Gruppen sind Mengen mit einer assoziativen 2-stelligen Verknüpfung, die ein neutrales Element besitzen und für die jedes Element ein Inverses besitzt. Wichtige Beispiele sind symmetrische Gruppen, allgemeine lineare Gruppen und deren Untergruppen.

(2) Konkret können wir Gruppen mittels Wirkungen als Symmetriegruppen, also Untergruppen von symmetrischen Gruppen, realisieren. Für Wirkungen von Gruppen auf endlichen Mengen gilt die Bahnbilanzformel.

(3) Ist G eine Gruppe und H ein Normalteiler von G, so trägt G/H wieder eine Gruppenstruktur. Beispiele für solche Quotientengruppen sind die Gruppen $(\mathbb{Z}/n\mathbb{Z}, \oplus)$.

(4) Gruppenhomomorphismen zerlegen sich kanonisch in Epi-, Iso- und Monomorphismen. Insbesondere sind homomorphe Bilder einer Gruppe isomorph zu Quotienten dieser Gruppe.

(5) Jede zyklische Gruppe ist isomorph zu einer der Gruppen $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N} \cup \{0\}$, insbesondere abelsch. Jede Gruppe von Primzahlordnung ist zyklisch.

[17.01.24]

5.3 Ringe und Körper

In vielen Strukturen, z.B. den gängigen Zahlbereichen, haben wir es nicht nur mit einer, sondern mit zwei Verknüpfungen zu tun (Addition und Multiplikation), die miteinander kompatibel sind. Solche Strukturen werden durch Ringe beschrieben.

Definition 5.3.1. Es sei $\mathscr{R} = (R, A, M, \iota, 0, 1)$ eine Algebra vom Typ (2,2,1,0,0). Wir schreiben

$$x + y := A(x, y) \quad \text{und} \quad x \cdot y := M(x, y)$$

und nennen A die *Addition* und M die *Multiplikation* von $\mathscr{R}$.

(i) $\mathscr{R}$ heißt ein *Ring*, falls $(R, A, \iota, 0)$ eine abelsche Gruppe und $(R, M, 1)$ ein Monoid ist und die folgenden *Distributivgesetze* gelten:

$$\forall\, a, b, c \in R : (a + b) \cdot c = (a \cdot c) + (b \cdot c) \text{ und } a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

(ii) $\mathscr{R}$ heißt ein *kommutativer Ring*, falls zusätzlich der Monoid $(R, M, 1)$ abelsch ist.

WARNUNG! Manche Autoren verlangen von einem Ring nicht, dass ein neutrales Element der Multiplikation existiert. Diese Autoren nennen dann das, was wir einen Ring nennen, einen „Ring mit Eins“. In den seltenen Fällen, wo wir es mit Strukturen zu tun haben, in denen die Multiplikation kein neutrales Element hat, die aber sonst alle Ringaxiome erfüllen, sprechen wir von einem *Ring ohne Eins* oder kurz einem *Rng*.

Bemerkung 5.3.2. Es sei $\mathscr{R} = (R, A, M, \iota, 0, 1)$ ein Ring.

(i) Die Addition A eines Rings ist stets als kommutativ angenommen! Wenn wir von einem *kommutativen* Ring sprechen, ist damit stets die Multiplikation gemeint.

(ii) Wir bezeichnen das Inverse von x bzgl. + mit $-x$. Falls x ein multiplikatives Inveses hat, so bezeichnen wir dieses mit x^{-1}. Für Potenzen bzgl. der beiden Operationen schreiben wir

$$nx := \underbrace{x + \cdots + x}_{n \text{ mal}} \quad \text{und} \quad x^n := \underbrace{x \cdot \cdots \cdot x}_{n \text{ mal}}.$$

wir setzen noch $(-n)x := -(nx)$ und, falls x ein multiplikatives Inverse besitzt, $x^{-n} := (x^{-1})^n$.

(iii) Soweit es die Assoziativgesetze erlauben, lassen wir Klammern weg; wir machen die üblich „Punkt- vor Strichrechnung“-Konvention. Malpunkte lassen wir häufig auch einfach ganz weg.

(iv) Statt $(R, A, M, \iota, 0, 1)$ schreiben wir häufig auch nur kurz R.

Beispiel 5.3.3. Ringe modellieren einerseits Zahlbereiche, andererseits[17] Funktionenmengen:

[17] Es ist eine der wesentlichen Erkenntnisse der Mathematik des 19. und 20. Jahrhunderts, dass sich Zahlbereiche wie die Menge der ganzen Zahlen und Funktionenmengen wie der Menge der reellen Polynomfunktionen strukturell so ähnlich sind, dass sich Methoden der Zahlentheorie gewinnbringend in der Funktionentheorie einsetzen lassen und umgekehrt.

(i) Die Zahlbereiche $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ und $(\mathbb{R},+,\cdot)$ sind Ringe.

(ii) Ist R ein (kommutativer) Ring und M eine beliebige Menge, so ist die Menge $\mathrm{Abb}(M,R)$ der Abbildungen von M nach R ein (kommutativer) Ring bzgl.

$$(f+g)(m) := f(m)+g(m) \quad \text{und} \quad (f\cdot g)(m) := f(m)\cdot g(m) \quad (f,g\in R^M, m\in M).$$

Er heißt der *Ring der R-wertigen Funktionen* auf M. Spezielle Beispiele mit besonderer Relevanz für die Analysis sind $\mathrm{Abb}(\mathbb{R},\mathbb{R})$, der *Ring der reell-wertigen Funktionen* auf $\mathbb{R}$, und $\mathrm{Abb}(\mathbb{N},\mathbb{R})$, der *Ring der reellen Folgen*.

(iii) Ist V ein $\mathbb{R}$-Vektorraum, so ist $\mathrm{End}_{\mathbb{R}}(V)$ ein (im Allgemeinen nicht-kommutativer) Ring bzgl. der Addition gegeben durch $(\varphi+\psi)(v) := \varphi(v)+\psi(v)$ und Multiplikation gegeben durch Verkettung. Er heißt der *Endomorphismen-Ring* von V.

Lemma 5.3.4. *Sei R ein Ring und $a,b\in R$. Dann gilt:*

(i) $a\cdot 0 = 0\cdot a = 0$.

(ii) Ist $0=1$*, so ist* $R=\{0\}$.

(iii) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$.

(iv) $(-a)\cdot(-b) = ab$.

(v) $(-1)\cdot a = -a$.

Beweis. (i) Aus $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$ folgt $0\cdot a = 0$, analog zeigt man $a\cdot 0 = 0$.

(ii) Wegen (i) gilt $a = a\cdot 1 = a\cdot 0 = 0$ für alle $a\in R$.

(iii) Wegen (i) gilt $a\cdot b+(-a)\cdot b = (a+(-a))\cdot b = 0$ und daher $(-a)\cdot b = -(a\cdot b)$, analog $a\cdot(-b) = -(a\cdot b)$.

(iv) und (v) folgen aus (iii). □

Bemerkung 5.3.5 (Unterringe und Ringhomomorphismen)**.** Genau wie für Gruppen können wir auch in der Kategorie der Ringe wieder Unterobjekte und Morphismen betrachten. Eine Teilmenge $R'\subseteq R$ heißt ein *Unterring*, wenn sie abgeschlossen unter allen Verknüpfungen von R ist (also insbesondere 0 und 1 enthält). Dann ist R' mit den Einschränkungen dieser Verknüpfungen selbst wieder ein Ring. Umgekehrt nennt man dann R eine *Ringerweiterung* von R'.

Bei Morphismen müssen wir aufpassen: Sind R und S zwei Ringen, so ist eine Abbildung $f: R\to S$ nach Definition ein *(Ringhomo-)Morphismus*, wenn f alle Verknüpfungen erhält. Dazu ist es erforderlich, dass

$$f(x+x') = f(x)+f(x') \quad \text{und} \quad f(xx') = f(x)f(x') \quad \text{für alle } x,x'\in R \tag{5.3.1}$$

gilt, aber das ist *nicht* genug! Da $(R,+,0)$ eine Gruppe ist, folgt zwar aus (5.3.1) und Bemerkung 5.2.11, dass $f(0)=0$ und $f(-x)=-f(x)$ gilt, aber die Bedingung

$$f(1) = 1 \tag{5.3.2}$$

folgt *nicht* aus (5.3.1) und muss daher zusätzlich gefordert werden. Mit der korrekten Definition ist das Bild eines Ringhomomorphismus ein Unterring[18] (Übung!).

[18] Wenn man (5.3.2) nicht fordern würde, dann wäre die Abbildung $f:\mathbb{R}\to\mathbb{R}^{2\times 2}$, $x\mapsto \begin{pmatrix} x & 0\\ 0 & 0\end{pmatrix}$ ein Morphismus, ihr Bild ist aber kein Unterring von $\mathbb{R}^{2\times 2}$, da es die $\mathbf{1}$ nicht enthält!

Bemerkung 5.3.6 (Kerne und Ideale)**.** Wie im Fall von Gruppen definiert man den *Kern* eines Ringhomomorphismus $f : R \to S$ als $\ker(f) := \{r \in R \mid f(r) = 0\}$. Ist $|S| \geq 2$, so ist dies niemals ein Ring, denn in diesem Fall gilt $f(1) = 1 \neq 0$, also $1 \notin \ker(f)$. Der Kern hat aber trotzdem eine interessante Struktur (nur eben keine Ringstruktur):

- Da $f : (R,+) \to (S,+)$ ein Gruppenhomomorphismus ist, ist $\ker(f)$ eine *Untergruppe* von $(R,+)$ (also ein Normalteiler, da $(R,+)$ abelsch ist).
- $\ker(f)$ ist abgeschlossen unter Multiplikation (und daher ein Rng). Allgemeiner gilt für alle $r \in R$ und $x \in \ker(f)$, dass

$$f(rx) = f(r)f(x) = f(r)0 = 0 = 0f(r) = f(x)f(r) = f(xr) \implies \{rx, xr\} \in \ker(f).$$

Allgemein nennt man eine Untergruppe I von $(R,+)$ ein *Ideal* und schreibt dafür[19] $I \trianglelefteq R$, falls $\{rx, xr\} \in I$ für alle $r \in R$ und $x \in I$ gilt. Der Kern eines Ringhomomorphismus ist also ein Ideal.

Beispiel 5.3.7 (Ideale in $\mathbb{Z}$)**.** Die abelschen Untergruppen von $(\mathbb{Z},+)$ sind nach Lemma 5.2.16 genau die Vielfachenmengen $n\mathbb{Z}$ mit $n \in \mathbb{N} \cup \{0\}$. Alle diese Teilmengen sind sogar Ideale des Rings $\mathbb{Z}$, denn für $m \in \mathbb{Z}$ und $nk \in n\mathbb{Z}$ gilt $m(nk) = n(km) \in n\mathbb{Z}$.

Ideale erlauben es uns, Quotienten von Ringen zu definieren, und auf diese Weise wichtige neue Beispiele für Ringe zu konstruieren.

Lemma 5.3.8. *Sei R ein Ring, $I \trianglelefteq R$ und $(R/I, \oplus)$ die Quotientengruppe von $(R,+)$ modulo $(I,+)$.*

(i) $\odot : R/I \times R/I \to R/I$, $(r+I) \odot (s+I) := rs + I$ *ist wohldefiniert.*

(ii) $(R/I, \oplus, \odot, (r+I \mapsto -r+I), 0+I, 1+I)$ *ist ein Ring.*

Beweis. (i) Seien $r, s, r', s' \in R$ mit $r + I = r' + I$ und $s + I = s' + I$. Dann gilt

$$i := r - r' \in I \quad \text{und} \quad j := s - s' \in I,$$

und daher

$$rs - r's' = rs + r's - r's - r's' = (r - r')s + r'(s - s') = is + r'j \in I + I \subseteq I,$$

also $rs + I = r's' + I$.

(ii) Wir wissen bereits, dass $(R/I, \oplus, 0+I)$ eine abelsche Gruppe ist. Das Assoziativgesetz gilt in $(R/I, \odot)$, denn für $r, s, t \in R$ gilt

$$((r+I)\odot(s+I))\odot(t+I) = (rs+I)\odot(t+I) = ((rs)t)+I = (r(st))+I = (r+I)\odot(st+I) = (r+I)\odot((s+I)\odot(t+I)).$$

Die anderen Axiome für die Multiplikation und die Distributivgesetze folgen analog aus den entsprechenden Axiomen für R. □

Definition 5.3.9. Der Ring $(R/I, \oplus, \odot)$ heißt der *Quotientenring* von R modulo I.

[19] Man benutzt dasselbe Symbol für Normalteiler von Gruppen und Idealen in Ringen. Die Bedeutung kann nur aus dem Kontext erschlossen werden.

Beispiel 5.3.10 (Restklassenringe)**.** Für $n \in \mathbb{N}$ ist $n\mathbb{Z}$ ein Ideal in $\mathbb{Z}$, daher können wir den Quotientenring $\mathbb{Z}/n\mathbb{Z}$ bilden. Dieser heißt der *Restklassenring* von $\mathbb{Z}$ modulo n. Als Menge ist nach wie vor $\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$, aber nun haben wir neben der Addition auch noch eine Multiplikation. Für $k, l \in \{0, \ldots, n-1\}$ gilt $[k] \odot [l] = [m]$, wobei m der Rest von kl bei Division durch n ist.

Der Ring $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$ ist für die Informatik und die Kombinatorik gleichermaßen von zentraler Bedeutung. Wir werden darauf noch zurückkommen.

Bemerkung 5.3.11 (Kanonische Projektion)**.** Nach Definition ist $\pi : R \to R/I$, $r \mapsto r + I$ ein Epimorphismus mit $\ker(\pi) = I$. Insbesondere sind die Ideal von R genau die Kerne von Ringhomomorphismen.

Bemerkung 5.3.12 (Kanonische Zerlegung)**.** Alles was wir über die kanonische Zerlegung eines Gruppenhomomorphismus gesagt haben, überträgt sich mutatis mutandis auf Ringhomomorphismen. Wir geben hier nur das Ergebnis an, und überlassen Ihnen die Details zur Übung.

Sei $f : R \to S$ ein beliebiger Ringhomomorphismus. Dann ist f insbesondere ein Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$ und hat als solcher eine kanonische Zerlegung der Form

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ R/\ker(f) & \xrightarrow[\quad \overline{f} \quad]{} & \mathrm{Bild}(f). \end{array}$$

Versieht man nun $R/\ker(f)$ mit der Quotientenringstruktur und $\mathrm{Bild}(f)$ mit der Ringstruktur als Unterring von S, so sind die Abbildungen π, $\overline{\varphi}$ und ι (nicht nur Gruppenhomomorphismen sondern sogar) Ringhomomorphismen.

Korollar 5.3.13 (Homomorphiesatz)**.** *Ist $f : R \to S$ ein Ringhomomorphismus, so ist*

$$\mathrm{Bild}(f) \cong R/\ker(f). \qquad \square$$

Die folgenden Übungen liefern eine Konstruktion der reellen Zahlen ausgehend von den rationalen Zahlen; wir setzen aus der ANALYSIS I den Begriff eines „vollständig angeordneten Körpers“sowie die Begriffe der Cauchyfolge und der Nullfolge voraus.

Übung 5.3.14 (Konstruktion der reellen Zahlen)**.** Wir nehmen zunächst an, dass ein vollständig angeordneter Körper $\mathbb{R}$ existiert. Zeigen Sie:

(i) Die rationalen Cauchyfolgen bilden einen Unterring $\mathfrak{C}$ von $\mathrm{Abb}(\mathbb{N}, \mathbb{Q})$.

(ii) Jede Folge $(a_n) \in \mathscr{C}$ konvergiert in $\mathbb{R}$ gegen einen Grenzwert $a = \lim a_n$.

(iii) Die Abbildung $\lim : \mathfrak{C} \to \mathbb{R}$, $(a_n) \mapsto \lim a_n$ ist ein Epimorphismus.

(iv) Es gilt $\mathbb{R} \cong \mathfrak{C}/\mathfrak{N}$, wobei $\mathfrak{N} := \ker(\lim) \trianglelefteq \mathfrak{C}$ die Menge der rationalen Nullfolgen ist. Unter diesem Isomorphismus entspricht die Ordnungslrelation $\leq$ von $\mathbb{R}$ der Ordnungsrelation auf $\mathfrak{C}/\mathfrak{N}$, die durch

$$[(a_n)] \leq [(b_n)] :\Leftrightarrow \exists n \in \mathbb{N}\ \forall m \geq n : a_m \leq b_n$$

gegeben ist.

(v) $\mathfrak{C}/\mathfrak{N}$ ist mit der obigen Ordnungsrelation ein vollständig angeordneter Körper, und jeder andere vollständig angeordnete Körper sind ist isomorph zu diesem.

Es gibt also (bis auf Isomorphie) höchstens einen vollständig angeordneten Körper, und wenn es überhaupt einen gibt, dann muss dieser isomorph zu $\mathfrak{C}/\mathfrak{N}$ sein! Dies liefert zugleich eine Strategie für den Nachweis der Existenz eines solchen Körpers:

Übung 5.3.15. Es sei $\mathfrak{C} \leq \mathrm{Abb}(\mathbb{N}, \mathbb{Q})$ der Unterring der rationalen Nullfolgen und $\mathfrak{N} \lhd \mathfrak{C}$ das Ideal der Nullfolgen. Zeigen Sie:

(i) $[(a_n)] \leq [(b_n)] :\Leftrightarrow \exists n \in \mathbb{N}\, \forall m \geq n : a_m \leq b_n$ definiert eine Ordnungsrelation auf $\mathfrak{C}/\mathfrak{N}$.

(ii) Der Quotientenring $\mathfrak{C}/\mathfrak{N}$ ist mit dieser Ordnungsrelation ein vollständig angeordneter Körper ist.

Insgesamt hat man damit gezeigt, dass es einen vollständig angeordneten Körper gibt, und dass dieser eindeutig bis auf Isomorphie ist.

Ab jetzt (bis einschließlich Korollar 5.3.37) sei R ein *kommutativer* Ring.

Definition 5.3.16. $x \in R$ heißt ein *Nullteiler*, falls $x \cdot y = 0$ für ein $y \in R \setminus \{0\}$ gilt.

Beispiel 5.3.17 (Ringe mit vielen Nullteilern)**.** Es seien $f, g \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ zwei Funktionen mit der Eigenschaft, dass $f(x) = 0$, falls $x < 0$ und $g(x) = 0$, falls $x > 0$. Dann ist $fg = 0$, also sind f und g Nullteiler in $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$.

Beispiel 5.3.18 (Ringe mit wenigen Nullteilern)**.** In den Ringen $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ ist 0 jeweils der einzige Nullteiler.

Definition 5.3.19. R heißt *Integritätsbereich*, falls $0 \neq 1$ und 0 der einzige Nullteiler[20] in R ist.

$\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ sind also Integritätsbereiche, $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ hingegen nicht.

Beispiel 5.3.20 (Nullteiler und Invertierbarkeit)**.** Ein invertierbare Element x von $(R, \cdot, 1)$ kann niemals ein Nullteiler sein. Ist nämlich $x^{-1}x = 1$ und $xy = 0$, so folgt $y = 1y = x^{-1}xy = x^{-1}0 = 0$. Die Umkehrung dieser Aussage gilt nicht, denn 2 ist in $\mathbb{Z}$ weder Nullteiler noch invertierbar. In endlichen Ringen kann das nach dem folgenden Lemma nicht passieren.

Lemma 5.3.21. *Sei R ein Ring, $x \in R \setminus \{0\}$ und $\lambda_x : R \to R$, $y \mapsto xy$.*

(i) x ist Nullteiler $\Leftrightarrow$ λ_x ist ist nicht injektiv.

(ii) x ist invertierbar in $(R, \cdot, 1)$ $\Leftrightarrow$ λ_x ist surjektiv.

(iii) Ist R endlich, so ist jedes $x \in R$ entweder ein Nullteiler oder invertierbar in $(R, \cdot, 1)$.

Beweis. (i) Ist x Nullteiler, so existiert ein $y \neq 0$ mit $\lambda_x(y) = 0 = \lambda_x(0)$, also ist λ_x nicht injektiv.

Ist λ_x nicht injektiv, so existieren $y \neq z$ mit $\lambda_x(y) = \lambda_x(z)$. Dann ist $x(y - z) = xy - xz = 0$, also ist x ein Nullteiler.

(ii) Ist x invertierbar und $y \in R$, so ist $y = \lambda_x(x^{-1}y) \in \mathrm{Bild}(\lambda_x)$, also ist λ_x surjektiv.

Ist λ_x surjektiv, so existiert ein $y \in R$ mit $\lambda_x(y) = 1$, also $xy = yx = 1$. Dann ist x invertierbar mit $x^{-1} = y$.

[20] Man nennt einen Ring, in dem 0 der einzige Nullteiler ist, traditionalle auch einen *nullteilerfreien* Ring, aber das ist verwirrend. Der Begriff Integritätsbereich deutet darauf hin, dass die Abwesenheit von nicht-trivialen Nullteilern zwischen Zahlbereichen und Funktionenringen unterscheidet.

(iii) Dies folgt aus (i) und (ii) und der Tatsache, dass jede injektive Selbstabbildung einer endlichen Menge automatisch bijektiv ist. □

Insbesondere ist in jede Restklasse in $\mathbb{Z}/n\mathbb{Z}$ entweder invertierbar oder ein Nullteiler.

Beispiel 5.3.22. In $\mathbb{Z}/6\mathbb{Z}$ gilt $[2][3] = [0] = [3][4]$ und $[5][5] = [1] = [1][1]$, also sind $[0]$, $[2]$, $[3]$, $[4]$ Nullteiler und $[1]$ und $[5]$ sind invertierbar.

Um Nullteiler in Restklassenringen systematisch zu verstehen, benötigen wir einige Begriffe und Resultate aus der elementaren Zahlentheorie:

Bemerkung 5.3.23 (Teilbarkeit und Primzahlen)**.** Sind $r,s,t \in \mathbb{N}$ mit $r = st$, so nennen wir s einen *Teiler* von r. Dann ist $t = r/s$ durch r und s eindeutig bestimmt und heißt der *Komplementärteiler* von s. Wir bezeichnen mit $\mathscr{T}_r$ die Menge der Teiler von r.

Für jedes $r \in \mathbb{N}$ sind 1 und r zwei (komplementäre) Teiler von r, die anderen Teiler von r heißen *nicht-triviale Teiler*. Eine natürliche Zahl $p \geq 2$, die keine nicht-trivialen Teiler besitzt, heißt *Primzahl*. Dies ist gleichbedeutend mit $|\mathscr{T}_p| = 2$.

Sind $m,n \in \mathbb{N}$, so ist $\mathscr{T}_m \cap \mathscr{T}_n$ eine endliche Menge natürlicher Zahlen, die die 1 enthält. Daher existiert $\mathrm{ggT}(m,n) := \max \mathscr{T}_m \cap \mathscr{T}_n$. Wir nennen $\mathrm{ggT}(m,n)$ den *größten gemeinsamen Teiler* von m und n.

Bemerkung 5.3.24 (Euklidischer Algorithmus)**.** Wir wollen den ggT von $m := 1071$ und $n := 1029$ bestimmen. Wiederholtes Anwenden der Division mit Rest liefert

$$\begin{array}{rcrcr} 1071 & = & 1 \cdot 1029 & + & 42 \\ 1029 & = & 24 \cdot 42 & + & 21 \\ 42 & = & 2 \cdot 21 & + & 0. \end{array} \tag{5.3.3}$$

Aus der letzten Zeile folgt, dass 42 ein Vielfaches von 21 ist. Aus der vorletzten Zeile folgt dann, dass 1029 ein Vielfaches von 21 ist. Aus der ersten Zeile folgt dann, dass 1071 ein Vielfaches von 21 ist. Folglich ist der „letzte Rest“ 21 ein gemeinsamer Teiler von a und b. Dieser ist sogar schon der *größte* gemeinsame Teiler: Ist nämlich t ein beliebiger Teiler von 1029 und 1071, so ist t wegen der ersten Zeile auch ein Teiler von 42 und dann wegen der zweiten Zeile auch ein Teiler von 21.

Durch wiederholte Division mit Rest erhält man also den ggT zweier natürlicher Zahl. Man nennt diesen Algorithmus[21] den *euklidischen Algorithmus*.

Bemerkung 5.3.25 (Erweiterter euklidischer Algorithmus)**.** Man kann aus den Gleichungen in (5.3.3) noch mehr ablesen. Ignoriert man die letzte Zeile und liest die anderen Zeilen rückwärts, so erhält man

$$21 = 1029 - 24 \cdot 42 \quad \text{und} \quad 42 = 1071 - 1 \cdot 1029.$$

Einsetzen liefert dann

$$21 = 1029 - 24 \cdot (1071 - 1 \cdot 1029) = (-24) \cdot 1071 + 25 \cdot 1029.$$

Wir haben also 21 als ganzzahlige Linearkombination von 1071 und 1029 geschrieben. Man nennt dieses Verfahren den *erweiterten euklidischen Algorithmus*.

[21] Zur besonderen historischen Bedeutung dieses Algorithmus bemerkt Donald E. Knuth auf S. 335 von „The art of computer programming“: *„We might call Euclid's method the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day.“*

Der euklidische Algorithmus und der erweiterte Algorithmus funktionieren für beliebige natürliche Zahlen m und n. Damit haben wir insbesondere bewiesen:

Lemma 5.3.26 (Lemma von Bezout)**.** *Für beliebige $m,n \in \mathbb{N}$ existieren $r,s \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(m,n) = rm + sn.$$

Die Zahlen r und s können mittels erweitertem euklidischen Algorithmus bestimmt werden. □

Daraus folgt nun leicht:

Proposition 5.3.27. *Es seien $m,n \in \mathbb{N}$.*

(i) *$[m]$ ist invertierbar in $(\mathbb{Z}/n\mathbb{Z}, \odot, 1) \iff \mathrm{ggT}(m,n) = 1$.*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ ist Integritätsbereich $\iff$ n ist Primzahl.*

Beweis. (i) „$\Longrightarrow$“: Angenommen $t := \mathrm{ggT}(m,n) > 1$; schreibe $m = rt$ und $n = st$ mit $1 < r < m$ und $1 < s < n$ Dann gilt $sm = rst = rn$ und daher $[s][m] = [0]$. Wegen $[s] \neq 0$ ist dann $[m]$ ein Nullteiler, also nicht invertiebar.

„$\Longleftarrow$“: Nach dem Lemma von Bezout existieren $r,s \in \mathbb{Z}$ mit $rm+sn = 1$. Dann gilt $[r][m] = [1] \in \mathbb{Z}/n\mathbb{Z}$, also ist $[r]$ invertierbar.

(ii) Nach (i) ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Integritätsbereich, wenn $1,\ldots,n-1$ teilerfremd zu n sind. Dies bedeutet aber gerade, dass n keine nicht-trivialen Teiler besitzt und daher eine Primzahl ist. □

Der Beweis von (i) zeigt, dass das Inverse einer invertierbaren Restklasse mittels erweitertem euklidischen Algorithmus explizit bestimmt werden kann.

Beispiel 5.3.28. Wir invertieren $[3] \in \mathbb{Z}/17\mathbb{Z}$. Es gilt

$$\begin{array}{rcl} 17 & = & 5\cdot 3 + 2 \\ 3 & = & 1\cdot 2 + 1 \\ 2 & = & 2\cdot 1 + 0, \end{array}$$

und folglich $1 = 3 - 1\cdot 2$ und $2 = 17 - 5\cdot 3$. Einsetzen liefert

$$1 = 3 - 1\cdot 2 = 3 - 1\cdot(17 - 5\cdot 3) = (-1)\cdot 17 + 6\cdot 3.$$

Folglich ist $[3]^{-1} = [6]$.

[19.01.24]

Bemerkung 5.3.29. Ist R ein Integritätsbereich, so schränkt sich die Multiplikation zu einer Abbildung $M : (R \setminus \{0\}) \times (R \setminus \{0\}) \to R \setminus \{0\}$ ein, und $(R \setminus \{0\}, M, 1)$ ist ein Monoid.

Definition 5.3.30. Ein Integritätsbereich heißt ein *Körper*, wenn $(R \setminus \{0\}, M, 1)$ eine Gruppe ist.

Beispiel 5.3.31. $\mathbb{Q}$ und $\mathbb{R}$ sind Körper. $\mathbb{Z}$ ist ein Integritätsbereich, der kein Körper ist, da 2 nicht invertierbar ist.

Aus Lemma 5.3.21 folgt sofort:

Korollar 5.3.32. *Jeder endliche Integritätsbereich ist ein Körper.* □

Beispiel 5.3.33. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn $n = p$ eine Primzahl ist. In diesem Fall schreiben wir auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. (Das $\mathbb{F}$ steht für engl. „field“= dt. „Körper“.)

Die gesamte Lineare Algebra funktioniert für Vektorräume über einem beliebigen Körper $\mathbb{K}$, nicht nur für $\mathbb{Q}$- und $\mathbb{R}$-Vektorräume. Inbesondere funktioniert sie über den endlichen Körpern $\mathbb{F}_p$. Das hat zahlreiche Anwendungen z.B. in der Kombinatorik:

Beispiel 5.3.34 (Modellieren mit endlichen Vektorräumen)**.** Ist p eine Primzahl M eine beliebige Menge, so ist die Menge $\mathrm{Abb}(M, \mathbb{F}_p)$ ein $\mathbb{F}_p$-Vektorraum unter punktweiser Addition und Skalarmultiplikation. Solche Funktionenräume tauchen in verschiedenen Kontexten auf:

(i) Jede Teilmenge $N \subseteq M$ definiert eine Funktion $\chi_N : M \to \mathbb{F}_2$ durch

$$\chi_N(x) := \begin{cases} [1], & \text{falls } x \in N, \\ [0], & \text{falls } x \notin N \end{cases},$$

und wir erhalten so eine Bijektion

$$\mathscr{P}(M) \to \mathrm{Abb}(M, \mathbb{F}_2), \quad N \mapsto \chi_N.$$

Unter dieser Bijektion entspricht die Vektoraddition gerade der symmetrischen Differenz $N_1 \Delta N_2 := N_1 \setminus N_2 \cup N_2 \setminus N_1$. Die Potenzmenge einer beliebigen Menge ist also eine abelsche Gruppe unter symmetrischer Differenz und sogar ein $\mathbb{F}_2$-Vektorraum mit Skalarmultiplikation definiert durch $[0] \cdot N = \emptyset$ and $[1] \cdot N = N$.

(ii) Ist M eine Konfiguration von Objekten, die jeweils p verschiedene Zustände (nummeriert als $[0], \ldots, [p-1]$) annehmen können, so können wir uns eine Abbildung von M nach $\mathbb{F}_p$ als einen Zustand des Systems vorstellen. Für $p = 2$ könnten die Elemente von M z.B. Lampen sein, und [1] bedeutet Licht ein und [0] bedeutet Licht aus, oder die Elemente könnten elektronische Bauteile sein und [1] bedeutet Strom ein und [0] bedeutet Strom aus. Diese Art der Modellierung mittels endlicher Vektorräume spielt u.a. in der Informatik eine große Rolle.

Man kann jeden Integritätsbereich zu einem Körper erweitern; das haben Sie im Prinzip schon in der Schule gelernt:

Konstruktion 5.3.35 (Quotientenkörper)**.** Sei R ein Integritätsbereich und $S := R \setminus \{0\}$. Auf $R \times S$ definieren wir eine Relation $\sim$ durch

$$(r_1, s_1) \sim (r_2, s_2) : \Longleftrightarrow r_1 s_2 - r_2 s_1 = 0.$$

Dann ist $\sim$ eine Äquivalenzrelation, und wir schreiben $\frac{r}{s} := [(r,s)]$ für die Klasse von $(r,s) \in R \times S$. Wir definieren dann $Q(R) := (R \times S)/\sim$; falls $R = \mathbb{Z}$, so ist $Q(R)$ gerade die Menge der rationalen Zahlen. In der Schule haben Sie gelernt, wie man solche Zahlen addieren und multiplizieren kann, und man kann sich davon überzeugen, dass das ganz allgemein funktioniert: Auf $Q(R)$ definiert man die Addition und Multiplikation durch

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

und wie im Fall von $\mathbb{Q}$ rechnet man nach, dass $Q(R)$ ein Körper ist. Dieser heißt der *Quotientenkörper*[22] von R. Wir können R als Unterring von $Q(R)$ auffassen, indem wir $r \in R$ mit $\frac{r}{1} \in Q(R)$ identifizieren[23]. Daraus folgt nun, dass jeder Integritätsbereich isomorph zu einem Unterring eines Körpers ist. Umgekehrt ist jeder Unterring eines Körpers (und allgemeiner jeder Unterring eines Integritätsbereiches) ein Integritätsbereich.

Übung 5.3.36. Beweisen Sie sorgfältig alle in Konstruktion 5.3.35 gemachten Behauptungen!

Wir fassen zusammen:

Korollar 5.3.37. *Für einen kommutativen Ring R sind die folgenden Aussagen äquivalent:*

(i) *R ist ein Integritätsbereich.*

(ii) *R ist isomorph zu einem Unterring eines Körpers.*

(iii) *R ist linkskürzbar, d.h. für alle $a, b, c \in R$ mit $a \neq 0$ gilt $ab = ac \implies b = c$.*

Beweis. (i)⇔(ii) folgt aus Konstruktion 5.3.35 und (ii)⇔(iii) folgt aus Lemma 5.3.21.(i). □

Bemerkung 5.3.38 (Charakteristischer Unterring)**.** Ist R ein Ring, so ist

$$\chi_R : \mathbb{Z} \to R, \quad n \mapsto n \cdot 1$$

ein Ringhomomorphismus (Übung!), genannt der *charakteristische Homomorphimus* von R. Sein Bild R_0 heißt der *charakteristische Unterring* von R.

Nach Bemerkung 5.3.6 ist $\ker(\chi_R)$ ein Ideal von $\mathbb{Z}$, und mit Beispiel 5.3.7 folgt, dass $\ker(\chi_R) = n\mathbb{Z}$ für ein $n \in \mathbb{N} \cup \{0\}$. Wir nennen n die *Charakteristik* von R. Nach dem Homomorphiesatz gilt dann $R_0 \cong (\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$.

Satz 5.3.39 (Charakteristik eines Körpers)**.** *Sei $\mathbb{K}$ ein Körper. Dann gibt es zwei Möglichkeiten:*

(i) $\operatorname{char}(\mathbb{K}) = 0$*; in diesem Fall ist $\mathbb{K}$ unendlich und der charakteristische Unterring ist isomorph zu $\mathbb{Z}$.*

[22] Die Terminologie ist sehr unglücklich: Quotientenkörper haben nichts mit Quotientengruppen oder Quotientenringen zu tun!

[23] Formaler: Die Abbildung $\iota : R \to Q(R)$, $r \mapsto \frac{r}{1}$ ist ein injektiver Ringhomomorphismus und R ist isomorph zu seinem Bild unter ι.

(ii) $\operatorname{char}(\mathbb{K}) = p > 0$*; in diesem Fall ist* p *eine Primzahl und der charakteristische Unterring ist ein endlicher Körper isomorph zu* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Insbesondere ist die Charakteristik eines endlichen Körpers stets eine Primzahl, und jeder endliche Körper enthält einen Körper isomorph zu $\mathbb{F}_p$.

Beweis. Sei $n := \operatorname{char}(\mathbb{K})$ und sei $R_0 \cong \mathbb{Z}/n\mathbb{Z}$ der charakteristische Unterring. Ist $n = 1$, so ist $1 = 0$, aber das kann in einem Körper nicht passieren. Ist $n > 1$, aber keine Primzahl, so gibt es einen von 0 verschiedenen Nullteiler in $R_0 \cong \mathbb{Z}/n\mathbb{Z}$ und daher in $\mathbb{K}$, Widerspruch. Es muss daher entweder $n = 0$ gelten oder n eine Primzahl sein. Die weiteren Aussagen folgen dann aus der vorhergehenden Bemerkung. □

Im Fall von endlichen Körpern erhält man daraus die folgende Einschränkung an die mögliche Anzahl der Elemente:

Korollar 5.3.40. *Ist* $\mathbb{K}$ *ein endlicher Körper der Charakteristik* p*, so ist* $|\mathbb{K}| = p^n$ *für ein* $n \in \mathbb{N}$.

Beweis. $\mathbb{K}$ enthält einen Unterkörper $\mathbb{K}_0$ mit p Elementen. Dann ist $\mathbb{K}$ ein $\mathbb{K}_0$-Vektorraum bzgl. seiner Addition und der Skalarmultiplikation gegeben durch die Einschränkung

$$\mathbb{K}_0 \times \mathbb{K} \to \mathbb{K}, \quad (\lambda, \mu) = \lambda\mu$$

der Multiplikation von $\mathbb{K}$. Da $\mathbb{K}$ endlich ist, ist $\mathbb{K}$ insbesondere ein endlichdimensionaler $\mathbb{K}_0$-Vektorraum und daher $\mathbb{K} \cong \mathbb{K}_0^n$ für ein $n \in \mathbb{N} \cup \{0\}$. Es gilt dann $|\mathbb{K}| = |\mathbb{K}_0|^n = p^n$. Wegen $0 \neq 1$ gilt außerdem $|\mathbb{K}| \geq 2$, also $n \neq 0$. □

Es gibt also keine Körper mit 12 Elementen. Aus Satz 5.3.39 und Korollar 5.3.40 folgt sofort:

Korollar 5.3.41. *Ist* p *eine Primzahl und* $\mathbb{K}$ *ein Körper mit* $\mathbb{K} = p$*, so ist* $\mathbb{K} \cong \mathbb{F}_p$. □

In der Vorlesung EINFÜHRUNG IN DIE ALGEBRA UND ZAHLENTHEORIE werden Sie lernen, dass es zu jeder Primzahlpotenz p^n bis auf Isomorphie genau einen Körper mit p^n Elementen gibt. Wir werden im nächsten Abschnitt Beispiele für solche Körper sehen.

Zusammenfassung von Abschnitt 5.3

(1) Ringe sind Strukturen mit zwei Verknüpfungen (Addition und Multiplikation), die Zahlbereiche und/oder Funktionenmengen modellieren.

(2) Ringhomomorphismen zerlegen sich kanonisch in Epi-, Iso- und Monomorphismen. Insbesondere sind homomorphe Bilder eines Rings isomorph zu Quotienten dieses Rings nach einem Ideal.

(3) Integritätsbereiche und Körper sind spezielle Klassen von (kommutativen) Ringen, in denen Linksmultiplikation mit einem Nichtnullelement injektiv bzw. surjektiv ist. Integritätsbereiche lassen sich stets zu Körpern erweitern, und endliche Integritätsbereiche sind Körper.

(4) Restklassenringe sind wichtige Beispiele für endliche kommutative Ringe, und Resklassenringe modulo Primzahlen sind wichtige Beispiele für endliche Körper. In diesen Ringen lassen sich multiplikative Inverse mittels erweitertem euklidischem Algorithmus bestimmen.

(5) Jeder endliche Körper entält eine isomorphe Kopie eines Restklassenkörpers und ist daher von Primpotenzordnung.

5.4 Polynomringe und Algebren

Bemerkung 5.4.1 (Formal unendliche Summen)**.** Es sei R ein beliebiger Ring und es bezeichne $c_0(R)$ die Menge aller Folgen $(a_n)_{n\in\mathbb{N}\cup\{0\}}$ von Elemente von R, so dass $a_n = 0$ für alle bis auf endlich viele $n \in \mathbb{N}$ gilt. Ist $(a_n) \in c_0(R)$, so existiert ein $N \in \mathbb{N}$, so dass $a_n = 0$ für alle $n > N$; wir definieren dann

$$\sum_{n=0}^{\infty} a_n := \sum_{n=0}^{N} a_n$$

und nennen diesen Ausdruck eine *formal unendliche Summe*. Eine solche Summe ist offensichtlich wohldefiniert, d.h. unabhängig von der Wahl von N, und es gelten die Rechenregeln

$$\sum_{n=0}^{\infty} a_n + \sum_{n=0}^{\infty} b_n = \sum_{n=0}^{\infty} (a_n + b_n) \quad \text{und} \quad \left(\sum_{n=0}^{\infty} a_n\right) \cdot \left(\sum_{n=0}^{\infty} b_n\right) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_m b_n \tag{5.4.1}$$

Definition 5.4.2. Sei R ein kommutativer Ring und $a = (a_n) \in c_0(R)$. Dann heißt

$$f_a : R \to R, \quad x \mapsto \sum_{n=0}^{\infty} a_n x^n$$

die zu a *assoziierte Polynomfunktion*, und wir nennen a eine *Koeffizientenfolge* für f. Wir bezeichnen mit $\mathrm{Pol}(R)$ die Menge aller solcher Polynomfunktionen.

Beispiel 5.4.3 (Reelle Polynomfunktionen)**.** Aus der Schule sind sie bereits mit reellen Polynomfunktionen wie z.B. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + x$ vertraut. Ist f eine reelle Polynomfunktion und (a_n) eine Koeffizientenfolge für f, dann gilt

$$a_n = \frac{f^{(n)}(0)}{n!},$$

wobei $f^{(n)}$ die $n$te Ableitung von f bezeichnet. Die Koeffizientenfolge ist also durch f eindeutig bestimmt, d.h. die Abbildung

$$\mathrm{Pol} : c_0(\mathbb{R}) \to \mathrm{Pol}(\mathbb{R}), \quad a \mapsto f_a$$

ist bijektiv. Insbesondere stimmen zwei reelle Polynomfunktionen genau dann überein, wenn sie dieselben Koeffizienten haben.

Beispiel 5.4.4 (Polynomfunktionen über $\mathbb{F}_2$)**.** Wir betrachten die Folge $a = (0,1,1,0,0,\dots) \in c_0(F_2)$. Die zugehörige Polynomfunktion ist

$$f_a : \mathbb{F}_2 \to \mathbb{F}_2, \quad x \mapsto x + x^2.$$

Wegen $[1] \oplus [1]^2 = [0] = [0] \oplus [0]^2$ ist f die Nullfunktion! Die Koeffizientenfolge a definiert also dieselbe Polynomfunktion wie die Nullfolge, d.h. die Abbildung

$$\mathrm{Pol} : c_0(\mathbb{F}_2) \to \mathrm{Pol}(\mathbb{F}_2), \quad a \mapsto f_a$$

ist *nicht* injektiv.

Bemerkung 5.4.5 (Faltung)**.** Sind $a, b \in c_0(R)$, so gelten für alle $x \in R$ die Identitäten

$$f_a(x) + f_b(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n \quad \text{und} \quad f_a(x) f_b(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n.$$

Wir definieren daher auf $c_0(R)$ Verknüpfungen

$$a+b := (a_n + b_n), \quad -a := (-a_n) \quad \text{und} \quad a * b := \left(\sum_{k=0}^{n} a_k b_{n-k} \right),$$

und erhalten

$$f_a + f_b = f_{a+b}, \quad -f_a = f_{-a} \quad \text{und} \quad f_a f_b = f_{a*b}. \tag{5.4.2}$$

Aus diesen Identitäten folgt, dass Pol(R) ein Unterring von Abb(R,R) ist. Die Verknüpfung $*$ heißt die *Faltung* auf $c_0(R)$.

Bemerkung 5.4.6. Man kann nachrechnen, dass $(c_0(R), +, *, -, 0, 1)$ stets ein Ring ist - hierbei ist $0 = (0,0,0,\dots)$ die Nullfolge und $1 = (1,0,0,\dots)$. Das direkte Nachrechnen der Assoziativität der Faltung ist allerdings sehr mühsam. Definieren wir $X := (0,1,0,0,\dots)$, so gilt $X^2 = (0,0,1,0,\dots)$, $X^3 = (0,0,0,1,0,\dots)$ usw., und daher können wir eine beliebige Folge $a = (a_n) \in c_0(R)$ schreiben als

$$a = a_0 + a_1 X + a_2 X^2 + \dots$$

Wir nennen a dann auch das *formale Polynom* über R in der *Unbestimmten* X mit Koeffizienten $a_0, a_1, \dots$. Der Ring $R[X] := (c_0(R), +, *, -, 0, 1)$ heißt entsprechend der *Polynomring* in der Unbestimmten X über R. In diesem Ring kann man genauso rechnen, wie sie das aus der Schule von reellen Polynomfunktionen gewohnt sind, also z.B.

$$(a_0 + a_1 X + \dots) * (b_0 + b_1 X + \dots) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \dots$$

Nach Bemerkung 5.4.5 ist die Abbildung

$$\mathrm{Pol} : R[X] \to \mathrm{Pol}(R), \quad a \mapsto f_a$$

ein Epimorphismus von Ringen, und nach Beispiel 5.4.4 ist dieser im Allgemeinen nicht injektiv. Ein formales Polynom enthält also im Allgemeinen mehr Informationen als die zugehörige Polynomfunktion!

Notation 5.4.7. Ist $a \in R[X]$ ein formales Polynom und $x \in R$ so schreiben wir häufig einfach $a(x) := \mathrm{Pol}(a)(x)$. Mit dieser Notation gilt dann gerade

$$(a_0 + a_1 X + \dots)(x) = a_0 + a_1 x + \dots,$$

d.h. wir werten ein formales Polynom $f \in R[X]$ an einer Stelle $x \in R$ aus, indem wir x für die Unbestimmte X einsetzen.

Da die Ringe $\mathbb{R}[X]$ und Pol($\mathbb{R}$) via Pol isomorph sind, spielt es über $\mathbb{R}$ keine Rolle, ob man mit formalen Polynomen oder mit Polynomfunktionen arbeitet. Über allgemeineren Ringen und Körpern R ist es meist vorteilhaft, mit formalen Polynomen zu arbeiten, da der Ring $R[X]$ häufig bessere Eigenschaften besitzt als der Ring Pol(R). Das wollen wir nun näher erläutern:

Bemerkung 5.4.8 (Grad und Leitkoeffizient)**.** Es sei R ein kommutativer Ring und $a \in R[X]$. Falls $a = 0$, so definieren wir den *Grad* von a als[24] $\deg(a) := -\infty$. Andernfalls existiert ein $n \in \mathbb{N} \cup \{0\}$ mit $a_n \neq 0$, und wir definieren $\deg(a) := \max\{n \in \mathbb{N}_0 \mid a_n \neq 0\}$, so dass

$$a = a_0 + a_1 X + \dots + a_{\deg(a)} X^{\deg(a)}.$$

[24] deg von engl. „degree“= dt. „Grad“

Wir nennen dann $a_{\deg}(a) \in R \setminus \{0\}$ den *Leitkoeffizienten* von a. Für $f, g \in R[X]$ gilt dann offensichtlich

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\} \quad \text{und} \quad \deg(f * g) \leq \deg(f) + \deg(g),$$

wobei nach Konvention $-\infty < n$ und $-\infty + n = n + (-\infty) = -\infty$ für alle $n \in \mathbb{N}_0$ gilt.

Ist R ein Integritätsbereich, so gilt sogar $\deg(f * g) = \deg(f) + \deg(g)$, und der Leitkoeffizient von $f * g$ ist das Produkt der Leitkoeffizienten von f und g.

Wir sehen nun einen ersten Vorteil des Rings $R[X]$ gegenüber dem Ring $\mathrm{Pol}(R)$:

Proposition 5.4.9. *Ist R ein Integritätsbereich, so auch $R[X]$. Der Ring $\mathrm{Pol}(R)$ muss hingegen kein Integritätsbereich sein.*

Beweis. Sind $f, g \in R[X] \setminus \{0\}$, so gilt $\deg(f) \geq 0$ und $\deg(g) \geq 0$ und daher $\deg(f * g) = \deg(f) + \deg(g) \geq 0$ und daher $f * g \neq 0$. Dagegen gilt in $\mathbb{F}_2$ dass $x(x+1) = x^2 + x = 0$, und daher ist $f(x) = x$ ein nicht-trivialer Nullteiler in $\mathrm{Pol}(\mathbb{F}_2)$. □

Eine besonders starke Theorie lässt sich für Polynomringe über Körpern entwickeln; das liegt daran, dass es in solchen Ringen eine Teilbarkeitstheorie gibt, die der Teilbarkeitstheorie in den ganzen Zahlen vergleichbar ist.

Ab jetzt sei $\mathbb{K}$ ein Körper.

Lemma 5.4.10 (Polynomdivision mit Rest)**.** *Ist $\mathbb{K}$ ein Körper und sind $f, g \in \mathbb{K}[X]$ Polynome mit $g \neq 0$, so gibt es $q, r \in \mathbb{K}[X]$ mit*

$$f = q * g + r \quad \text{und} \quad \deg(r) < \deg(g).$$

Beispiel 5.4.11. Für reelle Polynome (bzw. Polynomfunktionen) haben Sie Polynomdivision mit Rest bereits in der Schule gesehen, wir erinnern hier aber zur Sicherheit nochmal daran: Es seien $f = 5X^5 + 4X^4 + 3X^3 + 1$ und $g = 4X^4 + 4$ in $\mathbb{R}[X]$. Es gilt dann $5/4X * (4X^4 + 4) = 5X^5 + 5X$, und ziehen wir dieses Polynom von f ab, so erhalten wir ein Polynom von kleinerem Grad. Indem wir ein weiteres Vielfache von g abziehen, können wir den Grad der Differenz weiter reduzieren. Schematisch sieht das ganze so aus:

$$\begin{array}{rccccccccccl}
 & (& 5X^5 & + & 4X^4 & + & 3X^3 & & & + & 1 &) & \\
- & (& 5X^5 & & & & & + & 5X & & &) & \leftarrow \quad -5/4X * (4X^4+4) \\
\hline
 & (& & & 4X^4 & + & 3X^3 & - & 5X & + & 1 &) & \\
- & (& & & 4X^4 & & & & & + & 4 &) & \leftarrow \quad -1 * (4X^4+4) \\
\hline
 & & & & & & 3X^3 & - & 5X & - & 3 & &
\end{array}$$

also

$$5X^5 + 4X^4 + 3X^3 + 1 = (5/4X + 1) * (4X^4 + 4) + (3X^3 - 5X - 3),$$

wobei der Rest $3X^3 - X - 3$ echt kleineren Grad hat als der Divisor $X^4 + 1$.

Beweis von Lemma 5.4.10. Man geht genau wie im reellen Fall vor: Ist $\deg f = n \geq \deg g = m$ mit Leitkoeffizienten a_n und b_m, so ist $f^{(1)} := f - \frac{a_n}{b_m} X^{n-m} * g$ ein Polynom mit $\deg(f^{(1)}) < \deg(f)$. Wendet man dasselbe Verfahren auf $f^{(1)}$ an, so kann man den Grad durch Subtraktion von Vielfachen von g weiter reduzieren. Man erhält so eine Folge $f, f^{(1)}, f^{(2)}, \ldots$ von Polynomen von strikt fallendem Grad, und man subtrahiert so lange weiter, bis der Rest $f^{(k)}$ einen kleineren Grad hat als g. □

[24.01.24]

Da es im Polynomring $\mathbb{K}[X]$ genau wie in den natürlichen Zahlen eine Division mit Rest gibt, lassen sich weite Teile der Strukturtheorie von $\mathbb{Z}$ auf Polynomringe übertragen. Einige Begriffe müssen wir dazu etwas anpassen:

Bemerkung 5.4.12 (Teilbarkeit)**.** Sind $f,g,h \in \mathbb{K}[X]$ mit $f * g = h$, so nennen wir h ein *Vielfaches* von f und f einen *Teiler* von h, geschrieben $f|h$. Ein Teiler vom Grad 1 heißt ein *Linearfaktor*. Falls $f|h$ und $h|f$, so gilt $\deg f \le \deg h \le \deg f$, also $\deg f = \deg h$, und daher $\deg(f/h) = 0$. Das bedeutet gerade, dass $h = \lambda f$ für ein $\lambda \in \mathbb{K}^\times$. Man sagt dann, f und h sind *assoziiert*.

Sind $f,g,h \in \mathbb{K}[X]$ mit $h|f$ und $h|g$, so heißt h ein *gemeinsamer Teiler* von f und g. Ist h von maximalem Grad unter allen gemeinsamen Teilern, so heißt h ein *größter gemeinsamer Teiler* (kurz: ggT). Beachte, dass dann auch jedes zu h assoziierte Polynom ein ggT ist.

Für jedes $h \in \mathbb{K}[X]$ gilt $h|h$, und ist f ein Polynom vom Grad 0, so gilt $f|h$; diese Teiler von h heißen auch die *trivialen Teiler*. Ein Polynom heißt *irreduzibel* in $\mathbb{K}[X]$, wenn es vom Grad ≥ 1 ist und keine nicht-trivialen Teiler besitzt. Irreduzible Polynome spielen in Polynomringen eine ähnliche Rolle wie Primzahlen in der Zahlentheorie.

Hier ist eine erste Anwendung der Division mit Rest, die Ihnen im Spezialfall $\mathbb{K} = \mathbb{R}$ vermutlich aus der Schule bekannt ist.

Proposition 5.4.13 (Nullstellen und Linearfaktoren)**.** *Sei $f \in \mathbb{K}[X]$ und $\alpha \in \mathbb{K}$. Dann gilt:*

$$f(\alpha) = 0 \quad \Longleftrightarrow \quad (X - \alpha) \mid f.$$

Beweis. „$\Longleftarrow$“: Ist $f = (X-\alpha) * g$, so ist $f(\alpha) = (\alpha - \alpha) \cdot g(\alpha) = 0$.

„$\Longrightarrow$“: Sei α eine Nullstelle von f; wir dividieren f mir Rest durch $X - \alpha$:

$$f = g * (X - \alpha) + r \quad \text{mit } \deg(r) < \deg(X - \alpha) = 1.$$

Wegen $\deg(r) < 1$ gilt $r = \lambda \in \mathbb{K}$. Weiterhin gilt

$$0 = f(\alpha) = g(\alpha) \cdot (\alpha - \alpha) + r(\alpha) = 0 + \lambda,$$

also $r = \lambda = 0$. Dies zeigt, dass $f = (X - \alpha) * g$, also ist $(X - \alpha)$ ein Teiler von f. □

Korollar 5.4.14. *Ist $f \in \mathbb{K}[X] \setminus \{0\}$, so hat f höchstens $\deg(f)$ verschiedene Nullstellen.*

Beweis. Dies folgt aus Proposition 5.4.13 und der Tatsache, dass Division durch einen Linearfaktor den Grad eines Polynoms um 1 reduziert. □

Korollar 5.4.15. *Die Abbildung $\mathrm{Pol} : \mathbb{K}[X] \to \mathrm{Pol}(\mathbb{K})$ ist genau dann ein Isomorphismus, wenn der Körper $\mathbb{K}$ unendlich ist.*

Beweis. Es sei $f \in \mathbb{K}[X] \setminus \{0\}$. Dann gilt $f \in \ker(\Phi)$ genau dann, wenn jedes $\alpha \in \mathbb{K}$ eine Nullstelle von f ist. Ist $\mathbb{K}$ unendlich, so ist das nach Korollar 5.4.14 nicht möglich, also ist $\ker(\mathrm{Pol}) = \{0\}$. Ist hingegen $\mathbb{K}$ endlich, so liegt $\prod_{\alpha \in \mathbb{K}} (X - \alpha)$ im Kern von Pol. □

Die Unterscheidung zwischen formalen Polynomen und Polynomfunktionen ist also nur über endlichen Körpern relevant.

Korollar 5.4.16. *Sei $f \in \mathbb{K}[X]$ ein Polynom vom Grad 2 oder 3. Dann ist f genau dann irreduzibel in $\mathbb{K}[X]$, wenn f keine Nullstelle in $\mathbb{K}$ besitzt.*

Beweis. Wir haben bereits gesehen, dass f reduzibel ist, wenn f eine Nullstelle besitzt. Sei umgekehrt f reduzibel, d.h. $f = g * h$ mit Polynomen g und h vom Grad ≥ 1. Wegen

$$\deg(g) + \deg(h) = \deg(f) \leq 3$$

ist dann aber mindestens einer der beiden Grade von g und h gleich 1, d.h. f hat einen Linearfaktor und folglich eine Nullstelle. □

Beispiel 5.4.17. (i) Das Polynom $X^2+1 \in \mathbb{R}[X]$ hat keine Nullstelle, denn -1 ist kein Quadrat in $\mathbb{R}$. (Da $\mathbb{R}$ ein angeordneter Körper ist, ist jedes Quadrat nicht-negativ.) Folglich ist X^2+1 ein irreduzibles Polynom über $\mathbb{R}$.

(ii) Das Polynom $X^2 + X + [1] \in \mathbb{F}_2[X]$ ist irreduzibel, denn für $\alpha \in \mathbb{F}_2$ gilt $\alpha^2 + \alpha = 0$ und folglich $\alpha^2 + \alpha + [1] = [1] \neq [0]$.

(iii) Man beachte: Das Polynom $(X^2+1)^2 \in \mathbb{R}[X]$ hat keine Nullstelle (da X^2+1 keine hat), ist aber *nicht* irreduzibel, da es offensichtlich ein Produkt von zwei Polynomen vom Grad 2 ist. Korollar 5.4.16 gilt also im Grad 4 nicht mehr.

Bemerkung 5.4.18 (Erweiterter euklidischer Algorithmus für Polynome)**.** Wir betrachten die Polynome $f = X^5 + X^4 + X^3 + 1$ und $g = X^4 + 1$ in $\mathbb{F}_2[X]$. Wiederholte Division mit Rest liefert

$$\begin{aligned}(X^5 + X^4 + X^3 + 1) &= (X+1)\cdot(X^4+1) + (X^3+X)\\ (X^4+1) &= X\cdot(X^3+X) + (X^2+1)\\ (X^3+X) &= X\cdot(X^2+1) + 0.\end{aligned}$$

Wie im Fall von natürlichen Zahlen sieht man durch Lesen von unten nach oben, dass X^2+1 ein gemeinsamer Teiler von f und g ist. Ist umgekehrt h ein Teiler von f und g, so sieht man durch Lesen von oben nach unten, dass h ein Teiler von X^2+1 ist. Daher ist X^2+1 ein ggT von f und g. Weiter gilt in $\mathbb{F}_2[X]$, dass

$$\begin{aligned}X^2+1 &= (X^4+1) - X\cdot(X^3+X)\\ &= (X^4+1) - X\cdot((X^5+X^4+X^3+1) - (X+1)\cdot(X^4+1))\\ &= X\cdot(X^5+X^4+X^3+1) + (X^2+X+1)\cdot(X^4+1).\end{aligned}$$

Der erweiterte euklidische Algorithmus funktioniert in beliebigen Polynomringen über Körpern und liefert die folgenden Resultate:

Proposition 5.4.19. *Ist $h \in \mathbb{K}[X]$ ein ggT von $f, g \in \mathbb{K}[X]$, so ist jeder gemeinsame Teiler von f und g ein Teiler von h. Insbesondere ist h bis auf Assoziiertheit eindeutig.* □

Lemma 5.4.20 (Lemma von Bezout für Polynome)**.** *Sind $f, g \in \mathbb{K}[X]$ und ist h ein ggT von f und g, so existieren $r, s \in \mathbb{K}[X]$, so dass $h = r * f + s * g$.* □

Aus dem Ring der ganzen Zahlen haben wir durch Quotientenbildung die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ gewonnen. Wie überlegen uns nun, wie Quotientenringe von Polynomringen aussehen. Dies wird wichtige neue Beispiele für Körper liefern.

Beispiel 5.4.21. Ist R ein beliebiger kommutativer Ring und $s \in R$, so ist die Menge $(s) := \{rs \mid r \in R\}$ de Vielfachen von s ein Ideal in R, genannt das von s erzeugte *Hauptideal*. Jedes Polynom $f \in \mathbb{K}[X]$ definiert also ein Ideal $(f) \trianglelefteq \mathbb{K}[X]$. Unter Verwendung der Division mit Rest kann man zeigen, dass dies schon alle Ideale sind.

Lemma 5.4.22. *Jedes Ideal von $\mathbb{K}[X]$ ist ein Hauptideal.*

Der Beweis funktioniert genauso wie der Beweis, dass alle Ideale in $\mathbb{Z}$ Hauptideale sind.

Beweis. Sei $I \trianglelefteq R$. Ist $I = \{0\} = (0)$, so sind wir fertig. Andernfalls wähle ein $f \in I \setminus \{0\}$ von minimalem Grad. Da I ein Ideal ist, gilt dann $(f) \subseteq I$. Ist umgekehrt $g \in I$, so gilt $g = q * f + r$ für $q, r \in R$ mit $\deg(r) < \deg(f)$, und

$$r = g - q * f \in I.$$

Da f von minimalem Grad in $I \setminus \{0\}$ war, folgt $r = 0$, also $f \mid g$ und daher $g \in (f)$, also $I \subseteq (f)$. □

Wir haben gesehen, dass der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper ist, wenn n eine Primzahl ist. Der gleiche Beweis zeigt:

Satz 5.4.23 (Körper aus Polynomringen)**.** *Ist $f \in \mathbb{K}[X]$ mit $\deg(f) \geq 1$, so gilt*

$$\mathbb{K}[X]/(f) \textit{ ist ein Körper} \iff f \textit{ ist irreduzibel}.$$

Beweis. „$\Longrightarrow$“: Angenommen f ist nicht irreduzibel; dann existieren Polynome g, h vom Grad ≥ 1, so dass $f = gh$. Dann ist $\deg(g) < \deg(f)$ und $\deg(h) < \deg(f)$, also $f \nmid g$ und $f \nmid h$, und folglich

$$[g] \neq 0 \neq [h] \text{ in } \mathbb{K}[X]/(f), \quad \text{aber} \quad [g][h] = [f] = 0 \text{ in } \mathbb{K}[X]/(f).$$

Folglich hat $\mathbb{K}[X]/(f)$ Nullteiler und ist daher kein Integritätsbereich, insbesondere kein Körper.

„$\Longleftarrow$“: Sei f irreduzibel, $S := \mathbb{K}[X]/(f)$ und $\alpha \in S \setminus \{0\}$. Dann gilt $\alpha = [g]$ für ein g mit $f \nmid g$, also $g \notin (f)$. Da f irreduzibel ist, sind die einzigen Teiler von f die Polynome vom Grad 0 und f selbst. Wegen $f \nmid g$ ist aber f kein gemeinsamer Teiler von f und g, also ist 1 ein ggT von f und g. Nach Lemma 5.4.20 existieren dann Polynome m und n mit

$$m * f + n * g = 1 \quad \Longrightarrow \quad [m][f] + [n][g] = [1] \quad \Longrightarrow \quad [n] \cdot \alpha = [1].$$

Folglich ist α invertierbar. □

Konstruktion 5.4.24 (Kronecker-Erweiterung)**.** Es sei $f \in \mathbb{K}[X]$ mit $n := \deg(f) \geq 1$, etwa

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

Wir können $\mathbb{K}$ mit den Polynomen vom Grad ≤ 0 in $\mathbb{K}[X]$ identifizeren und erhalten einen Ringhomoorphismus

$$\iota : \mathbb{K} \to \mathbb{K}[X]/(f), \quad \lambda \mapsto [\lambda].$$

Dieser ist injektiv, denn ist $\lambda \in \ker(\iota)$, so ist λ ein Vielfaches von f. Wegen $\deg(\lambda) < \deg(f)$ ist das nur möglich, wenn $\lambda = 0$. Wir können daher $\mathbb{K}$ mit der Teilmenge $\iota(\mathbb{K})$ von $\mathbb{K}[X]/(f)$ identifizieren. Im Folgenden werden wir nicht zwischen $\mathbb{K}$ und $\iota(\mathbb{K})$ unterscheiden, da diese isomorph sind.

Ab jetzt sei f irreduzibel. Dann ist $\mathbb{L} := \mathbb{K}[X]/(f)$ ein Körper, der $\mathbb{K}$ als Unterkörper enthält. Insbesondere können wir Elemente von $\mathbb{K}$ mit Elementen von $\mathbb{L}$ multiplizieren und daher $\mathbb{L}$ als $\mathbb{K}$-Vektorraum auffassen. Man nennt $\mathbb{L}$ die *Kronecker-Erweiterung* von $\mathbb{K}$ zum Polynom f.

Wie können wir uns die Elemente von $\mathbb{L}$ vorstellen? Es sei $\alpha := [X] \in \mathbb{L}$ die Klasse von $X \in \mathbb{K}[X]$. Dann enthält $\mathbb{L}$ die Elemente von $\mathbb{K}$ sowie zusätzlich die Potenzen α, α^2, ... von α, sowie deren Produkte und Summen. Welche Rechenregeln gelten nun in $\mathbb{L}$ für diese Elemente (neben den aus $\mathbb{K}$ bekannten)? Die wichtigste Rechenregel ist, dass

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = [a_0 + a_1X + \cdots + a_nX^n] = [f(X)] = 0.$$

Fassen wir f also als Element von $\mathbb{L}[X]$ auf, so gilt gerade

$$f(\alpha) = 0.$$

Wir haben also zu $\mathbb{K}$ eine Nullstelle von f hinzugefügt! Falls $\deg f \geq 2$, so hatte f in $\mathbb{K}$ keine Nullstelle (da es irreduzibel war und daher keinen Linearfaktor haben kann), aber im größeren Körper $\mathbb{L}$ hat f eine Nullstelle. Wir können dann α^n als Linearkombination von $1, \alpha, \ldots, \alpha^{n-1}$ schreiben, denn

$$\alpha^n = -\frac{a_0}{a_n} - \frac{a_1}{a_n}\alpha - \cdots - \frac{a_{n-1}}{a_n}\alpha^{n-1}.$$

Dann können wir aber auch $\alpha^{n+1} = \alpha\alpha^n$ als Linearkombination von $\alpha, \ldots, \alpha^n$ und daher von $1, \alpha, \ldots, \alpha^{n-1}$ schreiben usw. Wir sehen daher, dass jedes Element von $\mathbb{L}$ von der Form

$$x = \lambda_0 + \lambda_1\alpha + \cdots + \lambda_{n-1}\alpha^{n-1} \quad \text{mit } \lambda_0, \ldots, \lambda_{n-1} \in \mathbb{K}$$

ist. Zwei solche Elemente addiert und multipliziert man wie Polynome in α, wobei man Potenzen der Form α^k mit $k \geq n$ wieder in kleinere Potenzen von α umschreiben kann.

Übung 5.4.25. Sei $f \in \mathbb{K}[X]$ irreduzibel vom Grad $n \geq 1$. Zeigen Sie, dass $1, \ldots, \alpha^{n-1}$ eine Basis des $\mathbb{K}$-Vektorraums $\mathbb{L} = \mathbb{K}[X]/(f)$ ist.

Beispiel 5.4.26 (Ein Körper mit 4 Elementen)**.** Gibt es einen Körper mit 4 Elementen? Der Ring $\mathbb{Z}/4\mathbb{Z}$ ist es jedenfalls nicht! Gibt es vielleicht einen anderen Weg einen solchen Körper zu konstruieren? Nach Beispiel 5.4.17.(ii) ist $X^2 + X + [1] \in \mathbb{F}_2[X]$ irreduzibel, wir erhalten also eine Kronecker-Erweiterung

$$\mathbb{L} := \mathbb{F}_2[X]/(X^2 + X + [1]).$$

Nach Konstruktion 5.4.24 hat $\mathbb{L}$ die vier Elemente

$$0 = [0], \quad 1 = [1], \quad \alpha := [X] \quad \text{und} \quad \beta := 1 + \alpha = [X + [1]].$$

Es gilt dann $\alpha^2 + \alpha + 1 = 0$, also $\alpha^2 = \alpha + 1 = \beta$. Daraus folgt dann, dass

$$\alpha\beta = \alpha + \alpha^2 = \alpha + \beta = 1 \quad \text{und} \quad \beta^2 = (1 + \alpha)^2 = 1 + \alpha + \alpha + \beta = 1 + \beta = \alpha.$$

Die Addition und Multiplikation in $\mathbb{L}$ sind also durch die folgenden Tabellen gegeben:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Übung 5.4.27. Finden Sie einen Körper mit 9 Elementen! [Anleitung: Finden Sie ein Polynom vom Grad 2 über $\mathbb{F}_3$, dass keine Nullstelle besitzt und betrachten Sie die zugehörige Kronecker-Erweiterung.]

Beispiel 5.4.28 (Komplexe Zahlen)**.** Nach Beispiel 5.4.17.(i) ist $f = X^2 + 1 \in \mathbb{R}[X]$ irreduzibel. Die zugehörige Kronecker-Erweiterung $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$ heißt *Körper der komplexen Zahlen*. Es ist üblich, die Klasse $[X] \in \mathbb{C}$ mit i zu bezeichnen. Nach Konstruktion 5.4.24 sind Elemente von $\mathbb{C}$ von der Form

$$z = a + bi \quad \text{mit } a, b \in \mathbb{R}, \quad \text{wobei} \quad i^2 + 1 = 0, \quad \text{also} \quad i^2 = -1.$$

Man überlege sich, dass sich daraus die folgenden Rechenregeln für Addition und Multiplikation ergeben:

$$(a+bi)+(c+di) = (a+c)+(b+d)i \quad \text{und} \quad (a+bi)(c+di) = (ac-bd)+(ad+bc)i.$$

Bemerkung 5.4.29 (Historisch-philosophische Bemerkung)**.** Wir haben gerade eine formale Zahlbereichserweiterung der reellen Zahlen vorgenommen, so dass es in unserer Welt nun eine „Zahl“ i gibt, deren Quadrat negativ ist. Aber gibt es eine solche Zahl wirklich? Historisch gesehen war das in der Mathematik jahrhundertelang eine zentrale Debatte.

Als die Pythagoräer entdeckten, dass $\sqrt{2}$ keine rationale Zahl ist, hat das ihr Weltbild erschüttert. Prominente Vertreter haben argumentiert, dass es solche irrationalen Zahlen in der Realität gar nicht gibt - wie der Name „irrational“ ja bereits andeutet. Bei den komplexen Zahlen – der Name wurde von Gauß 1831 in seiner Schrift „*Theoria residuorum biquadraticorum*“ eingeführt, aber das Konzept geht bis ins 16. Jahrhundert zurück – war der Widerstand ebenso stark. Descartes nannte nicht-reelle komplexe Zahlen „imaginär“, und selbst Geistesgrößen wie Leibniz waren sich nicht sicher, ob solche Zahlen wirklich existieren.[25] Ob es irrationale oder imaginäre Zahlen wirklich gibt, ist eine Frage für die Philosophie. Die moderne Mathematik hat zu dieser Fragestellung eine extrem pragmatische Haltung gefunden, die sich vielleicht am besten so zusammenfassen lässt:

> Nur weil etwas nicht real ist, heißt das noch lange nicht, dass es nicht nützlich ist!

Es ist, wie wir noch sehen werden, einfach ungemein praktisch, die Existenz imaginierter Objekte zu postulieren, und solange diese konsistent mit der bisherigen Theorie sind, kennt die moderne Mathematik in dieser Hinsicht keine Hemmungen. Wir werden im Folgenden viele Beispiele für Schlussweisen sehen, in denen formal definierte Objekte herangezogen werden, um Aussagen über reale (?) Objekte zu beweisen (vgl. etwa Übung 5.4.33). Dieser formalistische Zugang zur Mathematik (in der mathematische Objekte rein formale Begriffsbildungen ohne einen konkreten Inhalt sind) hat zu Beginn des 20. Jahrhunderts die Geometrie (David Hilbert) und Algebra (Emmy Noether) revolutioniert, und dominiert heute fast alle Gebiete der Mathematik.

Wenn wir nun von der Frage absehen, ob Zahlbereicherweiterungen wie die komplexen Zahlen wirklich existieren, dann bleibt immer noch die Frage, warum solche Erweiterungen nützlich sind.

[25] Leibniz nannte solche Zahlen eine „feine und wunderbare Zuflucht des menschlichen Geistes, beinahe ein Zwitterwesen zwischen Sein und Nichtsein“.

Bemerkung 5.4.30 (Polynome zerlegen)**.** Da das Polynom $f = X^2 + 1 \in \mathbb{R}[X]$ irreduzibel ist, können wir es nicht sinnvoll weiter zerlegen. Fassen wir hingegen f als Polynom über den komplexen Zahlen auf, so besitzt f zwei Nullstellen i und $-i$ und eine entsprechende Zerlegung $f = (X - i)(X + i)$ in Linearfaktoren. Solche Zerlegungen sind beim Rechnen mit Polynomen – wie sie vielleicht aus der Schule wissen – extrem hilfreich.

Man könnte nun auf die Idee verfallen, dass man zu einem gegebenen Körper $\mathbb{K}$ durch iteratives Bilden von Kronecker-Erweiterungen solange immer mehr Elemente hinzufügt, bis jedes Polynom vom Grad ≥ 1 eine Nullstelle hat - dann könnte man in dem so konstruierten Körper jede beliebige Polynom vom Grad ≥ 1 in Linearfaktoren zerlegen! Das Problem an der Idee ist, dass man durch das Hinzufügen neuer Elemente auch wieder neue Polynome erschafft, so dass nicht klar ist, ob dieser Prozess jemals zum Ende kommt. In der Vorlesung ALGEBRA werden Sie sehen, dass in der Tat jeder Körper zu einem größeren Körper erweitert werden kann, in dem jedes Polynom vom Grad ≥ 1 eine Nullstelle hat. Einen solchen Körper bezeichnet man als *algebraisch abgeschlossen*.

Im Allgemeinen ist es schwer eine algebraisch abgeschlossene Körpererweiterung eines gegebenen Körpers konkret anzugeben – trotz umfangreicher Bemühungen verstehen die Mathematiker die kleinste algebraische abgeschlossene Körpererweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen bis heute nicht, und seine Untersuchung ist eines der schwierigsten Probleme der modernen Algebra und Zahlentheorie. Es gibt aber eine prominente Ausnahme:

Satz 5.4.31 (Fundamentalsatz der Algebra)**.** *$\mathbb{C}$ ist ein algebraisch abgeschlossener Körper. Insbesondere hat jede nicht-konstante polynomielle Gleichung über $\mathbb{C}$ eine Lösung, und jedes $f \in \mathbb{C}[X]$ mit $\deg(f) \geq 1$ ist ein Produkt von Polynomen vom Grad 1.*

Trotz des unglücklichen Namens ist dies ein Satz der Analysis. Man beweist ihn in einer Vorlesung über FUNKTIONENTHEORIE ohne größere Anstrengung. Es gibt mehr oder weniger algebraische Beweise, aber diese sind alle sehr künstlich, und wir werden den Satz hier nicht beweisen. Für die Zwecke der linearen Algebra brauchen wir ohnehin nur eine schwächere Aussage, die wir sofort beweisen können. Dazu führen wir die folgende Sprechweise ein: Ist $\mathbb{L}$ ein Körper und $\mathbb{K}$ ein Unterkörper von $\mathbb{L}$, so nennen wir $\mathbb{L}$ eine *Körpererweiterung* von $\mathbb{K}$. Wegen $\mathbb{K} \subseteq \mathbb{L}$ gilt dann auch $\mathbb{K}[X] \subseteq \mathbb{L}[X]$, d.h. wie können jedes Polynom über $\mathbb{K}$ als Polynom über $\mathbb{L}$ auffassen.

Proposition 5.4.32 (Satz von Kronecker, Schwache Form)**.** *Sei $\mathbb{K}$ ein Körper und $f \in \mathbb{K}[X]$ mit $\deg(f) \geq 1$. Dann existiert eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$ mit der Eigenschaft, dass f als Element von $\mathbb{L}[X]$ ein Produkt von Linearfaktoren ist.*

Beweis. Wir beweisen die Aussage durch vollständige Induktion nach $n := \deg(f)$. Falls $n = 1$, so ist nichts zu zeigen. Sei also $n \geq 2$. Wir unterscheiden zwei Fälle:

FALL 1: f IST IRREDUZIBEL.

In diesem Falls $\mathbb{L}_1 := \mathbb{K}[X]/(f)$ eine Körpererweiterung von $\mathbb{K}$, in der f eine Nullstelle α hat, also gilt $f = (X - \alpha)f_1$ für ein $f_1 \in \mathbb{L}_1[X]$ vom Grad $< n$. Nach Induktionsvoraussetzung existiert nun eine weitere Körpererweiterung $\mathbb{L}_2$ von $\mathbb{L}_1$, über der f_1, und folglich f, in Linearfaktoren zerfällt.

FALL 2: f IST NICHT IRREDUZIBEL.

In diesem Fall ist $f = f_1 f_2$ für Polynome $f_1, f_2 \in \mathbb{K}[X]$ vom Grad $< n$. Nach Induktionsvoraussetzung existiert dann eine endliche Körpererweiterung $\mathbb{L}_1$ von $\mathbb{K}$, über der f_1 in Linearfaktoren

zerfällt, und analog eine endliche Körpererweiterung $\mathbb{L}_2$ von $\mathbb{L}_1$, über der f_2 in Linearfaktoren zerfällt. Folglich zerfällt auch f über $\mathbb{L}_2$ in Linearfaktoren. □

Im Fall von $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ können wir nach dem Fundamentalsatz der Algebra stets $\mathbb{L} = \mathbb{C}$ wählen. Ist hingegen $\mathbb{K}$ ein endlicher Körper, so muss man sich zur Angabe eines konkreten Modells für $\mathbb{L}$ durch mehrere Kronecker-Erweiterungen quälen. Zum Glück reicht es uns häufig aus zu wissen, dass ein Körper $\mathbb{L}$ wie im Satz von Kronecker existiert, wir müssen diesen nicht unbedingt angeben.

Übung 5.4.33. Sei $f \in \mathbb{R}[X]$ vom Grad $n \geq 1$. Zeigen Sie, dass f als Produkt von Polynomen vom Grad 1 und 2 geschrieben werden kann, indem Sie wie folgt vorgehen.

(i) Zeigen Sie, dass $f = \lambda(X - z_1)\cdots(X - z_n)$ mit $\lambda \in \mathbb{R}$ und $z_1, \ldots, z_n \in \mathbb{C}$. [Benutzen Sie den Fundamentalsatz der Algebra.]

(ii) Zeigen Sie: Ist $z_j \notin \mathbb{R}$, so existiert ein $k \in \{1, \ldots, n\}$ mit $z_j = \overline{z_k}$, wobei $\overline{a + bi} := a - bi$.

(iii) Zeigen Sie, dass $(X - z)(X - \overline{z}) \in \mathbb{R}[X]$ für alle $z \in \mathbb{C}$, und folgern Sie damit die Aussage über reelle Polynome.

[24.01.24]

Zum Abschluss dieses Kapitels kommen wir nun endlich zu den algebraischen Strukturen, die uns in der Linearen Algebra am meisten interessieren.

Definition 5.4.34. Es sei $\mathscr{A}$ eine Menge mit zwei Verknüpfungen + und $\circ$ und einer externen Verknüpfung $\mathbb{K} \times \mathscr{A} \to \mathscr{A}$, $(\lambda, A) \mapsto \lambda A$. Weiter sei $- : \mathscr{A} \to \mathscr{A}$ und $0,1 \in \mathscr{A}$. Dann heißt $(\mathscr{A}, +, \circ, \cdot, -, 0, 1)$ eine *assoziative* $\mathbb{K}$*-Algebra*, falls gilt:

(i) $(\mathscr{A}, +, \cdot)$ ist ein $\mathbb{K}$-Vektorraum mit Nullvektor 0.

(ii) $(\mathscr{A}, +, \circ, -, 0, 1)$ ist ein Ring.

(iii) Für jedes $x \in \mathscr{A}$ sind die Abbildungen $\mathscr{A} \to \mathscr{A}$, $y \mapsto x \circ y$ und $\mathscr{A} \to \mathscr{A}$, $y \mapsto y \circ x$ linear.

Eine $\mathbb{K}$-Algebra heißt *endlichdimensional*, falls $(\mathscr{A}, +, \cdot)$ endlichdimensional ist, und *kommutativ*, falls $(\mathscr{A}, +, \circ)$ kommutativ ist.

Beispiel 5.4.35. Für die Lineare Algebra gibt es vier fundamentale Beispiele von $\mathbb{K}$-Algebren

(i) Der Polynomring $\mathbb{K}[X]$ ist in natürlicher Weise eine kommutative assoziative $\mathbb{K}$-Algebr, denn man kann Polynome mit Skalaren auf die übliche Art multiplizieren, und die Multiplikation von Polynomen ist linear. Da $1, X, X^2, \ldots$ linear unabhängig sind, ist diese Algebra nicht endlich-dimensional.

(ii) Ist $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$, so ist $\mathbb{L}$ ein Ring, und definieren wir die Skalarmultiplikation $\mathbb{K} \times \mathbb{L} \to \mathbb{L}$ durch Einschränkung der Multiplikation auf $\mathbb{L}$, so wird $\mathbb{L}$ dadurch zu einer kommutativen assoziativen $\mathbb{K}$-Algebra. Diese kann endlichdimensional (z.B. $\mathbb{C}$ über $\mathbb{R}$ oder allgemeiner eine Kronecker-Erweiterung) oder unendlich-dimensional (z.B. $\mathbb{R}$ über $\mathbb{Q}$) sein.

(iii) Ist V ein $\mathbb{K}$-Vektorraum, so ist auch $\mathrm{End}_{\mathbb{K}}(V)$ ein $\mathbb{K}$-Vektorraum, und mit der Verkettung linearer Abbildungen sogar eine assoziative $\mathbb{K}$-Algebra. Diese ist nicht-kommutativ, falls $\dim_{\mathbb{K}}(V) > 1$, und genau dann endlich-dimensional, wenn V endlich-dimensional ist. Sie heißt die *allgemeine lineare Algebra* von V.

(iv) Für jedes $n \in \mathbb{N}$ bilden die quadratischen $(n \times n)$-Matrizen mit Matrizenmultiplikation und der üblichen Skalarmultiplikation und Addition eine $\mathbb{K}$-Algebra $\mathbb{K}^{n \times n}$, die $n$te *Matrizenalgebra* über $\mathbb{K}$.

Bemerkung 5.4.36 (Unteralgebren und Morphismen)**.** Wie üblich definieren wir Unterobjekte und Matrizen: Eine Teilmenge $\mathscr{B}$ einer assoziativen Algebra $\mathscr{A}$ heißt eine *Unteralgebra*, falls sie abgeschlossen unter Addition, interner und externer Multiplikation und Negation ist sowie 0 und 1 enthält. Unteralgebren der allgemeinen linearen Algebra bezeichnet man als *lineare Algebren*, und sie sind das Thema dieser Vorlesung.

Eine Abbildung $f : \mathscr{A} \to \mathscr{B}$ zwischen $\mathbb{K}$-Algebren ist ein Morphismus, falls

$$f(x+y) = f(x) + f(y), \quad f(\lambda x) = \lambda f(x), \quad f(x \circ y) = f(x) \circ f(y) \quad \text{und} \quad f(1) = 1 \quad (x, y \in \mathscr{A}, \lambda \in \mathbb{K}),$$

und das Bild eines solchen Morphismus ist wieder eine $\mathbb{K}$-Algebra. Der Kern $\ker(f) = \{a \in \mathscr{A} \mid f(a) = 0\}$ ist sowohl ein Ideal im Ring $\mathscr{A}$ als auch ein Untervektorraum des Vektorraums $\mathscr{A}$. Der

Quotient $\mathscr{A}/\ker(f)$ trägt daher sowohl eine Ringstruktur (als Quotientenring) als auch eine Vektorraumstruktur (als Quotientenvektorraum), und ist mit diesen selbst wieder eine $\mathbb{K}$-Algebra. Es gilt dann wie gewohnt der Homomorphiesatz

$$\mathrm{Bild}(f) \cong \mathscr{A}/\ker(f).$$

Wir betrachten einige wichtige Beispiele für Morphismen.

Beispiel 5.4.37 (Endomorphismen als Matrizen)**.** Ist V ein $\mathbb{K}$-Vektorraum der Dimension $n \in \mathbb{N}$ und $\mathscr{B}$ eine geordnete Basis von V, so ist die Abbildung

$$D_{\mathscr{B}} : \mathrm{End}_{\mathbb{K}}(V) \to \mathbb{K}^{n\times n}, \quad \Phi \mapsto D_{\mathscr{B}}(\Phi)$$

ein Isomorphismus. Dieser Isomorphismus zwischen der allgemeinen linearen Algebra eines endlichdimensionalen Vektorraums und einer Matrizenalgebra steht im Zentrum dieser Vorlesung, weil er es erlaubt abstrakte Probleme der linearen Algebra auf konkrete Probleme über Matrizen zu reduzieren, wobei alle relevanten Strukturen erhalten bleiben.

Beispiel 5.4.38 (Matrizenmodelle)**.** Es sei $\mathscr{A}$ eine endlichdimensionale(!) $\mathbb{K}$-Algebra. Wir definieren eine Abbildung

$$\ell : \mathscr{A} \to \mathrm{End}_{\mathbb{K}}(\mathscr{A}), \quad x \mapsto \ell_x, \quad \text{wobei} \quad \ell_x(y) := x \circ y.$$

Man rechnet leicht nach, dass ℓ ein Morphismus von $\mathbb{K}$-Algebren ist. Weiter gilt

$$x \in \ker(\ell) \implies \ell_x = 0 \implies \ell_x(1) = 0 \implies x = 0,$$

also ist ℓ injektiv und $\mathscr{A} \cong \ell(\mathscr{A}) \leq \mathrm{End}(\mathscr{A})$. Jede endlich-dimensionale $\mathbb{K}$-Algebra ist also (bis aus Isomorphie) linear! Wählen wir eine geordnete Basis $\mathscr{B}$ von $\mathscr{A}$ und setzen $n := \dim \mathscr{A}$, so erhalten wir einen Monomorphismus

$$\mathscr{A} \to \mathbb{K}^{n\times n}, \quad x \mapsto D_{\mathscr{B}}(\ell_x).$$

Das Bild eines solchen Monomorphismus bezeichnet man als *Matrizenmodell* für $\mathscr{A}$. Die Existenz solcher Modelle kann als Analogon zum Satz von Cayley für Gruppen gesehen werden: Jede abstrakte Algebra hat ein konkretes Modell.

Übung 5.4.39. Zeigen Sie, dass

$$\mathbb{C} \cong \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq \mathbb{R}^{2\times 2}.$$

Beispiel 5.4.40 (Einsetzungshomomorphismus)**.** Sei $\mathscr{A}$ eine $\mathbb{K}$-Algebra und $\alpha \in \mathscr{A}$. Für beliebige $a_0, \ldots, a_n \in \mathbb{K}$ ist dann der Ausdruck

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n \in \mathscr{A}$$

wohldefiniert. Das bedeutet aber gerade, dass wir Elemente von $\mathscr{A}$ (und nicht nur Elemente von $\mathbb{K}$) in Polynome über $\mathbb{K}$ einsetzen können! Beispielsweise können wir Matrizen oder komplexe Zahlen (oder sogar reelle Polynome...) in reelle Polynome einsetzen. Die Faltung ist gerade so definiert, dass die resultierende Abbildung

$$\mathrm{ev}_\alpha : \mathbb{K}[X] \to \mathscr{A}, \quad (a_0 + a_1X + \cdots + a_nX^n) \mapsto a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

ein Morphismus ist. Dieser heißt der *Einsetzungshomomorphismus*[26] an α. Wie im Fall von $\mathbb{K} = \mathscr{A}$ schreibt man kurz $f(\alpha) := \mathrm{ev}_\alpha(f)$.

[26] engl. „evaluation homomorphism“

Definition 5.4.41. Ist $\mathscr{A}$ eine $\mathbb{K}$-Algebra und $\alpha \in \mathscr{A}$, so heißt

$$\langle \alpha \rangle := \text{Bild}(\text{ev}_\alpha) = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in \mathbb{K}\}$$

die von α erzeugte *zyklische Algebra*.

Bemerkung 5.4.42 (Kern des Einsetzungshomomorphismus)**.** Ist $\mathscr{A}$ eine $\mathbb{K}$-Algebra und $\alpha \in \mathscr{A}$, so ist $\ker(\text{ev}_\alpha)$ ein Ideal in $\mathscr{A}$, und daher nach Lemma 5.4.22 ein Hauptideal. Wir finden also ein Polynom $\mu_\alpha \in \mathbb{K}$, so dass $\ker(\text{ev}_\alpha) = (\mu_\alpha)$. Das Polynom μ_α ist nicht eindeutig, aber eindeutig bis auf Assoziiertheit, denn ist μ'_α ein anderer Erzeuger des Kerns, so gilt $\mu_\alpha | \mu'_\alpha$ und $\mu'_\alpha | \mu_\alpha$. Falls $\mu_\alpha \neq 0$, so können wir den Leitkoeffizienten von μ_α auf 1 normieren, und dann ist μ_α eindeutig bestimmt. Ist die Algebra $\mathscr{A}$ endlichdimensional, so ist stets $\ker(\text{ev}_\alpha) \neq \{0\}$ (da $\mathbb{K}[X]$ unendlichdimensional ist), also ist $\mu_\alpha \neq 0$ für alle $\alpha \in \mathscr{A}$. Damit haben wir die folgende Proposition bewiesen.

Proposition 5.4.43. *Sei $\mathscr{A}$ eine endlichdimensionale assoziative $\mathbb{K}$-Algebra und $\alpha \in \mathscr{A}$. Dann existiert ein eindeutiges Polynom $\mu_\alpha \in \mathbb{K}[X] \setminus \{0\}$ mit den folgenden Eigenschaften:*

(M1) Der Leitkoeffizient von μ_α ist 1.

(M2) $\mu_\alpha(\alpha) = 0$.

(M3) Ist $f \in \mathbb{K}[X]$ mit $f(\alpha) = 0$, so gilt $\mu_\alpha \mid f$. □

Definition 5.4.44. Das Polynom μ_α aus Proposition 5.4.43 heißt das *Minimalpolynom* von α.

Als Spezialfall erhalten wir:

Korollar 5.4.45. *Sei $A \in \mathbb{K}^{n\times n}$. Dann existiert ein eindeutiges Polynom $\mu_A \in \mathbb{K}[X] \setminus \{0\}$ mit den folgenden Eigenschaften:*

(M1) Der Leitkoeffizient von μ_A ist 1.

(M2) $\mu_A(A) = 0$.

(M3) Ist $f \in \mathbb{K}[X]$ mit $f(A) = 0$, so gilt $\mu_A \mid f$. □

Zusammenfassung von Abschnitt 5.4

(1) Formale Polynome in einer Unbestimmten X über einem Körper (oder Integritätsbereich) $\mathbb{K}$ bilden selbst wieder einen Integritätsbereich $\mathbb{K}[X]$. Über einem unendlichen Körper können wir formale Polynome mit Polynomfunktionen identifizieren.

(2) In Polynomringen über Körpern gibt es eine Division mit Rest und daher ähnelt die Struktur von Polynomringen der Struktur von $\mathbb{Z}$ (erweiterter euklidischer Algorithmus, Ideale sind Hauptideale).

(3) Jedes Polynom in $\mathbb{K}[X]$ zerfällt über einer geeigneten Körpererweiterung von $\mathbb{K}$ in Linearfaktoren. Um solche Erweiterungen zu konstruieren, benutzt man die Kronecker-Konstruktion.

(4) In Polynome $f \in \mathbb{K}[X]$ kann man nicht nur Elemente von $\mathbb{K}$, sondern Elemente beliebiger $\mathbb{K}$-Algebren (z.B. Matrizen, Polynome, Körpererweiterungen, ...) einsetzen. Jedes solche Element wird von einem eindeutigen normierten Polynom von minimalem Grad, seinem sogenannten Minimalpolynom, annulliert.

6 Normalformen von Endomorphismen

6.1 Charakteristisches Polynom und Trigonalisierbarkeit

Wir haben in Abschnitt 4.5 gesehen, dass es sehr nützlich ist, wenn eine Matrix oder ein Endomorphismus diagonalisierbar sind. U.a. haben wir gesehen, wie wir mittels Diagonalisierung lineare Rekursionsgleichungen lösen, Pfade in Graphen zählen oder das Langzeitverhalten von Markov-Ketten bestimmen können. Mit den dort zur Verfügung stehenden Methoden konnten wir zwar die Diagonalisierbarkeit gewisser Matrizen/Endomorphismen nachprüfen, aber wir waren nicht in der Lage allgemeine Kriterien dafür zu geben, wann eine Matrix oder ein Endomorphismus diagonalisierbar ist. Dies wollen wir nun, als erste Anwendung der abstrakten Algebra, nachholen. Im Folgenden sei stets $\mathbb{K}$ ein Körper und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum.

Wir erinnern daran, dass die charakteristische Polynomfunktion χ_A einer Matrix $A \in \mathbb{K}^{n\times n}$ durch

$$\chi_A : \mathbb{K} \to \mathbb{K}, \quad \chi_A(x) := \det(x \cdot \mathbf{1} - A)$$

gegeben ist. Jetzt, da wir formal definiert haben, was Polynome sind, wollen wir uns als erstes einmal überlegen, warum das wirklich eine Polynomfunktion ist. Dazu brauchen wir die folgende Konstruktion:

Konstruktion 6.1.1 (Determinanten über Integritätsbereichen)**.** Sei R ein Integritätsbereich und $A \in R^{n\times n}$ eine quadratische Matrix mit Einträgen in R. Wir können R als Unterring eines Körpers $\mathbb{K}$ (z.B. des Quotientenkörpers $Q(R)$ von R) und A als eine Matrix in $\mathbb{K}^{n\times n}$ auffassen. Dann ist insbesondere die Determinante $\det(A) \in \mathbb{K}$ von A definiert. Da in der Leibnizformel bis auf Vorzeichen nur Summen von Produkten von Einträgen von A auftauchen und diese Einträge alle in R liegen, gilt dann sogar $\det(A) \in R$. Wir haben also eine wohldefinierte Abbildung $\det : R^{n\times n} \to R$.

WARNUNG ! Damit eine Matrix A über einem Integritätsbereich R invertierbar ist, reicht es nicht aus, dass $\det(A) \neq 0$ gilt. Vielmehr ist A genau dann invertierbar, wenn $\det(A)$ in R invertierbar ist. Der Beweis dieser Tatsache (mittels Cramerscher Regel) funktioniert genau wie der Beweis von Korollar 4.4.18.

Konstruktion 6.1.2 (Charakteristisches Polynom)**.** Ist $A \in \mathbb{K}^{n\times n}$ eine Matrix über einem Körper $\mathbb{K}$, dann ist $X \cdot \mathbf{1} - A \in \mathbb{K}[X]^{n\times n}$ eine Matrix über em Polynomring $\mathbb{K}[X]$. Da dieser ein Integritätsbereich ist, können wir nun das *charakteristische Polynom* von A als

$$\chi_A := \det(X \cdot \mathbf{1} - A) \in \mathbb{K}[X]$$

definieren. Nach Definition ist die zugehörige Polynomfunktion gerade die charakteristische Polynomfunktion, insbesondere sind die Eigenwerte von $\Phi_A : \mathbb{K} \to \mathbb{K}$ genau die Nullstellen von χ_A in $\mathbb{K}$. Aus der Leibnizformel folgt, dass $\deg(\chi_A) = n$ gilt und der Leitkoeffizient von χ_A durch 1 gegeben ist. Mit Korollar 5.4.14 folgt insbesondere, das A höchstens n verschiedene Eigenwerte haben kann.

Bemerkung 6.1.3 (Ähnlichkeitsinvarianz)**.** Wir erinnern daran, dass zwei Matrizen $A,B \in \mathbb{K}^{n\times n}$ *ähnlich* (über $\mathbb{K}$) sind, falls $B = SAS^{-1}$ für eine Matrix $S \in \mathrm{GL}_n(\mathbb{K})$ gilt. In diesem Fall gilt

$$\chi_B = \det(X\cdot\mathbf{1} - SAS^{-1}) = \det(S(X\cdot\mathbf{1}-A)S^{-1}) = \det(S)\det(X\cdot\mathbf{1}-A)\det(S)^{-1} = \chi_A.$$

Ist insbesondere Φ ein Endomorphismus eines n-dimensionalen $\mathbb{K}$-Vektorraums $\mathbb{K}^n$, so haben alle darstellenden Matrizen von Φ dasselbe charakteristische Polynom. Man bezeichnet dieses dann auch mit χ_Φ und nennt es das *charakteristische Polynom von* Φ .

Notation 6.1.4. Sind $A,B \in \mathbb{K}^{n\times n}$ ähnlich über $\mathbb{K}$, so schreiben wir im Folgenden kurz $A \sim_{\mathbb{K}} B$

Sind A und B reelle Matrizen, so können wir A und B auch als komplexe Matrizen auffassen. Es könnte dann passieren, dass $A \sim_{\mathbb{C}} B$, aber nicht $A \sim_{\mathbb{R}} B$ gilt. Mit Methoden, die ein wenig über diese Vorlesung hinausgehen[1], kann man beweisen, dass dies nicht der Fall ist.

Proposition 6.1.5 (Notwendige Bedingung für Diagonalisierbarkeit)**.** *Ist* $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *diagonalisierbar, so zerfällt* χ_Φ *in* $\mathbb{K}[X]$ *in Linearfaktoren. Genauer gilt*

$$\chi_\Phi(X) = (X-\lambda_1)\cdots(X-\lambda_n),$$

wobei $\{\lambda_1,\ldots,\lambda_n\}$ *die Menge der Eigenwerte von* Φ *ist.*

Beweis. Ist $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ diagonalisierbar und A eine darstellende Matrix von Φ, so gilt $A \sim_{\mathbb{K}} D = \mathrm{diag}(\lambda_1,\ldots,\lambda_n)$ für gewisse $\lambda_1,\ldots,\lambda_n$, und folglich

$$\chi_\Phi = \chi_A = \chi_D = \det(\mathrm{diag}(X-\lambda_1,\ldots,X-\lambda_n)) = (X-\lambda_1)\cdots(X-\lambda_n).$$

Die Nullstellen $\lambda_1,\ldots,\lambda_n$ von χ_Φ sind dann genau die Eigenwerte. □

Die Umkehrung von Proposition 6.1.5 gilt nicht. Es gibt nämlich sehr viele Matrizen, deren charakteristisches Polynom zerfällt:

Bemerkung 6.1.6 (Matrizen mit zerfallendem charakteristischen Polynom)**.** Es sei $A \in \mathbb{K}^{n\times n}$ eine obere Dreiecksmatrix der Form

$$A = \begin{pmatrix} \lambda_1 & * & \ldots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \ldots & 0 & \lambda_n \end{pmatrix}.$$

Dann gilt $\chi_A = \det(X\cdot\mathbf{1}-A) = (X-\lambda_1)\cdots(X-\lambda_n)$, also zerfällt das charakteristische Polynom von A. Im Allgemeinen ist A aber nicht diagonalisierbar: Ist z.B.

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

so ist 0 der einzige Eigenwert von A. Wäre A diagonalisierbar, so wäre also $A \sim \mathrm{diag}(0,0)$ und daher $A = 0$, Widerspruch.

[1] vgl. Theorem 4 in `https://kconrad.math.uconn.edu/blurbs/linmultialg/potdiagonalizable.pdf`

Definition 6.1.7. Eine Matrix $A \in \mathbb{K}^{n\times n}$ heißt *trigonalisierbar*, falls A (über $\mathbb{K}$) ähnlich zu einer oberen Dreiecksmatrix ist. Analog heißt $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *trigonalisierbar*, falls es eine geordnete Basis $\mathscr{B} = (v_1, \ldots, v_n)$ von V gibt, so dass $D_{\mathscr{B}}(\Phi)$ eine obere Dreiecksmatrix ist.

Bemerkung 6.1.8 (Trigonalisierbarkeit)**.** Die folgenden Aussagen ergeben sich sofort aus Bemerkung 6.1.6 und der Definition:

(i) $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ ist genau dann trigonalisierbar wenn eine (bzw. jede) darstellende Matrix $\mathbb{K}$-trigonalisierbar ist.

(ii) Gilt $A \sim_{\mathbb{K}} B$, so ist A genau dann trigonalisierbar, wenn B trigonalisierbar ist.

(iii) Das charakteristische Polynom eines trigonalisierbaren Endomorphismus bzw. einer trigonalisierbaren Matrix zerfällt im entsprechenden Polynomring in Linearfaktoren.

(iv) Jede diagonalisierbare Matrix bzw. jeder diagonalisierbare Endomorphismus ist trigonalisierbar, aber die Umkehrung gilt nicht.

Unser nächstes Ziel ist die folgende Umkehrung von Teil (iii) der Bemerkung:

Satz 6.1.9 (Trigonalisierbarkeitskriterium)**.** *$\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ ist genau dann trigonalisierbar, wenn χ_Φ in $\mathbb{K}[X]$ in Linearfaktoren zerfällt.*

Der Beweis von Satz 6.1.9 wird uns ein explizites Verfahren zum Auffinden einer geordneten Basis $\mathscr{B}$ liefern, bzgl. derer die darstellende Matrix von Φ obere Dreiecksform annimmt.

Bemerkung 6.1.10. Ist $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ und $\mathscr{B} = (v_1, \ldots, v_n)$ eine geordnete Basis von V, so sagen wir, dass $\mathscr{B}$ den Endomorphismus Φ trigonalisiert, wenn $D_{\mathscr{B}}\Phi$ eine obere Dreiecksmatrix ist. Dies bedeutet gerade, dass Elemente $a_{ij} \in \mathbb{K}$ (nämlich die Einträge von $D_{\mathscr{B}}(\Phi)$) existieren, so dass

$$\left\{\begin{array}{lcl} \Phi(v_1) &=& a_{11}v_1, \\ \Phi(v_2) &=& a_{22}v_2 + a_{12}v_1, \\ \Phi(v_3) &=& a_{33}v_3 + a_{23}v_2 + a_{13}v_1, \\ & \ldots, & \\ \Phi(v_n) &=& a_{nn}v_n + a_{(n-1)n}v_{n-1} + \cdots + a_{1n}v_1. \end{array}\right. \tag{6.1.1}$$

Nach Bemerkung 6.1.6 sind dann die Eigenwerte von Φ gegeben durch $\lambda_1 := a_{11}, \ldots, \lambda_n := a_{nn}$. Man beachte, dass einige dieser Eigenwerte übereinstimmen können. Der Vektor v_1 ist nach Definition gerade ein Eigenvektor von Φ zum Eigenwert λ_1. Es wäre schön, wenn die anderen v_k ebenfalls Eigenvektoren wären, denn dann könnte man sie leicht ausrechnen, aber das ist nicht der Fall: v_2 muss kein Eigenvektor zum Eigenwert λ_2 sein, sondern lediglich ein „Eigenvektor modulo $\mathbb{K}v_1$“. Diese Idee wollen wir nun präzisieren.

Definition 6.1.11. Sei $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$. Ein Unterraum $U \leq V$ heißt Φ-*invariant*, falls $\Phi(U) \subseteq U$.

Konstruktion 6.1.12 (Induzierter Endomorphism)**.** Es seien $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ und $U_1 < U_2 \leq V$ zwei Φ-invariante Unterräume. Wir nennen dann U_2/U_1 einen Φ-*invarianten Subquotienten* von V. Für alle $u_1 \in U_1$ und $u_2 \in U_2$ gilt dann

$$\Phi(u_1 + u_2) = \Phi(u_1) + \Phi(u_2) \in \Phi(u_2) + \Phi(U_1) \subseteq \Phi(u_2) + U_1,$$

und daher ist die Abbildung

$$\Phi_{U_2/U_1} : U_2/U_1 \to U_2/U_1, \quad u_2 + U_1 \mapsto \Phi(u_2) + U_1$$

wohldefiniert. Sie ist offensichtlich linear und heißt der *induzierte Endomorphismus* von Φ auf U_2/U_1. Speziell für $U_1 = \{0\}$ erhalten wir

$$\Phi_{U_2} : U_2 \to U_2, \quad u_2 \mapsto \Phi(u_2).$$

Beispiel 6.1.13. Es sei $\mathscr{B} = (v_1, \ldots, v_n)$ eine Basis, die $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ trigonalisiert. Wir definieren

$$U_0 := \{0\}, \quad U_1 := \langle v_1 \rangle, \quad U_2 := \langle v_1, v_2 \rangle, \quad \ldots, \quad U_n := \langle v_1, \ldots, v_n \rangle. \tag{6.1.2}$$

Dann sind $U_0, \ldots, U_n$ allesamt Φ-invariante Unterräume und in der Notation von Bemerkung 6.1.10 gilt:

- $\Phi_{V/U_0}(v_1) = \lambda_1 v_1$.
- $\Phi_{V/U_1}(v_2 + U_1) = \lambda_2(v_2 + U_1)$.
- $\Phi_{V/U_2}(v_3 + U_2) = \lambda_3(v_3 + U_2)$.

Die Vektoren $v_k + U_{k-1}$ sind also jeweils Eigenvektoren von Φ_{V/U_k}. Ist umgekehrt $v_k + U_{k-1}$ jeweils ein Eigenvektor von Φ_{V/U_k}, so bedeutet diese gerade, dass Elemente $a_{ij} \in \mathbb{K}$ gibt, die (6.1.1) erfüllen. Damit haben wir die folgende Aussage bewiesen.

Lemma 6.1.14. *Es seien $\mathscr{B} = (v_1, \ldots, v_n)$ eine geordnete Basis von V, $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ und $U_1, \ldots, U_{n-1}$ wie in* (6.1.2) *definiert. Dann wird Φ durch $\mathscr{B}$ genau dann trigonalisiert, wenn die folgenden Bedingungen erfüllt sind:*

- *v_1 ist ein Eigenvektor von Φ (und folglich ist U_1 invariant).*
- *v_2 ist ein Eigenvektor von Φ_{V/U_1} (und folglich ist U_2 invariant).*
- $\ldots$
- *v_n ist ein Eigenvektor von $\Phi_{V/U_{n-1}}$.* □

[31.01.24]

Konstruktion 6.1.15 (Darstellende Matrizen induzierter Endomorphismen)**.** Wir kann man sich induzierte Endomorphismen auf invarianten Subquotienten in Matrizensprache vorstellen? Im Allgemeinen ist das schwierig, aber wenn man geschickte Basen wählt, dann geht es!

Es seien also $U_1 < U_2 \leq V$ zwei Φ-invariante Unterräume. Wir wählen eine geordnete Basis $\mathscr{B}_1 = (v_1, \ldots, v_k)$ von U_1 und ergänzen diese zu einer geordneten Basis $\mathscr{B} = (v_1, \ldots, v_n)$ von U_2. Da U_1 und U_2 invariant sind, gibt es dann Elemente $a_{ij}, b_{ij}, c_{ij} \in \mathbb{K}$ mit

$$\begin{aligned}
\Phi(v_1) &= a_{11}v_1 + \cdots + a_{k1}v_k \\
&\cdots \\
\Phi(v_k) &= a_{1k}v_1 + \cdots + a_{kk}v_k \\
\Phi(v_{k+1}) &= b_{11}v_1 + \cdots + b_{k1}v_k + c_{11}v_{k+1} + \cdots + c_{(n-k)1}v_n \\
&\cdots \\
\Phi(v_n) &= b_{1(n-k)}v_1 + \cdots + b_{k(n-k)}v_k + c_{1(n-k)}v_{k+1} + \cdots + c_{(n-k)(n-k)}v_n,
\end{aligned}$$

also ist $D_{\mathscr{B}}(\Phi)$ von der Form

$$D_{\mathscr{B}}(\Phi_{U_2}) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \text{ mit } A = (a_{ij}) \in \mathbb{K}^{k\times k},\ B = (b_{ij}) \in \mathbb{K}^{k\times(n-k)},\ C = (c_{ij}) \in \mathbb{K}^{(n-k)\times(n-k)}.$$

Nach Definition ist $A = D_{\mathscr{B}_1}(\Phi_{U_1})$. Was ist mit den anderen Untermatrizen?

Wir überlegen uns zunächst, dass $\mathscr{B}_2 = (v_{k+1} + U_1, \ldots, v_n + U_1)$ eine geordnete Basis von U_2/U_1 ist. Ist nämlich $\pi : U_2 \to U_2/U_1$ die kanonische Projektion, so gilt $\pi[\{v_1, \ldots, v_n\}] = \{0 + U_1\} \cup \mathscr{B}_2$. Da π ein Epimorphismus ist (also Erzeugendensysteme auf Erzeugendensysteme abbildet), folgt sofort, dass $\mathscr{B}_2$ ein Erzeugendensystem von U_2/U_1. Wegen $\dim U_2/U_1 = \dim U_2 - \dim U_1 = n - k = |\mathscr{B}_2|$ folgt dann, dass $\mathscr{B}_2$ eine Basis ist.

Es gilt nun

$$\begin{aligned}
\Phi_{U_2/U_1}(v_{k+1} + U_1) &= c_{11}v_{k+1} + \cdots + c_{(n-k)1}v_n + U_1 \\
&\cdots \\
\Phi_{U_2/U_1}(v_n + U_1) &= c_{1(n-k)}v_{k+1} + \cdots + c_{(n-k)(n-k)}v_n + U_1,
\end{aligned}$$

also gilt $C = D_{\mathscr{B}_2}\Phi_{U_2/U_1}$. Damit haben wir gezeigt, dass

$$D_{\mathscr{B}}(\Phi_{U_2}) = \begin{pmatrix} D_{\mathscr{B}_1}(\Phi_{U_1}) & * \\ 0 & D_{\mathscr{B}_2}(\Phi_{U_2/U_1}) \end{pmatrix}. \tag{6.1.3}$$

Korollar 6.1.16. *Ist $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ und sind $U_1 < U_2 \leq V$ zwei Φ-invariante Unterräume, so gilt*

$$\chi_{\Phi_{U_2}} = \chi_{\Phi_{U_1}} * \chi_{\Phi_{U_2/U_1}}.$$

□

Die folgende Konstruktion liefert nun einen konstruktiven Beweis für Satz 6.1.9:

Konstruktion 6.1.17 (Konstruktion einer trigonalisierenden Basis)**.** Es sei $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$, dessen charakteristisches Polynom χ_Φ in Linearfaktoren zerfällt. Wir konstruieren eine geordnete Basis $\mathscr{B} = (v_1, \ldots, v_n)$ wie in Lemma 6.1.14:

SCHRITT 1: χ_Φ besitzt mindestens eine Nullstelle, also besitzt Φ einen Eigenwert λ_1 und daher einen Eigenvektor $v_1 \in V \setminus \{0\}$. Es gilt dann $\Phi(v_1) = \lambda_1 v_1$, und wir setzen $U_1 := \langle v_1 \rangle$. (Wenn man eine Nullstelle λ_1 von χ_Φ gefunden hat, kann man v_1 durch Lösen eines LGS bestimmen.)

SCHRITT 2: Falls $\dim V \geq 2$, so betrachten wir Φ_{V/U_1}. Nach Korollar 6.1.16 ist $\chi_{\Phi_{V/U_1}}$ ein Teiler von χ_{Φ_V} (vom Grad ≥ 1) und zerfällt daher in Linearfaktoren. Wir finden dann einen Eigenwert λ_2 und zugehörigen Eigenvektor $v_2 + U_1$. Es gilt dann

$$\Phi_{V/U_1}(v_2 + U_1) = \lambda_2 v_2 + U_1,$$

und wir setzen $U_2 := \langle v_1, v_2 \rangle$. (Wenn man eine Nullstelle λ_2 von $\chi_{\Phi_{V/U_1}}$ gefunden hat, kann man v_2 durch Lösen eines LGS bestimmen.)

SCHRITT 3: Falls $\dim V \geq 3$, so betrachten wir Φ_{V/U_2}. Nach Korollar 6.1.16 ist $\chi_{\Phi_{V/U_2}}$ ein Teiler von χ_{Φ_V} (vom Grad ≥ 1) und zerfällt daher in Linearfaktoren. Wir finden dann einen Eigenwert λ_3 und zugehörigen Eigenvektor $v_3 + U_2$. Es gilt dann

$$\Phi_{V/U_2}(v_3 + U_2) = \lambda_3 v_3 + U_2,$$

und wir setzen $U_3 := \langle v_1, v_2, v_3 \rangle$. (Wenn man eine Nullstelle λ_3 von $\chi_{\Phi_{V/U_3}}$ gefunden hat, kann man v_3 durch Lösen eines LGS bestimmen.)

...

Nach n Schritten haben wir dann eine Basis $\mathscr{B} = (v_1, \ldots, v_n)$ gefunden, die Φ trigonalisiert.

An dieser Stelle haben wir Satz 6.1.9 bewiesen. Der Algorithmus zur Bestimmung einer trigonalisierenden Basis aus Konstruktion 6.1.17 ist wenig effizient und von eher theoretischer Natur. Eine vollbesetzte (6×6)-Matrix mit diesem Algorithmus zu trigonalisieren macht keinen Spaß (und wird von Ihnen auch nicht verlangt). Sie sollten aber in der Lage sein, Ihren Computer dazu zu bringen, Ihnen eine trigonalisierende Basis zu berechnen.

Übung 6.1.18 (Trigonalisierbarkeit und Fahnen)**.** Wir erinnern daran, dass eine echt aufsteigende Folge $U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_l$ von Unterräumen von V eine *echte Fahne* der *Länge* l heisst (vgl. Übung 2.5.18). Wir nennen eine solche Fahne Φ-*invariant*, wenn $U_0, \ldots, U_l$ allesamt Φ-invariante Unterräume von V sind. Nach Übung 2.5.18 ist die Länge einer echten Fahne in V nach oben durch $\dim_{\mathbb{K}} V$ beschränkt. Wir nennen daher eine echte Fahne *maximal*, wenn sie von der Länge $l = \dim_{\mathbb{K}} V$ ist.

Zeigen Sie, dass ein Endomorphismus $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ genau dann trigonalisierbar, wenn er eine invariante maximale echte Fahne besitzt.

In Matrizensprache besagt Satz 6.1.9:

Korollar 6.1.19 (Trigonalisierbarkeit von Matrizen)**.** *Sei $A \in \mathbb{K}^{n \times n}$. Dann gilt $A \sim_{\mathbb{K}} B$ für eine obere Dreiecksmatrix $B \in \mathbb{K}^{n \times n}$ genau dann, wenn χ_A in $\mathbb{K}[X]$ in Linearfaktoren zerfällt.* □

Der Körper $\mathbb{K}$ spielt in dieser Aussage, eine wichtige Rolle: Ist $\mathbb{L}$ eine Körpererweiterung von $\mathbb{L}$, so kann es durchaus passieren, dass χ_A in $\mathbb{L}[X]$, aber nicht in $\mathbb{K}[X]$ in Linearfaktoren zerfällt. Das bedeutet dann, dass A über $\mathbb{L}$, aber nicht über $\mathbb{K}$ ähnlich zu einer oberen Dreiecksmatrix ist.

Definition 6.1.20. Sei $A \in \mathbb{K}^{n \times n}$ und $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$. Wir sagen, dass A $\mathbb{L}$-*trigonalisierbar* ist, wenn A aufgefasst als Element von $\mathbb{L}^{n \times n}$ trigonalisierbar ist.

Beispiel 6.1.21 (Reelle vs. komplexe Trigonalisierbarkeit)**.** Jede reelle Matrix ist nach Korollar 6.1.19 $\mathbb{C}$-trigonalisierbar, da $\mathbb{C}$ nach dem Fundamentalsatz der Algebra algebraisch abgeschlossen ist und χ_A (wie jedes Polynom) über $\mathbb{C}$ in Linearfaktoren erfüllt. Dagegen ist nicht jede reelle Matrix $\mathbb{R}$-trigonalisierbar. Z.B. haben wir in Beispiel 4.5.12 gesehen, dass die Drehmatrix

$$A := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},$$

das charakteristische Polynom $\chi_A = x^2 - 2\cos(\theta)x + 1$ besitzt, das für $\theta \notin \mathbb{Z}\pi$ keine reelle Nullstelle hat.

Übung 6.1.22. Was sind die komplexen Eigenwerte der obigen Drehmatrix A? Ist A, aufgefasst als komplexe Matrix, diagonalisierbar?

Korollar 6.1.23. *Für jede Matrix $A \in \mathbb{K}^{n\times n}$ existiert eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$, so dass A $\mathbb{L}$-trigonalisierbar ist.*

Beweis. Dies folgt sofort aus Proposition 5.4.32 und Satz 6.1.9. □

Wir geben nun eine überraschende Anwendung von Korollar 6.1.23:

Satz 6.1.24 (Satz von Cayley[2]–Hamilton[3])**.** *Für jede Matrix $A \in \mathbb{K}^{n\times n}$ gilt*

$$\chi_A(A) = 0,$$

d.h. A ist eine Nullstelle seines eigenen charakteristischen Polynoms.

Beweis. Es sei $\mathbb{L}$ wie in Korollar 6.1.23. Wir fassen A als Element von $\mathbb{L}^{n\times n}$ auf – dies ändert das charakteristische Polynom von A ja nicht! Es existiert dann $S \in \mathrm{GL}_n(\mathbb{L})$, so dass $B := SAS^{-1} \in \mathbb{L}^{n\times n}$ eine obere Dreiecksmatrix ist. Es gilt dann aber $\chi_A = \chi_B$, und daher

$$\chi_A(A) = \chi_B(A) = \chi_B(S^{-1}BS) = S^{-1}\chi_B(B)S.$$

Es genügt daher zu zeigen, dass $\chi_B(B) = 0$ gilt. Nun ist aber B von der Form

$$B = \begin{pmatrix} \lambda_1 & * & \dots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}, \quad (\lambda_1, \dots, \lambda_n \in \mathbb{L})$$

und es gilt $\chi_B(X) = (X - \lambda_1)\cdots(X - \lambda_n)$. Betrachten wir die invariante Fahne gegeben durch $U_0 := \{0\}$ und $U_k := \langle e_1, \dots, e_k \rangle$ für $k \in \{1, \dots, n\}$, so gilt

$$Be_k \in \lambda_k e_k + U_{k-1} \implies (B - \lambda_k \cdot \mathbf{1})(U_k) \subseteq U_{k-1}.$$

Schematisch können wir das schreiben als

$$\{0\} = U_0 \xleftarrow{B-\lambda_1\cdot\mathbf{1}} U_1 \xleftarrow{B-\lambda_2\cdot\mathbf{1}} \dots \xleftarrow{B-\lambda_{n-1}\cdot\mathbf{1}} U_{n-1} \xleftarrow{B-\lambda_n\cdot\mathbf{1}} U_n = V.$$

Daraus folgt insbesondere, dass

$$\chi_B(B) = (B - \lambda_1 \cdot \mathbf{1})\cdots(B - \lambda_n \cdot \mathbf{1}) = 0.$$ □

[2] Vgl. die Fußnote zu Satz 5.2.20.

[3] Sir William Rowan Hamilton, engl. Mathematiker (1805-1865)

Mittels Korollar 5.4.45 lässt sich der Satz von Cayley-Hamilton auch wie folgt formulieren:

Korollar 6.1.25 (Satz von Cayley-Hamilton, 2. Form)**.** *Sei $A \in \mathbb{K}^{n\times n}$. Dann ist das Minimalpolnom μ_A von A ein Teiler des charakteristischen Polynoms χ_A.* □

Bemerkung 6.1.26 (Ein imaginärer Beweis?)**.** Unser Beweis des Satzes von Cayley-Hamilton verwendet in entscheidender Weise die Existenz eines gewissen Erweiterungskörpers $\mathbb{L}$ von $\mathbb{K}$, der in der Aussage des Satzes gar nicht vorkommt. Das ist eine erste eindrückliche Veranschaulichung des Prinzips, dass es nützlich sein kann zu seinem mathematischen Universum „formale“ oder „imaginäre“ Objekte hinzuzufügen, um damit Aussagen über „reale“ Objekte zu beweisen. In den folgenden Anwendungen des Satzes spielt die Körpertheorie keine Rolle, sie war nur ein Hilfsmittel um den Satz zu beweisen. (Es gibt auch Beweise, die keine Körpertheorie benutzen, aber wir haben diesen Beweis gewählt, um die Vorzüge des abstrakten Zugangs zu verdeutlichen.)

Übung 6.1.27. Was ist falsch am folgenden „Beweis“ des Satzes von Cayley–Hamilton: Es gilt ja $\chi_A(X) = \det(X \cdot \mathbf{1} - A)$, also doch sicher

$$\chi_A(A) = \det(A \cdot \mathbf{1} - A) = \det(A - A) = \det(0) = 0?$$

Bemerkung 6.1.28 (Minimalpolynom einer trigonalisierbaren Matrix)**.** Es sei $A \in \mathbb{K}^{n\times n}$ eine trigonalisierbare Matrix und es seien $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ die *verschiedenen* Eigenwerte von A, so dass

$$\chi_A = (X - \lambda_1)^{e_1}(X - \lambda_2)^{e_2} \cdots (X - \lambda_k)^{e_k}.$$

Nach dem Satz von Cayley–Hamilton gilt dann

$$\mu_A = (X - \lambda_1)^{f_1}(X - \lambda_2)^{f_2} \cdots (X - \lambda_k)^{f_k}$$

für gewisse $f_j \in \{0, 1, \dots, e_j\}$. Wir behaupten, dass sogar stets $f_j \geq 1$ gilt. Wäre nämlich z.B. $f_1 = 0$ und wäre v_1 ein Eigenvektor von A zum Eigenwert λ_1, dann wäre $(A - \lambda_j \cdot \mathbf{1})v_1 = (\lambda_1 - \lambda_j)v_1$ für alle $j \geq 2$, und daher

$$0 = \mu_A(A)v_1 = \prod_{j=2}^{k}(A - \lambda_j \cdot \mathbf{1})^{f_j} v_1 = \left(\prod_{j=2}^{k}(\lambda_1 - \lambda_j)^{f_j}\right) v_1 \implies \prod_{j=2}^{k}(\lambda_1 - \lambda_j)^{f_j} = 0,$$

im Widerspruch dazu, dass $\lambda_1 - \lambda_j \neq 0$ für alle $j \geq 2$. Damit haben wir die folgende Proposition bewiesen.

Proposition 6.1.29 (Nullstellen des Minimalpolynoms)**.** *Ist $A \in \mathbb{K}^{n\times n}$ eine trigonalisierbare Matrix und sind $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ die verschiedenen Eigenwerte von A, so existieren natürliche Zahlen $e_1, \dots, e_k, f_1, \dots, f_k$ mit $1 \leq f_j \leq e_j$ für alle $j \in \{1, \dots, k\}$, so dass*

$$\chi_A = (X - \lambda_1)^{e_1}(X - \lambda_2)^{e_2} \cdots (X - \lambda_k)^{e_k} \quad \text{und} \quad \mu_A = (X - \lambda_1)^{f_1}(X - \lambda_2)^{f_2} \cdots (X - \lambda_k)^{f_k}.$$

Insbesondere haben χ_A und μ_A dieselben Nullstellen (nämlich die Eigenwerte von A). □

Definition 6.1.30. Wir nennen e_k die *algebraische Vielfachheit* des Eigenwerts λ_k.

Übung 6.1.31. Folgern Sie aus Proposition 6.1.29, dass $A \in \mathbb{K}^{n\times n}$ genau dann trigonalisierbar ist, wenn μ_A über $\mathbb{K}$ in Linearfaktoren zerfällt.

Beispiel 6.1.32. Mittels Proposition 6.1.29 kann man Minimalpolynome trigonalisierbarer Matrizen konkret bestimmen:

(i) Ist $A \in \mathbb{K}^{n\times n}$ trigonalisierbar mit n *verschiedenen* Eigenwerten $\lambda_1,\dots,\lambda_n$, so ist $\mu_A = \chi_A = (X-\lambda_1)\cdots(X-\lambda_n)$.

(ii) Ist $A \in \mathbb{K}^{n\times n}$ trigonalisierbar mit nur einem Eigenwert λ, so ist $\chi_A = (X-\lambda)^n$. Es gilt dann $\mu_A = (X-\lambda)^k$, wobei $k \le n$ die kleinste natürliche Zahl mit $(A-\lambda\cdot\mathbf{1})^k = 0$ ist. Da es nur endlich viele Möglichkeiten für k gibt, kann man k durch Ausprobieren ermitteln.

(iii) Ist $A \in \mathbb{K}^{2\times 2}$ mit $\chi_A = (X-\lambda)^2$ für ein $\lambda \in \mathbb{K}$, so gibt es für das Minimalpolynom von A zwei Möglichkeiten: Falls $A = \lambda\cdot\mathbf{1}$, so ist $(X-\lambda)(A) = 0$ und daher $\mu_A = X-\lambda$. Andernfalls ist $\mu_A = (X-\lambda)^2$.

(iv) Beide in (iii) genannten Fälle können eintreten. Dazu betrachten wir die Matrizen.

$$A := \begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} \quad \text{und} \quad B := \begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}.$$

Es gilt dann $\chi_A = \chi_B = (X-\lambda)^2$, also haben A und B dasselbe charakteristische Polynom. Die Minimalpolynome sind aber verschieden, denn es gilt $\mu_A = X-\lambda$ und $\mu_B = (X-\lambda)^2$.

Bemerkung 6.1.33 (Ähnlichkeitsinvarianz des Minimalpolynoms)**.** Das Minimalpolynom einer Matrix ist eine Ähnlichkeitsinvariante: Sind $A,B \in \mathbb{K}^{n\times n}$ und $S \in \mathrm{GL}_n(\mathbb{K})$ mit $B = SAS^{-1}$, so gilt $B^k = SA^kS^{-1}$ für alle $k \in \mathbb{N}$ und daher

$$f(B) = Sf(A)S^{-1} \quad \text{für alle } f \in \mathbb{K}[X].$$

Insbesondere gilt für alle $f \in \mathbb{K}[X]$, dass

$$f(B) = 0 \iff Sf(A)S^{-1} = 0 \iff f(A) = 0,$$

und dies impliziert $\mu_A = \mu_B$. Wir haben also gezeigt, dass

$$A \sim_{\mathbb{K}} B \implies \mu_A = \mu_B. \tag{6.1.4}$$

Beispiel 6.1.34. Die Matrizen A und B aus Beispiel 6.1.32.(iv) haben dasselbe charakteristische Polynom. Sie sind aber nicht ähnlich, weil sie verschiedene Minimalpolynome haben, insbesondere ist B nicht diagonalisierbar. Dies zeigt dass das charakteristische Polynom alleine nicht ausreicht, um Matrizen bis auf Ähnlichkeit zu klassifizieren, ja, nicht einmal, um ihre Diagonalisierbarkeit zu entscheiden.

Wenn wir das Minimalpolynom einer trigonalisierbaren Matrix einmal bestimmt haben, dann können wir damit in der zyklischen Algebra $\langle A\rangle$ effizient rechnen, in dem wir verwenden, dass die Abbildung

$$\mathbb{K}[X]/(\mu_A) \to \langle A\rangle \subseteq \mathbb{K}^{n\times n}, \quad f \mapsto f(A)$$

ein Isomorphismus ist. Wir führen dies in einem Beispiel vor.

Beispiel 6.1.35 (Rechnen in zyklischen Matrizenalgebren)**.** Wir betrachten die Matrix

$$A := \begin{pmatrix}1 & 4 & 1\\ 0 & 2 & 2\\ 1 & 0 & -3\end{pmatrix} \in \mathbb{R}^{3\times 3}.$$

Wir bestimmen zunächst das Minimalpolynom von A. Das charakteristische Polynom ist

$$\begin{aligned}\chi_A &= \begin{vmatrix} X-1 & -4 & -1 \\ 0 & X-2 & -2 \\ -1 & 0 & X+3 \end{vmatrix} = (X-1)\cdot\begin{vmatrix} X-2 & -2 \\ 0 & X+3 \end{vmatrix} + (-1)\cdot\begin{vmatrix} -4 & -1 \\ X-2 & -2 \end{vmatrix} \\ &= (X-1)(X-2)(X+3)-(8+X-2) = X^3-8X = X(X-2\sqrt{2})(X+2\sqrt{2}).\end{aligned}$$

Da alle Nullstellen einfach sind, folgt, dass dies bereits das Minimalpolynom ist, also

$$\mu_A(X) = X^3-8X \quad \text{und daher } \langle A\rangle \cong \mathbb{R}[X]/(X^3-8X).$$

Insbesondere gilt $A^3 = 8A$ und daher

$$A^{100} = A\cdot(A^3)^{33} = A\cdot(8A)^{33} = 8^{33}\cdot A\cdot(A^3)^{11} = 8^{44}\cdot A^{12} = 8^{48}\cdot A^4 = 8^{49}A^2.$$

Das liefert eine sehr schnelle Methode, um A^{100} zu berechnen - viel schneller als z.B. diagonalisieren. Da 0 ein Eigenwert von A ist, hat A einen nicht-trivialen Kern (=Eigenraum zum Eigenwert 0), und ist daher nicht invertierbar. Ist $f \in \mathbb{K}[X]$, so gilt

$$f(A) \text{ invertierbar} \iff [f] \in \mathbb{R}[X]/(X^3-8X) \text{ invertierbar} \iff 1 \text{ ist ein ggT von } f \text{ und } X^3-8X.$$

Betrachten wir konkret das Polynom X^2+1. Dieses ist irreduzibel kein Teiler von X^3-8X, also ist 1 ein ggT von X^2+1 und X^3-8X, und folglich ist $A^2+\mathbf{1}$ eine invertierbare Matrix. Die Inverse können wir mittels erweitertem euklidischem Algorithmus bestimmen: Es gilt

$$\begin{aligned}(X^3-8X) &= X*(X^2+1)+(-9X)\\ (X^2+1) &= (-\frac{1}{9}X)*(-9X)+1\\ (-9X) &= (-9X)*1+0.\end{aligned}$$

Rückwärts einsetzen liefert

$$\begin{aligned}1 &= (X^2+1)+(\frac{1}{9}X)*(-9X)\\ &= (X^2+1)+(\frac{1}{9}X)*[(X^3-8X)-X*(X^2+1)]\\ &= (\frac{1}{9}X)*(X^3-8X)+(-\frac{1}{9}X^2+1)*(X^2+1).\end{aligned}$$

In $\mathbb{R}[X]/(X^3-8X)$ gilt folglich

$$[-\frac{1}{9}X^2+1]*[X^2+1] = 1, \quad \text{und daher} \quad [X^2+1]^{-1} = [-\frac{1}{9}X^2+1].$$

Wir schließen damit, dass

$$(A^2+\mathbf{1})^{-1} = -\frac{1}{9}A^2+\mathbf{1}.$$

Definition 6.1.36. Es sei $A \in \mathbb{K}^{n\times n}$ und $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$. Wir schreiben dann

$$\operatorname{spec}_{\mathbb{L}}(A) := \{\lambda \in \mathbb{L} \mid (\lambda\cdot\mathbf{1}-A) \text{ ist nicht invertierbar}\}$$

und nennen $\operatorname{spec}_{\mathbb{L}}(A)$ das *Spektrum* von A über $\mathbb{L}$.

Nach Definition ist das Spektrum also gerade die Menge der Eigenwerte[4] von A, aufgefasst als Matrix über dem entsprechenden Körper. Analog definiert man das Spektrum eines Endomorphismus.

Da die Eigenwerte über $\mathbb{L}$ die Nullstellen des charakteristischen Polynoms von A in $\mathbb{L}$ sind und das charakteristische Polynom nicht von $\mathbb{L}$ anhängt, gilt insbesondere

$$\operatorname{spec}_{\mathbb{K}}(A) = \operatorname{spec}_{\mathbb{L}}(A) \cap \mathbb{K}. \tag{6.1.5}$$

Beispiel 6.1.37 (Polynome und Eigenwerte)**.** Sei $A \in \mathbb{K}^{n\times n}$ und $f \in \mathbb{K}[X]$. Naiver Weise könnte man vermuten, dass dann $\operatorname{spec}_{\mathbb{K}}(f(A)) = f[\operatorname{spec}_{\mathbb{K}}(A)]$ gilt. Das ist im Allgemeinen aber nicht der Fall. Sei z.B.

$$A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2} \quad \text{und} \quad f = X^2.$$

Es gilt dann $\chi_A = X^2 + 1$ und daher $\operatorname{spec}_{\mathbb{R}}(A) = \emptyset$. Dagegen gilt

$$X^2 = \operatorname{diag}(-1,-1) \implies \operatorname{spec}_{\mathbb{R}}(A^2) = \{-1\}.$$

Es sind also scheinbar Eigenwerte aus dem Nichts entstanden. Wenn man verstehen will, was hier wirklich passiert, muss man sich die Situation über den komplexen Zahlen anschauen: Es ist $\operatorname{spec}_{\mathbb{C}}(A) = \{-i, i\}$ und es gilt

$$\operatorname{spec}_{\mathbb{C}}(A^2) = \{-1\} = \{(-i)^2, i^2\}.$$

Die Erklärung für den reellen Eigenwert -1 von A^2 liegt also im Komplexen!

[4] Ist W ein beliebiger $\mathbb{K}$-Vektorraum (nicht notwendig endlichdimensional) und $\Phi \in \operatorname{End}_{\mathbb{K}}(W)$, so heißt λ ein *Spektralwert* von Φ, falls $\lambda \cdot \mathrm{Id} - \Phi$ nicht bijektiv ist, und die Menge aller Spektralwerte von Φ heißt das *Spektrum* $\operatorname{spec}_{\mathbb{K}}(\Phi)$ von Φ. Im endlichdimensionalen Fall sind die Spektralwerte genau die Eigenwerte, denn ein Endomorphismus ist in diesem Fall genau dann bijektiv, wenn er trivialen Kern hat, aber im unendlichdimensionalen Fall muss man zwischen Eigenwerten und Spektralwerten unterscheiden.

[02.02.24]

Satz 6.1.38 (Spektraler Abbildungssatz für Polynome)**.** *Es sei $A \in \mathbb{K}^{n\times n}$ und $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$, so dass χ_A über $\mathbb{L}$ in Linearfaktoren zerfällt. Dann gilt für alle $f \in \mathbb{K}[X]$, dass*

$$\operatorname{spec}_{\mathbb{K}}(f(A)) = f[\operatorname{spec}_{\mathbb{L}}(A)] \cap \mathbb{K}.$$

Ist insbesondere $\mathbb{K}$ algebraisch abgeschlossen (z.B. $\mathbb{K} = \mathbb{C}$) oder A bereits $\mathbb{K}$-trigonalisierbar, so gilt $\operatorname{spec}_{\mathbb{K}}(f(A)) = f[\operatorname{spec}_{\mathbb{K}}(A)]$.

Beweis. Wegen (6.1.5) dürfen wir annehmen, dass $\mathbb{K} = \mathbb{L}$ gilt, so dass A trigonalisierbar ist. Wir finden dann $S \in \mathrm{GL}_n(\mathbb{L})$ mit

$$SAS^{-1} = B = \begin{pmatrix} \lambda_1 & * & \dots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}, \quad \text{wobei} \quad \operatorname{spec}_{\mathbb{L}}(A) = \operatorname{spec}_{\mathbb{L}}(B) = \{\lambda_1, \dots, \lambda_n\}.$$

Es gilt dann

$$\forall\, k \in \mathbb{N}\colon B^k = \begin{pmatrix} \lambda_1^k & * & \dots & * \\ 0 & \lambda_2^k & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \lambda_n^k \end{pmatrix} \Longrightarrow \forall\, f \in \mathbb{L}[X]\colon f(B) = \begin{pmatrix} f(\lambda_1) & * & \dots & * \\ 0 & f(\lambda_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & f(\lambda_n) \end{pmatrix}.$$

Daraus folgt sofort, dass für alle $f \in \mathbb{L}[X]$ schon $\operatorname{spec}_{\mathbb{L}}(f(B)) = \{f(\lambda_1), \dots, f(\lambda_n)\} = f[\operatorname{spec}_{\mathbb{L}}(A)]$ gilt. Andererseits gilt für alle $k \in \mathbb{N}$, dass $B^k = SA^kS^{-1}$, und daher $f(B) = Sf(A)S^{-1}$. Insbesondere gilt

$$\operatorname{spec}_{\mathbb{L}}(f(A)) = \operatorname{spec}_{\mathbb{L}}(f(B)) = f[\operatorname{spec}_{\mathbb{L}}(A)] \qquad \square$$

Zusammenfassung von Abschnitt 6.1

(1) Die Eigenwerte eines Endomorphismus oder einer Matrix sind die Nullstellen des charakteristischen Polynoms, insbesondere gibt es nur endlich viele solche Eigenwerte.

(2) Ein Endomorphismus oder eine Matrix ist genau dann trigonalisierbar, wenn sein/ihr charakteristisches Polynom in Linearfaktoren zerfällt. Durch eine geeignete Körpererweiterung kann dies stets erreicht werden.

(3) Das Minimalpolynom eines Endomorphismus oder einer Matrix ist stets ein Teiler des charakteristischen Polynoms (Satz von Cayley-Hamilton) mit denselben Nullstellen (nämlich den Eigenwerten).

(4) Mittels Cayley–Hamilton können wir häufig Minimalpolynome praktisch ausrechnen. Dies erlaubt es uns, in zyklischen Matrizenalgebren effizient zu rechnen.

(5) Setzt man eine Matrix in ein Polynom ein, so transformieren sich die Eigenwerte entsprechend, sofern der Grundkörper hinreichend groß gewählt ist.

6.2 Diagonalisierbarkeit

In diesem Abschnitt sei $\mathbb{K}$ ein Körper, V ein n-dimensionaler $\mathbb{K}$-Vektorraums und $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$. Weiter sei $A \in \mathbb{K}^{n\times n}$ eine darstellende Matrix für Φ. Wir gehen der Frage nach, unter welchen Bedingungen Φ bzw. A diagonalisierbar ist. Wir fassen zunächst zusammen was wir schon wissen.

Bemerkung 6.2.1 (Was wir schon wissen)**.** Wir kennen bereits zwei Bedingungen, die diagonalisierbare Endomorphismen bzw. Matrizen erfüllen müssen.

(i) Nach dem 1. Diagonalisierbarkeitskriterium (Proposition 4.5.5) sind Φ bzw. A genau dann diagonalisierbar, wenn V eine Basis aus Eigenvektoren von Φ bzw. A besitzt. Diese Bedingung ist allerdings nicht leicht direkt zu überprüfen.

(ii) Ist Φ bzw. A diagonalisierbar, dann muss nach Satz 6.1.9 bzw. Korollar 6.1.19 das charakteristische Polynom in $\mathbb{K}[X]$ in Linearfaktoren zerfallen. Nach dem Satz von Cayley-Hamilton muss dann auch das Minimalpolynom in Linearfaktoren zerfallen. Diese Bedingungen sind allerdings nur notwendig für die Diagonalisierbarkeit und nicht hinreichend, vgl. Beispiel 6.1.34.

Wir werden nun zuerst das erste Diagonalisierbarkeitskriterium etwas umformulieren, so dass man es leichter anwenden kann. Dazu beobachten wir:

Lemma 6.2.2. *Seien $\lambda_1,\dots,\lambda_k \in \mathbb{K}$ paarweise verschiedene Eigenwerte von Φ. Dann gilt*

$$\sum_{i=1}^{k} V_{\lambda_i}(\Phi) = \bigoplus_{i=1}^{k} V_{\lambda_i}(\Phi).$$

Mit anderen Worten: Die Summe von Eigenräumen zu verschiedenen Eigenwerten ist stets direkt.

Beweis. Seien $u_i \in V_{\lambda_i}(\Phi)$ mit

$$u_1 + u_2 + \cdots + u_k = 0 \tag{6.2.1}$$

Wir zeigen mittels vollständiger Induktion nach k, dass dann $u_1 = \cdots = u_k = 0$ gilt. Im Fall $k = 1$ ist nichts zu zeigen. Sei also $k \geq 2$ und die Behauptung für $k-1$ bewiesen. Einerseits gilt dann

$$\lambda_k u_1 + \cdots + \lambda_k u_k = \lambda_k(u_1 + u_2 + \cdots + u_k) = 0, \tag{6.2.2}$$

andererseits liefert Anwenden von Φ auf (6.2.1) die Gleichung

$$0 = \Phi(0) = \Phi(\sum_{i=1}^{k} u_i) = \sum_{i=1}^{k} \Phi(u_i) = \sum_{i=1}^{k} \lambda_i \cdot u_i. \tag{6.2.3}$$

Subtrahiert man nun (6.2.2) von (6.2.3) so erhält man

$$0 = \sum_{i=1}^{k} (\lambda_i - \lambda_k)u_i = \sum_{i=1}^{k-1} (\lambda_i - \lambda_k)u_i.$$

Dies ist nun eine Summe mit $k-1$ Termen, und wegen $(\lambda_i - \lambda_k)u_i \in V_{\lambda_i}(\Phi)$ lässt sich die Induktionsvoraussetzung anwenden. Wir erhalten also $u_1 = \cdots = u_{k-1} = 0$, und Einsetzen in (6.2.1) liefert dann schlussendlich auch noch $u_k = 0$. □

Bemerkung 6.2.3. Wir betrachten den Unterraum

$$V(\Phi) := \bigoplus_{\lambda \in \operatorname{spec}_{\mathbb{K}}(\Phi)} V_\lambda(\Phi).$$

Nach Konstruktion ist dies ist ein Φ-invarianter Unterraum von V, und es gilt

$$\dim_{\mathbb{K}} V(\Phi) = \sum_{\lambda \in \operatorname{spec}_{\mathbb{K}}(\Phi)} \dim V_\lambda(\Phi).$$

Nach dem 1. Diagonalisierbarkeitskriterium ist $V(\Phi)$ der eindeutige größte Φ-invariante Unterraum U, so dass $\Phi|_U$ diagonalisierbar ist. Insbesondere gilt

$$\Phi \text{ diagonalisierbar} \iff V = V(\Phi) \iff \dim_{\mathbb{K}} V = \dim_{\mathbb{K}} V(\Phi).$$

Damit haben wir insbesondere das folgende Kriterium bewiesen.

Korollar 6.2.4 (2. Diagonalisierbarkeitskriterium)**.** *Φ ist genau dann diagonalisierbar, wenn*

$$\sum_{\lambda \in \operatorname{spec}_{\mathbb{K}}(\Phi)} \dim_{\mathbb{K}} V_\lambda(\Phi) = \dim_{\mathbb{K}} V. \qquad \square$$

Definition 6.2.5. Wir nennen $d_\lambda := \dim_{\mathbb{K}} V_\lambda(\Phi)$ die *geometrische*[5] *Vielfachheit* des Eigenwerts λ von Φ

Um ein noch besseres Kriterium zu erhalten, bringen wir nun noch unsere notwendige Bedingung ins Spiel. Es seien $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von Φ. Falls Φ diagonalisierbar (oder, allgemeiner, trigonalisierbar) ist, so können wir χ_Φ zerlegen als

$$\chi_\Phi = (X - \lambda_1)^{e_1} \cdots (X - \lambda_k)^{e_k},$$

wobei e_j die algebraische Vielfachheit von λ_j bezeichnet. Es gilt dann insbesondere

$$e_1 + \cdots + e_k = \deg(\chi_\Phi) = n.$$

Lemma 6.2.6 (Geometrische vs. algebraische Vielfachheit)**.** *Sei Φ trigonalisierbar mit verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_k$ und zugehörigen algebraischen Vielfachheiten $e_1, \dots, e_k$. Dann gilt*

$$d_j := \dim_{\mathbb{K}} V_{\lambda_j}(\Phi) \le e_j \quad \textit{für alle } j \in \{1, \dots, k\}.$$

Beweis. Sei $j \in \{1, \dots, k\}$. Wir setzen $U := V_{\lambda_j}(\Phi)$, so dass $d_j = \dim_{\mathbb{K}} U$. Dann ist U ein Φ-invarianter Unterraum und nach Definition gilt $\Phi_U = \lambda_j \cdot \mathrm{Id}$ und daher $\chi_{\Phi_U} = (X - \lambda_j)^{d_j}$. Nach Korollar 6.1.16 gilt

$$\chi_\Phi = \chi_{\Phi_U} * \chi_{\Phi_{V/U}},$$

und daher ist χ_{Φ_U} ein Teiler von χ_Φ. Da $(X - \lambda_j)$ kein Teiler von $(X - \lambda_i)$ für $i \neq j$ ist, folgt daraus, dass $d_j \le e_j$ gilt. $\square$

Falls Sie sich nicht merken können, welche der beiden Vielfachheiten kleiner ist, hier eine Gedächtnisstütze: *„d wie Dimension kommt vor e wie Exponent."*

[5] Sowohl die algebraische als auch die geometrische Vielfachheit eines Eigenwerts sind algebraisch definierte natürliche Zahlen, die eine geometriscshe Bedeutung tragen. Mir ist nicht klar, in welchem Sinne die algebraische Vielfachheit „algebraischer" und die geometrische Vielfachheit „geometrischer" sein soll, aber die Terminologie ist nun einmal wie sie ist.

Korollar 6.2.7 (3. Diagonalisierbarkeitskriterium)**.** *Φ ist genau dann diagonalisierbar, wenn die folgenden beiden Bedingungen erfüllt sind.*

(i) *χ_Φ zerfällt über $\mathbb{K}$ als $\chi_\Phi = (X-\lambda_1)^{e_1}\cdots(X-\lambda_k)^{e_k}$, wobei $\lambda_1,\dots,\lambda_k$ die verschiedenen Eigenwerte von Φ sind.*

(ii) *Für alle $j \in \{1,\dots,k\}$ gilt $d_j := \dim V_{\lambda_j}(\Phi) = e_j$ („geometrische Vielfachheit = algebraische Vielfachheit“).*

Beweis. Wir zeigen zunächst, dass die beiden Bedingungen notwendig sind. Für (i) folgt dies sofort aus Satz 6.1.9. Falls (ii) verletzt ist, so existiert ein j mit $d_j < e_j$. Dann gilt aber wegen Lemma 6.2.6, dass

$$\sum_{\lambda\in\operatorname{spec}(\Phi)} \dim_{\mathbb{K}} V_\lambda(\Phi) = d_1+\cdots+d_k < e_1+\cdots+e_k = n,$$

und daher ist Φ nach dem 2. Diagonalisierbarkeitskriterium nicht diagonalisierbar.

Die Bedingungen sind aber nach demselben Kriterium auch hinreichend, denn falls (i) und (ii) gelten, so ist

$$\sum_{\lambda\in\operatorname{spec}(\Phi)} \dim_{\mathbb{K}} V_\lambda(\Phi) = d_1+\cdots+d_k = e_1+\cdots+e_k = n. \qquad \square$$

Bemerkung 6.2.8 (Arbeit sparen)**.** Die Bedingungen des 3. Diagonalisierbarkeitskriteriums sind in der Praxis meist leichter zu überprüfen als die Bedingungen der ersten beiden Kriterien. Um (ii) zu überprüfen muss man im schlimmsten Fall aber immer noch für jeden Eigenwert ein LGS lösen. (Wenn man bei *einem* der Eigenwerte eine zu geringe geometrische Vielfachheit gefunden hat, kann man natürlich aufhören zu rechnen.) Glücklicherweise kann man sich häufig sehr viel Arbeit sparen, indem man verwendet, dass jeder Eigenwert mindestens die geometrische Vielfachheit 1 besitzt (da es zu jedem Eigenwert mindestens eine Eigengerade gibt). Man muss also die Bedingung (ii) nur für Eigenwerte λ_j von algebraischer Vielfachheit $e_j \geq 2$ überprüfen.

Als Spezialfall halten wir fest:

Korollar 6.2.9 (Hinreichende Bedingung)**.** *Zerfällt das charakteristische Polynom eines Endomorphismus in paarweise verschiedene Linearfaktoren, so ist dieser diagonalisierbar.* $\square$

Bemerkung 6.2.10 (Ableitungstrick)**.** Wenn man weiß, dass χ_Φ in Linearfaktoren zerfällt, so kann man mit einem kleinen Trick leicht feststellen, ob das charakteristische Polynom eine mehrfache Nullstelle besitzt. Dazu betrachtet man die *formale Ableitung*, die durch

$$(a_0 + a_1X + \cdots + a_nX^n)' := a_1 + \cdots + na_nX^{n-1}$$

gegeben ist und die Produktregel $(f*g)' = f'*g + f*g'$ erfüllt (Übung!). Es gilt dann

$$f = \prod_{i=1}^{n}(X-\lambda_i) \implies f' = \sum_{i=1}^{n}\prod_{j\in\{1,\dots,n\}\setminus\{i\}}(X-\lambda_j).$$

Falls $\lambda_j = \lambda_k$ für ein $j \neq k$ gilt, so ist $(X-\lambda_j)$ ein Teiler von f', und daher ein nicht-trivialer gemeinsamer Teiler von f und f'. Falls die Nullstellen $\lambda_1,\dots,\lambda_n$ paarweise verschieden sind, so ist λ_j eine Nullstelle aller Summanden von f' mit Ausnahme des $j$ten Summanden, und daher keine Nullstelle von f'. Das bedeutet aber dann gerade, dass f und f' keine gemeinsamen Teiler vom Grad ≥ 1 haben.

Korollar 6.2.11. *Ist Φ trigonalisierbar und besitzen χ_Φ und χ'_Φ keine gemeinsamen Teiler vom Grad ≥ 1, so ist Φ diagonalisierbar.* □

Bemerkung 6.2.12. Die Bedingung aus Korollar 6.2.9 ist hinreichend, aber nicht notwendig: Die Matrix $A := \mathrm{diag}(1,1)$ ist diagonalisierbar mit $\chi_A = (X-1)^2$. Wegen des Satzes von Cayley-Hamilton impliziert die Bedingung aus Korollar 6.2.9, dass das Minimalpolynom in paarweise verschiedene Linearfaktoren zerfällt. Es stellt sich nun heraus, dass diese schwächere Bedingung sowohl hinreichend als auch notwendig ist.

Satz 6.2.13 (4. Diagonalisierbarkeitskriterium)**.** *Φ ist genau dann diagonalisierbar, wenn das Minimalpoylnom μ_Φ über $\mathbb{K}$ in paarweise verschiedene Linearfaktoren zerfällt.*

Beweis. Es sei $\mathrm{spec}_{\mathbb{K}}(\Phi) = \{\lambda_1, \ldots, \lambda_k\}$, wobei $\lambda_1, \ldots, \lambda_k$ paarweise verschieden sind.

Sei zunächst Φ diagonalisierbar. Wir finden dann eine geordnete Basis $\mathscr{B}$ von V mit

$$A := D_{\mathscr{B}}(\Phi) = \mathrm{diag}(\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots, \lambda_2, \ldots, \lambda_k \ldots, \lambda_k).$$

Nach Proposition 6.1.29 ist

$$m := (X-\lambda_1)\cdots(X-\lambda_k)$$

ein Teiler von μ_Φ. Es gilt aber

$$\begin{aligned} m(A) &= \mathrm{diag}(0, \ldots, 0, \lambda_2, \ldots, \lambda_2, \ldots, \lambda_k \ldots, \lambda_k)\mathrm{diag}(\lambda_1, \ldots, \lambda_1, 0, \ldots 0, \ldots, \lambda_k \ldots, \lambda_k) \\ &\quad \cdots \mathrm{diag}(\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots, \lambda_2, \ldots, 0 \ldots, 0) = 0, \end{aligned}$$

und folglich $m(A) = 0$. Dies zeigt, dass $\mu_\Phi = \mu_A = m$, also zerfällt μ_Φ in paarweise verschiedene Linearfaktoren.

Umgekehrt zerfalle μ_Φ in paarweise verschiedene Linearfaktoren. Nach Proposition 6.1.29 gilt dann $\mu_A = (X-\lambda_1)\cdots(X-\lambda_k)$. Wir zeigen, dass $V = V_{\lambda_1}(\Phi) \oplus \cdots \oplus V_{\lambda_k}(\Phi)$ durch Induktion nach k. Ist $k = 1$, so haben wir $\mu_\Phi(X) = X - \lambda_1$, also $\Phi = \lambda_1 \cdot \mathrm{Id}$, und daher ist Φ diagonalisierbar.

Sei nun $k \geq 2$ und $U := \mathrm{Bild}(\Phi - \lambda_k \cdot \mathrm{Id})$. Wir behaupten, dass U ein Φ-invarianter Unterraum ist. Ist nämlich $u \in U$, so existiert $v \in V$ mit $u = \Phi(v) - \lambda_k v$, und folglich

$$\Phi(u) = \Phi(\Phi(v) - \lambda_k v) = \Phi(\Phi(v)) - \lambda_k \Phi(v) = (\Phi - \lambda_k \cdot \mathrm{Id})(\Phi(v)) \in U.$$

Andererseits gilt für $u = \Phi(v) - \lambda_k v \in U$ stets

$$(\Phi - \lambda_1 \cdot \mathbf{1})\cdots(\Phi - \lambda_{k-1} \cdot \mathbf{1})(u) = (\Phi - \lambda_1 \cdot \mathbf{1})\cdots(\Phi - \lambda_k \cdot \mathbf{1})(v) = \mu_\Phi(\Phi)(v) = 0.$$

Ist also $\Phi_U : U \to U$ der induzierte Endomorphismus, so gilt

$$\mu_{\Phi_U}(X) \,\big|\, (X-\lambda_1)\cdots(X-\lambda_{k-1}).$$

Dieses Minimalpolynom hat keine mehrfachen Nullstellen. Andererseits gilt $\dim U < \dim V$, da sonst $\Phi - \lambda_k \cdot \mathrm{Id}$ surjektiv, also bijektiv, und λ_k kein Eigenwert wäre. Nach Induktionsvoraussetzung gilt daher

$$U = U_{\lambda_1}(\Phi_U) \oplus \cdots \oplus U_{\lambda_{k-1}}(\Phi_U),$$

und wegen $U_{\lambda_i}(\Phi_U) \subseteq V_{\lambda_i}(\Phi)$ insbesondere

$$\dim U = \sum_{i=1}^{k-1} \dim U_{\lambda_i}(\Phi_U) \leq \sum_{i=1}^{k-1} \dim V_{\lambda_i}(\Phi).$$

Andererseits gilt

$$n = \dim(\text{Bild}(\Phi - \lambda_k \cdot \text{Id})) + \dim(\ker(\Phi - \lambda_k \cdot \text{Id}) = \dim U + \dim V_{\lambda_k}(\Phi),$$

und daher

$$n \leq \left(\sum_{i=1}^{k-1} \dim V_{\lambda_i}(\Phi)\right) + \dim V_{\lambda_k}(\Phi) = \sum_{i=1}^{k} \dim V_{\lambda_i}(\Phi).$$

Nach dem 2. Diagonalisierbarkeitskriterium ist Φ daher diagonalisierbar. □

Bemerkung 6.2.14. Wir erinnern daran, dass Φ genau dann trigonalisierbar ist, wenn μ_Φ über $\mathbb{K}$ in Linearfaktoren zerfällt (vgl. Übung 6.1.31). Damit Φ diagonalisierbar ist, müssen wir nach dem obigen Kriterium zusätzlich verlangen, dass μ_Φ und μ'_Φ keinen gemeinsamen Teiler vom Grad ≥ 1 haben.

Beispiel 6.2.15 (Involutionen sind diagonalisierbar)**.** Ein Endomorphismus Φ heißt eine *Involution*, falls $\Phi^2 = \text{Id}$. In diesem Fall ist das Minimalpolynom von Φ ein Teiler von $X^2 - 1 = (X-1)(X+1)$. Falls $\text{char}(\mathbb{K}) \neq 2$, so gilt $1 \neq -1$, also ist über einem Körper der Charakteristik $\neq 2$ jede Involution diagonalisierbar. Insbesondere gilt dann

$$V = V_1(\Phi) \oplus V_{-1}(\Phi).$$

Man kann also jedes $v \in V$ eindeutig schreiben als Summe zweier Eigenvektoren, einen zum Eigenwert 1 (*Fixvektor*) und einen zum Eigenwert -1. Wir können diese Zerlegung aber auch direkt raten: Ist $v \in V$, so gilt (unter der stehenden Annahme $\text{char}(\mathbb{K}) \neq 2$), dass

$$\frac{1}{2}(v + \Phi(v)) \in V_1(\Phi), \quad \frac{1}{2}(v - \Phi(v)) \in V_{-1}(\Phi) \quad \text{und} \quad \frac{1}{2}(v + \Phi(v)) + \frac{1}{2}(v - \Phi(v)) = v.$$

Es ist also $\frac{1}{2}(v + \Phi(v))$ der Fixanteil von v und $\frac{1}{2}(v - \Phi(v))$ der Anteil an v im Eigenraum zu -1.

Als konkretes Beispiel ist z.B. die Involution $\Phi : \mathbb{K}^{n\times n} \to \mathbb{K}^{n\times n}$, $A \mapsto A^\top$. Ein Eigenvektor von Φ zum Eigenwert 1 bzw. -1 heißt eine *symmetrische* bzw. *schief-symmetrische* Matrix. Die Diagonalisierbarkeit von Φ besagt nun gerade, dass sich jede Matrix A eindeutig in einen symmetrischen Anteil $\frac{1}{2}(A + A^\top)$ und einen schief-symmetrischen Anteil $\frac{1}{2}(A - A^\top)$ zerlegen lässt.

Man kann das 4. Diagonalisierbarkeitskriterium aber häufig auch verwenden, um zu zeigen, dass ein Endomorphismus *nicht* diagonalisierbar ist. Wir führen dies an einem Beispiel vor.

Definition 6.2.16. Sei $\lambda \in \mathbb{K}$. Der Endomorphismus Φ heißt *λ-potent*, falls ein $k \in \mathbb{N}$ existiert mit $(\Phi - \lambda \cdot \text{Id})^k = 0$. Ist $\lambda = 0$, so heißt Φ *nilpotent*, ist $\lambda = 1$, so heißt Φ *unipotent*.

Beispiel 6.2.17. Unipotente Elementarmatrizen sind unipotent (daher der Name).

Proposition 6.2.18 (Nicht-diagonalisierbare Endomorphismen)**.** *Sei $\lambda \in \mathbb{K}$.*

(i) Ist Φ nilpotent, so gilt $\Phi^k = 0$ für ein $k \leq n$.

(ii) Ist Φ nilpotent und $\Phi \neq 0$, so ist Φ nicht diagonalisierbar.

(iii) Ist Φ λ-potent und $\Phi \neq \lambda \cdot \text{Id}$, so ist Φ nicht diagonalisierbar.

(iv) Ist Φ unipotent und $\Phi \neq \text{Id}$, so ist Φ nicht diagonalisierbar.

(v) Unipotente Elementarmatrizen sind nicht diagonalisierbar.

Beweis. Sei zunächst Φ nilpotent, A eine darstellende Matrix von Φ und $k \in \mathbb{N}$ mit $A^k = 0$. Es sei nun $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$, so dass χ_A (und daher μ_A) über $\mathbb{L}$ in Linearfaktoren zerfällt. Wir fassen A als Matrix in $\mathbb{L}^{n\times n}$ auf.

Wegen $A^k = 0$, gilt dann $\mu_A \mid X^k$. Mit Proposition 6.1.29 folgt, dass $\operatorname{spec}_{\mathbb{L}}(A) = \{0\}$. Da χ_A über $\mathbb{L}$ in Linearfaktoren zerfällt, folgt, dass $\chi_A = X^n$. (i) folgt dann sofort aus dem Satz von Cayley-Hamilton. Aus dem 4. Diagonalisierbarkeitskriterium folgt dann, dass

$$\Phi \text{ diagonalisierbar} \iff \mu_\Phi(X) = X \iff \Phi = 0,$$

also (ii). Ist Φ λ-potent, so ist $\Psi := \Phi - \lambda \cdot \mathrm{Id}$ nilpotent, und Anwenden von (ii) auf Ψ liefert (iii). (iv) und (v) sind Spezialfälle von (iii). □

Übung 6.2.19 (Diagonalisierbarkeit induzierter Endomorphismen)**.** Es sei $\Phi \in \operatorname{End}_{\mathbb{K}}(V)$ und $U_1 < U_2 \leq V$ zwei Φ-invariante Unterräume und $f \in \mathbb{K}[X]$. Zeigen Sie:

(i) U_1 und U_2 sind $f(\Phi)$-invariant.

(ii) Es gilt $f(\Phi)_{U_2/U_1} = f(\Phi_{U_2/U_1})$.

[*Hinweis:* Machen Sie sich zunächst klar, dass für Blockmatrizen die Identität

$$\begin{pmatrix} A & * \\ 0 & C \end{pmatrix}^k = \begin{pmatrix} A^k & * \\ 0 & C^k \end{pmatrix} \quad (k \in \mathbb{N})$$

gilt.]

(iii) $\mu_{\Phi_{U_2/U_1}}$ ist ein Teiler von μ_Φ.

(iv) Ist Φ diagonalisierbar, so auch Φ_{U_2/U_1}.

Zusammenfassung von Abschnitt 6.2

(1) Ein Endomorphismus oder einer Matrix sind genau dann diagonalisierbar, wenn ihr charakteristisches Polynom in Linearfaktoren zerfällt und die geometrischen und algebraischen Vielfachheiten der Eigenwerte übereinstimmen.

(2) Ein Endomorphismus oder eine Matrix sind genau dann diagonalisierbar, wenn ihr Minimalpolynom in paarweise verschiedene Linearfaktoren zerfällt. Dies ist insbesondere dann der Fall, wenn schon das charakteristische Polynom in paarweise verschiedene Linearfaktoren zerfällt.

(3) Involutionen sind stets diagonalisierbar, nilpotente oder unipotente Matrizen hingegen nur, wenn sie Vielfache der Einheitsmatrix sind.

[09.02.24]

6.3 Simultane Diagonalisierbarkeit

Es sei $\mathbb{K}$ ein Körper und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum der Dimension n. Es bezeichne $\mathrm{Diag}(n,\mathbb{K}) \subseteq \mathbb{K}^{n\times n}$ die Teilmenge der Diagonalmatrizen.

Wir haben gesehen, dass man durch geschickte Wahl einer Basis in vielen Fällen einen Endomorphismus durch eine besonders einfache Matrix (Diagonal- bzw. obere Dreiecksmatrix) darstellen kann, was das Rechnen mit Endomorphismen ungemein erleichtert - solange wir immer nur *einen* Endomorphismus (und seine Potenzen) betrachten. Was aber, wenn wir zwei oder mehr Endomorphismen gegeben haben?

Definition 6.3.1. Eine Teilmenge $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ heißt *simultan diagonalisierbar*, falls eine geordnete Basis $\mathscr{B}$ von V existiert, so dass $D_{\mathscr{B}}(\Phi) \in \mathrm{Diag}(n,\mathbb{K})$ für alle $\Phi \in \mathscr{A}$. In diesem Fall sagen wir dann, dass $\mathscr{B}$ die Menge $\mathscr{A}$ *simultan diagonalisiert*.

Analog heißt eine Teilmenge $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$ *simultan diagonalisierbar*, falls eine Matrix $S \in \mathrm{GL}_n(\mathbb{K})$ existiert, so dass $SAS^{-1} \in \mathrm{Diag}(n,\mathbb{K})$ für alle $A \in \mathscr{A}$ gilt.

Bemerkung 6.3.2 (Der Fall von zwei Endomorphismen)**.** Nach Definition ist eine einelementige Teilmenge $\mathscr{A} = \{\Phi\} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ genau dann diagonalisierbar, wenn ihr einziges Element Φ diagonalisierbar ist. Simultane Diagonalisierbarkeit ist also nur für Mengen, die mindestens zwei Elemente enthalten, ein neuer Begriff.

Eine zweielementige Teilmenge $\mathscr{A} = \{\Phi,\Psi\} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ ist nach Definition genau dann simultan diagonalisierbar, wenn es eine geordnete Basis $\mathscr{B} = (v_1,\dots,v_n)$ von V und Elemente $\lambda_1(\Phi),\dots,\lambda_n(\Phi),\lambda_1(\Psi),\dots,\lambda_n(\Psi)$ gibt, so dass

$$D_{\mathscr{B}}(\Phi) = \mathrm{diag}(\lambda_1(\Phi),\dots,\lambda_n(\Phi)) \quad \text{und} \quad D_{\mathscr{B}}(\Psi) = \mathrm{diag}(\lambda_1(\Psi),\dots,\lambda_n(\Psi)).$$

Dies bedeutet aber gerade, dass

$$v_1 \in V_{\lambda_1(\Phi)}(\Phi) \cap V_{\lambda_1(\Psi)}(\Psi), \quad \dots, \quad v_n \in V_{\lambda_n(\Phi)}(\Phi) \cap V_{\lambda_n(\Psi)}(\Psi).$$

Die Vektoren $v_1,\dots,v_n$ haben also die folgenden beiden Eigenschaften: Sie liegen in den Schnitten von Eigenräumen von Φ mit Eigenräumen von Ψ, und sie sind nicht 0. Man sagt daher, $v_1,\dots,v_n$ sind *simultane Eigenvektoren* von Φ und Ψ.

Beispiel 6.3.3 (Zwei simultan diagonalisierbare Matrizen)**.** Wir betrachten die beiden reellen Matrizen

$$A := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{und} \quad B := \begin{pmatrix} 3 & 3 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

Wir berechnen zunächst das charakteristische Polynom und die Eigenwerte von A:

$$\chi_A(X) = (X-1)^2(X-2) \quad \Longrightarrow \quad \mathrm{spec}(A) = \{1,2\}.$$

Für die zugehörigen Eigenräume gilt

$$V_1(A) = \ker(\mathbf{1} - A) = \ker\begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} = \ker\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \langle e_1, e_2 \rangle.$$

und

$$V_2(A) = \ker(2\cdot\mathbf{1} - A) = \ker\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} = \langle e_1 + e_2 + e_3 \rangle.$$

Für beide Eigenwerte stimmt also die algebraische und geometrische Vielfachheit überein, und daher ist A ist diagonalisierbar. Analog rechnet man

$$\chi_B(X) = (X-3)(X-6)^2 \quad \Longrightarrow \quad \operatorname{spec}(B) = \{3,6\}.$$

Die zugehörigen Eigenräume sind also

$$V_3(B) = \ker(3\cdot\mathbf{1} - B) = \ker\begin{pmatrix} 0 & -3 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -3 \end{pmatrix} = \ker\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \langle e_1 \rangle$$

und

$$V_6(B) = \ker(6\cdot\mathbf{1} - B) = \ker\begin{pmatrix} 3 & -3 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \ker\begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \langle e_1 + e_2, e_1 + e_2 + e_3 \rangle,$$

also ist B diagonalisierbar.

Wie steht es nun um die simultane Diagonalisierbarkeit? Die nicht-trivialen Schnitte der Eigenräume von A und B sind gerade

$$V_1(A) \cap V_3(B) = \langle e_1 \rangle, \quad V_1(A) \cap V_6(B) = \langle e_1 + e_2 \rangle \quad \text{und} \quad V_2(A) \cap V_6(B) = \langle e_1 + e_2 + e_3 \rangle.$$

Daher sind beispielsweise $v_1 := e_1$, $v_2 := e_1 + e_2$ und $v_3 := e_1 + e_2 + e_3$ simultane Eigenvektoren von A und B, uns setzen wir $\mathscr{B} := (v_1, v_2, v_3)$, so erhalten wir

$$D_{\mathscr{B}}(\Phi_A) = \operatorname{diag}(1,1,2) \quad \text{und} \quad D_{\mathscr{B}}(\Phi_B) = \operatorname{diag}(3,6,6)$$

Insbesondere sind A und B simultan diagonalisierbar.

Für Mengen $\mathscr{A}$ mit mehr als zwei Elementen führen wir analog die folgenden Begriffe ein:

Definition 6.3.4. Sei $\mathscr{A} \subseteq \operatorname{End}_{\mathbb{K}}(V)$ und $\lambda : \mathscr{A} \to \mathbb{K}$ eine Abbildung. Dann heißt

$$V_\lambda(\mathscr{A}) := \bigcap_{\Phi \in \mathscr{A}} V_{\lambda(\Phi)}(\Phi) = \{v \in V \mid \forall\, \Phi \in \mathscr{A} :\, \Phi(v) = \lambda(\Phi) v\}$$

der *simultane Eigenraum* von $\mathscr{A}$ zu λ. Falls $V_\lambda(\mathscr{A}) \neq \{0\}$, so heißt λ ein *simultaner Eigenwert* von $\mathscr{A}$, und $v \in V_\lambda(\mathscr{A}) \setminus \{0\}$ heißt ein *simultaner Eigenvektor* von $\mathscr{A}$.

Beachten Sie, dass ein simultaner Eigenwert kein Skalar, sondern eine Abbildung ist! Man kann sich einen solchen simultanen Eigenwert auch als eine durch $\mathscr{A}$ indizierte Liste von Skalaren vorstellen – zu jedem Element Φ von $\mathscr{A}$ gibt es einen Skalar, der besagt, wie der zugehörige simultane Eigenvektor von Φ gestreckt/gestaucht/gespiegelt werden soll. Im obigen Beispiel waren die drei simultanen Eigenwerte gerade die Funktionen $\lambda_{1,3}$, $\lambda_{1,6}$ und $\lambda_{2,6}$ mit

$$\lambda_{i,j} : \{\Phi, \Psi\} \to \mathbb{R}, \quad \Phi \mapsto i, \quad \Psi \mapsto j.$$

Genau wie im Fall $|\mathscr{A}| = 2$ zeigt man:

Proposition 6.3.5. *Eine Teilmenge $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ (bzw. $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$) ist genau dann simultan diagonalisierbar, wenn V eine Basis aus simultanen Eigenvektoren von $\mathscr{A}$ besitzt.* □

Dieses Kriterium ist wieder schwer nachzuprüfen, und wir werden im Folgenden bessere Kriterien finden.

Bemerkung 6.3.6 (Algebra der Diagonalmatrizen)**.** Die Teilmenge $\mathrm{Diag}(n,\mathbb{K}) \subseteq \mathbb{K}^{n\times n}$ ist eine *kommutative* $\mathbb{K}$-Unteralgebra. Dies folgt aus der Kommutativität der Skalarmultiplikation und der Tatsache, dass für $\lambda_1,\dots,\lambda_n,\mu_1,\dots,\mu_n \in \mathbb{K}$ stets $\mathrm{diag}(\lambda_1,\dots,\lambda_n)+\mathrm{diag}(\mu_1,\dots,\mu_n) = \mathrm{diag}(\lambda_1+\mu_1,\dots,\lambda_n+\mu_n)$ und $\mathrm{diag}(\lambda_1,\dots,\lambda_n)\mathrm{diag}(\mu_1,\dots,\mu_n) = \mathrm{diag}(\lambda_1\mu_1,\dots,\lambda_n\mu_n)$ gilt.

Sind insbesondere $A,B \in \mathrm{Diag}(n,\mathbb{K})$, so auch AB (insbesondere λB für $\lambda \in \mathbb{K}$) und $A+B$. Allgemeiner gilt: Ist $\mathscr{D} \subseteq \mathrm{Diag}(n,\mathbb{K})$, so auch die von $\mathscr{D}$ erzeugte Algebra $\langle\mathscr{D}\rangle_{\mathrm{alg}}$. Nach Definition ist dies gerade die kleinste assoziative $\mathbb{K}$-Algebra, die $\mathscr{D}$ enthält – ihre Elemente sind Linearkombinationen von Produkten von Elementen aus $\mathscr{D}$.

Bemerkung 6.3.7. Aus Bemerkung 6.3.6 folgt, dass eine Teilmenge $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ (bzw. $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$) genau dann simultan diagonalisierbar ist, wenn die von $\mathscr{A}$ erzeugte Algebra simultan diagonalisierbar ist. Wir dürfen also – indem wir $\mathscr{A}$ durch $\langle\mathscr{A}\rangle_{\mathrm{alg}}$ ersetzen – im Folgenden stets annehmen, dass $\mathscr{A}$ eine Unteralgebra von $\mathrm{End}_{\mathbb{K}}(\mathscr{A})$ (bzw. $\mathbb{K}^{n\times n}$) ist. Dies sei ab jetzt der Fall.

Für jede Basis $\mathscr{B}$ erhalten wir einen Monomorphismus $D_{\mathscr{B}} : \mathscr{A} \to \mathbb{K}^{n\times n}$. Falls $\mathscr{A}$ von $\mathscr{B}$ simultan diagonalisiert wird, so erhalten wir einen Monomorphismus $D_{\mathscr{B}} : \mathscr{A} \to \mathrm{Diag}(n,\mathbb{K})$. Dann muss aber die Algebra $\mathscr{A} \cong D_{\mathscr{B}}[\mathscr{A}]$ als Unteralgebra von $\mathrm{Diag}(n,\mathbb{K})$ kommutativ sein! Damit haben wir gezeigt:

Proposition 6.3.8 (Notwendige Bedingung)**.** *Ist $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ simultan diagonalisierbar, so ist jedes $\Phi \in \mathscr{A}$ ist diagonalisierbar und die Elemente von $\mathscr{A}$ kommutieren, d.h. $\Phi\circ\Psi = \Psi\circ\Phi$ für alle $\Phi,\Psi \in \mathscr{A}$.* □

Beispiel 6.3.9. Die Matrizen aus Beispiel 6.3.5 kommutieren. Genauer gilt

$$AB = \begin{pmatrix} 3 & 3 & 6 \\ 0 & 6 & 6 \\ 0 & 0 & 12 \end{pmatrix} = BA.$$

Wir werden noch sehen, dass die notwendige Bedingung aus Proposition 6.3.8 schon hinreichend ist. Dazu stellen wir zunächst einige Vorüberlegungen zu simultanen Eigenwerten und Eigenräumen an.

Lemma 6.3.10 (Simultane Eigenwerte als Charaktere)**.** *Sei $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ eine Unteralgebra und λ ein simultaner Eigenwert von $\mathscr{A}$. Dann ist $\lambda : \mathscr{A} \to \mathbb{K}$ ein Morphismus von $\mathbb{K}$-Algebren.*

Beweis. Seien $\Phi,\Psi \in \mathscr{A}$ und $v \in V_\lambda(\mathscr{A}^*) \setminus \{0\}$. Dann gilt

$$\lambda(\Phi+\Psi)\cdot v = (\Phi+\Psi)(v) = \Phi(v)+\Psi(v) = (\lambda(\Phi)+\lambda(\Psi))v \quad\Longrightarrow\quad \lambda(\Phi+\Psi) = \lambda(\Phi)+\lambda(\Psi).$$

Analog zeigt man $\lambda(\mathrm{Id}) = 1$, $\lambda(\Phi\circ\Psi) = \lambda(\Phi)\lambda(\Psi)$ und $\lambda(\mu\Phi) = \mu\lambda(\Phi)$ für $\mu \in \mathbb{K}$. □

Man nennt einen Morphismus von einer $\mathbb{K}$-Algebra $\mathscr{A}$ in den Grundkörper $\mathbb{K}$ auch einen *Charakter* von $\mathscr{A}$. Simultane Eigenwerte sind also Charaktere.

Wie im Fall eines einzelnen Endomorphismus zeigt man:

Lemma 6.3.11. *Ist $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ und sind $\lambda_1, \dots, \lambda_k$ paarweise verschiedene simultane Eigenwerte von $\mathscr{A}$, so gilt*

$$V_{\lambda_1}(\mathscr{A}) + \cdots + V_{\lambda_k}(\mathscr{A}) = V_{\lambda_1}(\mathscr{A}) \oplus \cdots \oplus V_{\lambda_k}(\mathscr{A}),$$

d.h. die Summe verschiedener simultaner Eigenräume ist direkt.

Beweis. Wir argumentieren mittels Induktion nach k; für $k = 1$ ist nichts zu zeigen. Sei also $k \geq 2$ und seien $v_1 \in V_{\lambda_1}(\mathscr{A})$, …, $v_k \in V_{\lambda_k}(\mathscr{A})$ mit

$$v_1 + \cdots + v_k = 0. \tag{6.3.1}$$

Wir müssen zeigen, dass $v_1 = v_2 = \cdots = v_k = 0$. Wegen $\lambda_1 \neq \lambda_2$ existiert $\Phi \in \mathscr{A}$ mit $\lambda_1(\Phi) \neq \lambda_2(\Phi)$. Wir fixieren ein solches Φ und setzen

$$I_1 := \{i \in \{1, \dots, k\} \mid \lambda_i(\Phi) = \lambda_1(\Phi)\} \quad \text{und} \quad I_2 := \{1, \dots k\} \setminus I_1.$$

Dann gilt $1 \in I_1$ und $2 \in I_2$, also sind I_1.und I_2 nichtleer. Wegen (6.3.1) gilt

$$\sum_{i \in I_1} v_i = -\sum_{i \in I_2} v_i.$$

Die linke Seite ist im Eigenraum $V_{\lambda_1(\Phi)}(\Phi)$ enthalten und die rechte Seite in

$$W := \sum_{j \in I_2} V_{\lambda_j(\Phi)}(\Phi).$$

Da die Summe von Eigenräumen von einem einzelnen Endomorphismus direkt ist, gilt $V_{\lambda_1(\Phi)}(\Phi) \cap W = \{0\}$, also

$$\sum_{i \in I_1} v_i = -\sum_{i \in I_2} v_i = 0.$$

Diese beiden Summen sind nun aber jeweils in einer Summe von höchstens $k - 1$ simultanen Eigenräumen enthalten. Nach Induktionsvoraussetzung sind diese Summen direkt, also folgt $v_1 = v_2 = \cdots = v_k = 0$. □

Als letzte Zutat benötigen wir noch die folgende wichtige Beobachtung:

Lemma 6.3.12 (Invarianz von Eigenräumen)**.** *Seien $\Phi, \Psi \in \mathrm{End}_{\mathbb{K}}(V)$. Falls $\Phi \circ \Psi = \Psi \circ \Phi$, so ist jeder Eigenraum von Φ automatisch Ψ-invariant.*

Beweis. Sei λ ein Eigenwert von Φ und $v \in V_\lambda(\Phi)$. Setze $w := \Psi(v)$. Dann gilt

$$\Phi(w) = \Phi(\Psi(v)) = (\Phi \circ \Psi)(v) = (\Psi \circ \Phi)(v) = \Psi(\Phi(v)) = \Psi(\lambda v) = \lambda \Psi(v) = \lambda w,$$

also ist $w \in V_\lambda(\Phi)$. Dies zeigt, dass $\Psi(v) \in V_\lambda(\Phi)$ für alle $v \in V_\lambda(\Phi)$, also $\Psi[V_\lambda(\Phi)] \subseteq V_\lambda(\Phi)$. □

Damit können wir nun simultane Diagonalisierbarkeit wie folgt charakterisieren:

Satz 6.3.13 (Kriterium für simultane Diagonalisierbarkeit)**.** *Für $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ sind die folgenden Aussagen äquivalent:*

(i) $\mathscr{A}$ ist simultan diagonalisierbar.

(ii) V besitzt eine Basis aus simultanen Eigenvektoren von $\mathscr{A}$.

(iii) Sind $\lambda_1,\dots,\lambda_k$ die verschiedenen simultanen Eigenwerte von $\mathscr{A}$, so gilt

$$V = V_{\lambda_1}(\mathscr{A}) \oplus \cdots \oplus V_{\lambda_k}(\mathscr{A})$$

(iv) Jedes $\Phi \in \mathscr{A}$ ist diagonalisierbar und $\Phi \circ \Psi = \Psi \circ \Phi$ für alle $\Phi, \Psi \in \mathscr{A}$.

Beweis. (i)$\Longleftrightarrow$(ii): Proposition 6.3.5.

(ii)$\Longrightarrow$(iii): Wegen (ii) enthält $V_{\lambda_1}(\mathscr{A}) \cup \cdots \cup V_{\lambda_k}(A)$ eine Basis von V, also gilt insbesondere $V = \langle V_{\lambda_1}(\mathscr{A}) \cup \cdots \cup V_{\lambda_k}(A)\rangle = V_{\lambda_1}(\mathscr{A}) + \cdots + V_{\lambda_k}(A)$. Nach Proposition 6.3.11 ist die Summe direkt.

(iii)$\Longrightarrow$(i): Sind $\lambda_1,\dots,\lambda_k$ wie in (iii), und $(v_1^{(1)},\dots,v_{d_1}^{(1)})$, $\dots$, $(v_1^{(k)},\dots,v_{d_k}^{(k)})$ geordnete Basen von $V_{\lambda_1}(\mathscr{A}), \dots V_{\lambda_k}(\mathscr{A})$, so ist

$$\mathscr{B} := (v_1^{(1)},\dots,v_{d_1}^{(1)},\dots,v_1^{(k)},\dots,v_{d_k}^{(k)})$$

eine geordnete Basis von V, und für $\Phi \in \mathscr{A}$ gilt

$$D_{\mathscr{B}}(\Phi) = \operatorname{diag}(\lambda_1(\Phi),\dots,\lambda_1(\Phi),\dots,\lambda_k(\Phi),\dots,\lambda_k(\Phi)),$$

also ist $\mathscr{A}$ simultan diagonalisierbar bzgl. $\mathscr{B}$.

(i)$\Longrightarrow$(iv): Proposition 6.3.8.

(iv)$\Longrightarrow$(iii) Wir argumentieren mit Induktion nach $n := \dim_{\mathbb{K}} V$. Falls $n \le 1$, so ist nichts zu zeigen. Sei also $n \ge 2$. Falls $V = V_\lambda(\mathscr{A})$ für ein $\lambda : \mathscr{A} \to \mathbb{K}$, so sind wir fertig. Andernfalls existiert ein $\Phi \in \mathscr{A}$ mit mindestens 2 verschiedenen Eigenwerten, und wir nummerieren diese durch als $\lambda_1,\dots,\lambda_k$ mit $k \ge 2$. Wir definieren dann

$$U := V_{\lambda_1}(\Phi) \quad \text{und} \quad W := V_{\lambda_2}(\Phi) \oplus \cdots \oplus V_{\lambda_k}(\Phi),$$

so dass $V = U \oplus W$ eine Zerlegung in nicht-triviale Φ-invariante Unterräume ist. Nach Lemma 6.3.12 sind U und W invariant unter jedem $\Psi \in \mathscr{A}$. Sei

$$\mathscr{A}_U := \{\Psi_U \mid \Psi \in \mathscr{A}\} \subseteq \operatorname{End}_{\mathbb{K}}(U) \quad \text{und} \quad \mathscr{A}_W := \{\Psi_W \mid \Psi \in \mathscr{A}\} \subseteq \operatorname{End}_{\mathbb{K}}(W).$$

Nach Übung 6.2.19 erfüllen $\mathscr{A}_U$ und $\mathscr{A}_W$ die Bedingung (iv). Nach Induktionsvoraussetzung zerfallen daher U und W in simultane Eigenräume bzgl. $\mathscr{A}_U$ bzw. $\mathscr{A}_W$, und folglich zerfällt V in simultane Eigenräume bzgl. $\mathscr{A}$. □

Der Satz motiviert die folgende Definition:

Definition 6.3.14. Eine kommutative Unteralgebra $\mathscr{A} \subseteq \operatorname{End}_{\mathbb{K}}(V)$ (bzw. $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$) heißt eine *torale Unteralgebra*, falls jedes ihrer Elemente diagonalisierbar ist. Eine torale Unteralgebra $\mathscr{A} \subseteq \operatorname{End}_{\mathbb{K}}(V)$ heißt *maximal toral*, wenn es keine torale Unteralgebra $\mathscr{B}$ mit $\mathscr{B} \supsetneq \mathscr{A}$ gibt.

Korollar 6.3.15. *Eine Teilmenge $\mathscr{A} \subseteq \operatorname{End}_{\mathbb{K}}(V)$ (bzw. $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$) ist genau dann simultan diagonalisierbar, wenn sie in einer maximal toralen Unteralgebra enthalten ist.*

Beweis. Nach Satz 6.3.13 ist jede torale Unteralgebra (also auch jede ihrer Teilmengen) simultan diagonalisierbar.

Ist umgekehrt $\mathscr{A}$ simultan diagonalisierbar, so folgt aus Satz 6.3.13 und Bemerkung 6.3.7, dass die von $\mathscr{A}$ erzeugte Unteralgebra toral ist. Es sei nun $\mathscr{B} \supset \mathscr{A}$ die torale Unteralgebra von maximal möglicher Dimension. Diese existiert, da $\operatorname{End}_{\mathbb{K}}(V)$ endlichdimensional ist, und ist offensichtlich maximal toral. □

Es stellt sich daher nun die Frage, wie man die maximalen toralen Unteralgebren von $\mathrm{End}_{\mathbb{K}}(V)$ (bzw. $\mathbb{K}^{n\times n}$ charakterisieren kann.

Bemerkung 6.3.16. Es sei $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$ eine torale Unteralgebra. Nach Satz 6.3.13 existiert dann ein $S \in \mathrm{GL}_n(\mathbb{R})$, so dass

$$S\mathscr{A}S^{-1} := \{SAS^{-1} \mid A \in \mathscr{A}\} \subseteq \mathrm{Diag}_n(\mathbb{K}).$$

Nun ist die Abbildung

$$\mathscr{A} \to S\mathscr{A}S^{-1}, \quad A \mapsto SAS^{-1}$$

aber ein linearer Isomorphismus (sogar ein Isomorphismus von $\mathbb{K}$-Algebren), und folglich $\dim \mathscr{A} = \dim S\mathscr{A}S^{-1} \leq \dim \mathrm{Diag}_n(\mathbb{K}) = n$, und es gilt Gleichheit genau dann, wenn $S\mathscr{A}S^{-1} = \mathrm{Diag}_n(\mathbb{K})$.

Satz 6.3.17 (Konjugationssatz für maximale torale Unteralgebren)**.** *Für eine torale Unteralgebra $\mathscr{A} \subseteq \mathbb{K}^{n\times n}$ sind äquivalent:*

(i) $\dim \mathscr{A} = n$.

(ii) Es existiert $S \in \mathrm{GL}_n(\mathbb{K})$ *mit* $S\mathscr{A}S^{-1} = \mathrm{Diag}_n(\mathbb{K})$.

(iii) $\mathscr{A}$ *ist maximal toral.*

Sind $\mathscr{A}$ und $\mathscr{B}$ zwei maximal torale Unteralgebren von $\mathbb{K}^{n\times n}$, so existiert $S \in \mathrm{GL}_n(\mathbb{K})$ mit $S\mathscr{A}S^{-1} = \mathscr{B}$, und insbesondere sind $\mathscr{A}$ und $\mathscr{B}$ isomorph zueinander.

Beweis. Wir haben gerade gesehen, dass (i) $\iff$ (ii).

(i) $\implies$ (iii) Sei $\dim \mathscr{A} = n$. Falls $\mathscr{B} \supsetneq \mathscr{A}$ eine größere torale Unteralgebra wäre, so wäre einerseits $\dim \mathscr{B} \geq n+1$, andererseits existierte $S \in \mathrm{GL}_n(\mathbb{K})$ mit $S\mathscr{B}S^{-1} \subseteq \mathrm{Diag}_n(\mathbb{K})$ und folglich $\dim \mathscr{B} \leq n$.

(iii) $\implies$ (i) Sei $\mathscr{A}$ maximal toral und $S \in \mathrm{GL}_n(\mathbb{K})$ mit $S\mathscr{A}S^{-1} \subseteq \mathrm{Diag}_n(\mathbb{K})$. Nach der letzten Bemerkung gilt stets $\dim \mathscr{A} \leq n$; wäre $\dim \mathscr{A} < n$, so wäre $S\mathscr{A}S^{-1} \subsetneq \mathrm{Diag}_n(\mathbb{K})$. Dann wäre aber

$$\mathscr{B} := S^{-1}\mathrm{Diag}_n(\mathbb{K})S$$

eine torale Unteralgebra, die $\mathscr{A}$ echt enthält, im Widerspruch zur Maximalität. □

Wir verstehen also diejenigen kommutativen Unteralgebren von $\mathbb{K}^{n\times n}$, die aus diagonalisierbaren Elementen bestehen. Dies ist ein erster wichtiger Schritt zu einem tieferen Verständnis der Struktur von $\mathbb{K}^{n\times n}$ (bzw. der dazu isomorphen allgemeinen linearen Algebra $\mathrm{End}_{\mathbb{K}}(V)$). Hier ist ein weiterer Schritt.

Definition 6.3.18. Sei $A \in \mathbb{K}^{n\times n}$. Der *Zentralisator*[6] von A in $\mathbb{K}^{n\times n}$ ist gegeben durch

$$\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A) := \{B \in \mathbb{K}^{n\times n} \mid AB = BA\}.$$

Man kann sich überlegen, dass der Zentralisator einer Matrix stets eine $\mathbb{K}$-Unteralgebra ist.

Satz 6.3.19 (Zentralisatoren diagonalisierbarer Matrizen)**.** *Sei $A \in \mathbb{K}^{n\times n}$ eine diagonalisierbare Matrix.*

(i) Ist $|\mathrm{spec}_{\mathbb{K}}(A)| = n$*, so ist* $\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$ *eine maximale torale Unteralgebra von* $\mathbb{K}^{n\times n}$.

[6] engl. „centraliser“ (BE) oder „centralizer “ (AE).

(ii) Ist $|\mathrm{spec}_{\mathbb{K}}(A)| < n$*, so ist* $\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$ *nicht kommutativ (bzgl. Matrizenmultiplikation), von Dimension* $> n$ *und erhält eine nicht-diagonalisierbare Matrix.*

Beweis. (i) Zerlege $V = \mathbb{K}v_1 \oplus \cdots \oplus \mathbb{K}v_n$, wobei v_i ein Eigenvektor von A zum Eigenwert λ_i ist. Ist nun $B \in \mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$, so erhält B nach Lemma 6.3.12 diese Eigenräume, was gerade bedeutet, dass $v_1, \ldots, v_n$ auch Eigenvektoren von B sind. Setzen wir $S := (v_1, \ldots, v_n) \in \mathbb{K}^{n\times n}$, so ist $S^{-1}BS$ diagonal. Wir sehen also, dass

$$S^{-1}\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)S \subseteq \mathrm{Diag}_n(\mathbb{K}) \quad \Longrightarrow \quad \mathrm{Cent}_{\mathbb{K}^{n\times n}}(A) \subseteq S\mathrm{Diag}_n(\mathbb{K})S^{-1} =: \mathscr{A}.$$

Insbesondere gilt auch $A \in \mathscr{A}$, und da $\mathscr{A}$ abelsch ist, ist andererseits $\mathscr{A} \subseteq \mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$, also muss Gleichheit gelten. Nach Satz 6.3.17 ist aber $\mathscr{A}$ eine maximal torale Unteralgebra.

(ii) Ist A diagonalisierbar und $\mathrm{spec}_{\mathbb{K}}(A) < n$, so ist V die direkte Summe von weniger als n Eigenräumen von A. Folglich gibt es dann mindestens einen Eigenraum $V_{\lambda_1}(A)$ der Dimension ≥ 2. Seien $V_{\lambda_2}(A)$, …, $V_{\lambda_k}(A)$ die übrigen Eigenräume. Ist nun $\Psi_1 \in \mathrm{End}(V_{\lambda_1}(A))$ beliebig und sind $\mu_2, \ldots, \mu_n \in \mathbb{K}$, so existiert eine eindeutige Matrix B mit

$$Bv = \begin{cases} \Psi_1(v), & v \in V_{\lambda_1}(A) \\ \mu_j v, & v \in V_{\lambda_j}(A),\ j \geq 2 \end{cases},$$

und nach Konstruktion gilt $AB = BA$. Jede solche Matrix liegt also im Zentralisator von A. Dies zeigt, dass $\dim \mathrm{Cent}_{\mathbb{K}^{n\times n}}(A) \geq (\dim V_{\lambda_1}(A))^2 - \dim V_{\lambda_1}(A) + n > n$. Da $\mathrm{End}(V_{\lambda_1}(A))$ nicht kommutativ ist, ist auch $\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$ nicht kommutativ. Eine nicht-diagonalisierbare Matrix erhält man, indem man Ψ_1 nicht-diagonalisierbar wählt - wir wissen ja, das nicht-diagonalisierbare (2×2)-Matrizen existieren, z.B. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. □

Korollar 6.3.20. *Für eine diagonalisierbare Matrix* $A \in \mathbb{K}^{n\times n}$ *sind äquivalent:*

(i) $|\mathrm{spec}_{\mathbb{K}}(A)| = n$.

(ii) $\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$ *ist kommutativ.*

(iii) $\dim \mathrm{Cent}_{\mathbb{K}^{n\times n}}(A) \leq n$.

(iv) $\mathrm{Cent}_{\mathbb{K}^{n\times n}}(A)$ *ist eine maximal torale Unteralgebra.* □

Bemerkung 6.3.21. Hat $\mathbb{K}$ mindestens n verschiedene Elemente $\lambda_1, \ldots, \lambda_n$, so ist umgekehrt jede maximale torale Unteralgebra $\mathscr{A}$ von $\mathbb{K}^{n\times n}$ der Zentralisator einer Matrix mit n verschiedenen Eigenwerten: Wir können ja $\mathscr{A}$ schreiben als $\mathscr{A} = S\mathrm{Diag}_n(\mathbb{K})S^{-1}$ für eine Matrix $S \in \mathrm{GL}_n(\mathbb{K})$, und es gilt dann

$$\mathscr{A} = \mathrm{Cent}_{\mathbb{K}^{n\times n}}(S \cdot \mathrm{diag}(\lambda_1, \ldots, \lambda_n) \cdot S^{-1}).$$

Bemerkung 6.3.22. Aus Satz 6.3.19 folgt, dass die Dimension des Zentralisators einer diagonalisierbaren reellen Matrix unstetig variiert. Damit ist das Folgende gemeint: Wir definieren eine Funktion $D : \mathbb{R}^{n\times n} \to \mathbb{N}$ durch $D(A) := \dim \mathrm{Cent}_{\mathbb{R}^{n\times n}}(A)$. Wir sagen, dass eine Folge $(A_k) \in \mathbb{R}^{n\times n}$ gegen eine Matrix $A \in \mathbb{R}^{n\times n}$ *konvergiert*, geschrieben $A_k \to A$, falls für alle $i, j \in \{1, \ldots, n\}$ die Folge der (i,j)-ten Einträge von (A_k) für $k \to \infty$ gegen den (i,j)-ten Eintrag von A konvergiert. Ist z.B.

$$A_k := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2+\frac{1}{k} \end{pmatrix} \quad \text{und} \quad A := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

so gilt $A_k \to A$. Andererseits gilt $D(A_k) = 3$ und $D(A) > 3$, also $D(A_k) \not\to D(A)$. In diesem Sinne ist also die Funktion D unstetig.

Man kann Satz 6.3.13 benutzen, um die Diagonalisierbarkeit von Endomorphismen zu beweisen. Dazu muss man nämlich nur zeigen, dass der gegebene Endomorphismus mit hinreichend vielen simultan diagonalisierbaren Endomorphismen vertauscht:

Satz 6.3.23 (Diagonalisierbarkeit durch Kommutativität)**.** *Sei $\mathscr{A} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ simultan diagonalisierbar, so dass jeder simultane Eigenraum von $\mathscr{A}$ die Dimension 1 hat. Falls $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ mit jedem $\Psi \in \mathscr{A}$ vertauscht (d.h. $\Phi \circ \Psi = \Psi \circ \Phi$), dann ist auch Φ diagonalisierbar und $\mathscr{A} \cup \{\Phi\}$ ist simultan diagonalisierbar.*

Beweis. Nach Annahme gilt $V = V_1 \oplus \cdots \oplus V_n$, wobei $V_1, \ldots, V_n$ die (nach Annahme) eindimensionalen simultanen Eigenräume von $\mathscr{A}$ sind. Nach Lemma 6.3.12 sind die Eigenräume der Elemente von $\mathscr{A}$ invariant unter Φ, und da $V_1, \ldots, V_n$ Schnitte solcher Eigenräume sind, sind auch diese invariant. Für $j \in \{1, \ldots, n\}$ ist wegen $\dim V_j = 1$ die Abbildung $\Phi_{V_j} : V_j \to V_j$ durch Multiplikation mit einer Konstanten λ_j gegeben. Dann ist aber $V_j \subseteq V_{\lambda_j}(\Phi)$, und folglich ist V die direkte Summe der Eigenräume von Φ. □

Der Spezialfall $|\mathscr{A}| = 1$ liefert:

Korollar 6.3.24. *Es seien $\Phi, \Psi \in \mathrm{End}_{\mathbb{K}}(V)$. Besitzt Ψ die maximal mögliche Anzahl von $\dim_{\mathbb{K}}(V)$ verschiedenen Eigenwerten und gilt $\Phi \circ \Psi = \Psi \circ \Phi$, so ist Φ diagonalisierbar.* □

Ist $|\mathbb{K}| \geq \dim V$, so gilt nach Bemerkung 6.3.21 auch die Umkehrung: Ist Φ diagonalisierbar, so finden wir ein Ψ mit $\dim_{\mathbb{K}}(V)$ verschiedenen Eigenwerten, das mit Φ vertauscht. In der Praxis ist es aber oft einfacher, mehrere kommutierende Endomorphismen wie in Satz 6.3.23 zu finden.

[14.02.24]

Zum Abschluss dieses Abschnitte wollen wir noch eine wichtige Anwendung von Satz 6.3.23 diskutieren.

Bemerkung 6.3.25 (Harmonische Funktionen und Laplace-Operator)**.** Es sei $\mathcal{G} = (V, E)$ ein einfacher gerichteter Graph. Wir erinnern daran, dass dies bedeutet, dass V eine nichtleere Menge (die *Eckenmenge*) und E eine Teilmenge von $V \times V$ (die *Menge der gerichteten Kanten*) ist. Ist $(v_1, v_2) \in E$ so nennen wir v_2 ein *Kind* von v_1 und schreiben $v_1 \to v_2$. Wir nennen eine Funktion $f : V \to \mathbb{C}$ *harmonisch*, wenn der Funktionswert von f an jedem Knoten v genau der Durchschnittswert der Funktionswerte der Kinder ist. Definieren wir den *Grad*[7] einer Ecke x als

$$|x| := |\{y \mid x \to y\}|,$$

so ist eine Funktion also $f : V \to \mathbb{C}$ also genau dann harmonisch, wenn für alle $x \in V$ die Gleichung

$$f(x) = \frac{1}{|x|} \sum_{x \to y} f(y)$$

gilt. Die harmonischen Funktionen auf $\mathcal{G}$ bilden einen Untervektorraum $\mathcal{H}(\mathcal{G})$ des $\mathbb{C}$-Vektorraum $\mathrm{Abb}(V, \mathbb{C})$ der Abbildungen von V nach $\mathbb{C}$. Zum Beweis überlegt man sich, dass die Abbildung

$$\Delta_{\mathcal{G}} : \mathrm{Abb}(V, \mathbb{C}) \to \mathrm{Abb}(V, \mathbb{C}), \quad \Delta(f)(x) := \sum_{x \to y} (f(x) - f(y)) = |x| f(x) - \sum_{x \to y} f(y).$$

linear ist und $\mathcal{H}(\mathcal{G}) = \ker(\Delta)$ gilt. Die lineare Abbildung $\Delta_{\mathcal{G}}$ heißt der *Laplace-Operator*[8] auf $\mathcal{G}$. Die harmonischen Funktionen sind also genau die Eigenvektoren von $\Delta_{\mathcal{G}}$ zum Eigenwert 0. Allgemeiner interessiert man sich auch für beliebige Eigenvektoren von $\Delta_{\mathcal{G}}$. Da es sich bei diesen Eigen„vektoren“ um Funktionen handelt, bezeichnet man sie auch als *Eigenfunktionen*.

Wir werden uns im Folgenden auf den Fall beschränken, dass V endlich ist. In diesem Fall ist $\mathrm{Abb}(V, \mathbb{C}) \cong \mathbb{C}^{|V|}$ endlichdimensional. Für eine Ecke $v \in V$ bezeichne $\delta_v : V \to \mathbb{C}$ die Funktion mit

$$\delta_v(w) = \begin{cases} 1, & \text{falls } v = w \\ 0, & \text{falls } v \neq w. \end{cases}$$

Für $f \in \mathrm{Abb}(V, \mathbb{C})$ gilt dann

$$f(x) = \sum_{v \in V} f(v) \delta_v,$$

und folglich ist $B = \{\delta_v \mid v \in V\}$ eine Basis von $\mathrm{Abb}(V, \mathbb{C})$. Nummerieren wir B durch, so erhalten wir eine geordnete Basis $\mathcal{B} = (\delta_{v_1}, \ldots, \delta_{v_n})$ und es gilt

$$D_{\mathcal{B}}(\Delta_{\mathcal{G}}) = \mathrm{diag}(|v_1|, \ldots, |v_n|) - A,$$

wobei A die Adjazenzmatrix von $\mathcal{G}$ ist. Es stellt sich nun die Frage, ob $\Delta_{\mathcal{G}}$ diagonalisierbar ist, oder mit anderen Worten ob jede Funktion als Linearkombination von Eigenfunktionen geschrieben werden kann. Falls dies der Fall ist, so möchte man Funktionen in $\mathrm{Abb}(V, \mathbb{C})$ explizit als Linearkombinationen von Eigenfunktionen darstellen. Dieses „Zerlegen in Eigenfunktionen“ bezeichnet man als *harmonische Analyse*.

[7] Engl. „degree“ oder „valency“, im Deutschen daher manchmal auch „Valenz“ genannt

[8] Dieser Operator ist bis auf Vorzeichen eine diskrete Version des gleichnamigen Differentialoperators aus der Analysis.

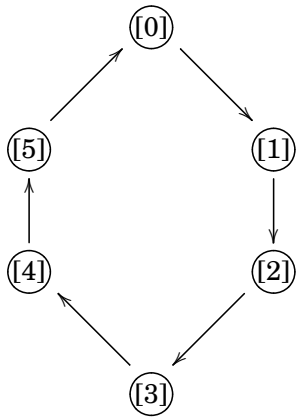
Für allgemeine Graphen kann es ziemlich schwierig sein, explizite Eigenfunktionen zu konstruieren. In besonders symmetrischen Fällen kann man aber mit einem Trick, der auf simultaner Diagonalisierbarkeit beruht, Eigenfunktionen konstruieren. Das wollen wir nun vorführen. Wir führen zunächst einige Beispiele für besonders symmetrische Graphen ein:

Definition 6.3.26. Sei G eine beliebige Gruppe und S ein beliebiges Erzeugendensystem von G. Wir definieren den *Cayley-Graphen* $\mathrm{Cay}(G,S)$ als den Graphen mit Eckenmenge $V = G$ und Kantenmenge

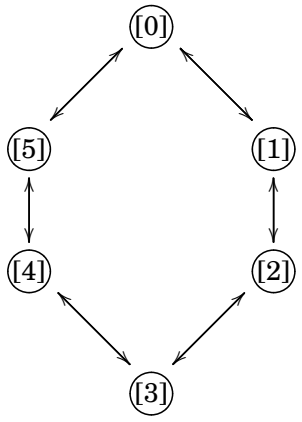
$$E = \{(g, gs) \mid g \in G, s \in S\}.$$

Wir verbinden also zwei Gruppenelemente mit einem Pfeil, wenn sie sich nur durch Multiplikation mit einem Element aus S von *rechts* unterscheiden.

Beispiel 6.3.27. Es sei $G = (\mathbb{Z}/6\mathbb{Z}, +)$. Wählen wir $S := \{[1]\}$, so ist $\mathrm{Cay}(G,S)$ ein „orientierter 6-Zykel“:



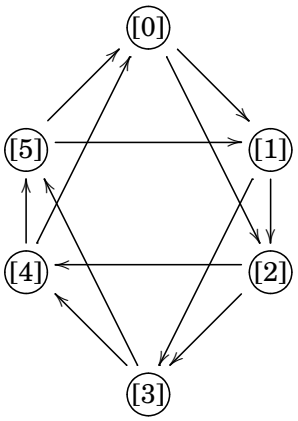
Wählen wir hingegen $S := \{[1],[5]\}$, so ist $\mathrm{Cay}(G,S)$ ein „unorientierter 6-Zykel“:



Allgemein ist $\mathrm{Cay}(\mathbb{Z}/n\mathbb{Z}, \{[1]\})$ ein „orientierter n-Zykel“ und $\mathrm{Cay}(\mathbb{Z}/n\mathbb{Z}, \{[1],[n-1]\})$ ein „unorientierter n-Zykel“. Durch Hinzunahme weiterer Erzeuger kann man kompliziertere Graphen

erzeugen, z.B. sieht $\mathrm{Cay}(\mathbb{Z}/6\mathbb{Z}, \{[1],[2]\})$ so aus:

(6.3.2)



Bemerkung 6.3.28 (Symmetrien von Cayleygraphen)**.** Ist $\mathscr{G} = (V,E)$ ein einfacher gerichteter Graph, so definieren wir seine *Automorphismengruppe*

$$\mathrm{Aut}(\mathscr{G}) = \{f \in \mathrm{Sym}(V) \mid \forall\, v,w \in V : (v,w) \in E \Leftrightarrow (f(v),f(w)) \in E\}.$$

Die Größe dieser Gruppe ist ein Maß dafür, wie „symmetrisch“ der Graph ist. Der orientierte n-Zykel hat z.B. eine n-fache „Drehsymmetrie“, die Symmetriegruppe des unorientierten n-Zykels ist sogar noch größer, nämlich die Dieder-Gruppe D_{2n}.

Ist $\mathscr{G} = \mathrm{Cay}(G,S)$ ein Cayleygraph, so wirkt g auf $V = G$ durch $g.v := gv$. Für $v,w \in V$ gilt dann

$$(v,w) \in E \iff \exists s \in S : vs = w \iff \exists s \in S : gvs = gw \iff (gv,gw) \in E.$$

Folglich erhalten wir einen Gruppenmonomorphismus

$$\iota : G \to \mathrm{Aut}(\mathrm{Cay}(G,S)), \quad \iota(g)(v) := g.v,$$

und es gilt insbesondere $|\mathrm{Aut}(\mathrm{Cay}(G,S))| \geq |G|$. In diesem Sinne sind Cayley-Graphen sehr symmetrisch. Das werden wir im folgenden ausnutzen.

Konstruktion 6.3.29 (Lineare Wirkung auf Funktionenräumen)**.** Wirkt eine Gruppe G auf einer Menge M, so erhalten wir einen Homomorphismus

$$T : G \to \mathrm{End}_{\mathbb{K}}(\mathrm{Abb}(M,\mathbb{K})), \quad T(g)(f)(m) := f(g^{-1}.m).$$

Dass $T(g)$ für jedes $g \in G$ linear ist, folgt unmittelbar aus der Definition. Dass T ein Homomorphismus ist, folgt aus

$$T(gh)(f)(m) = f((gh)^{-1}.m) = f(h^{-1}.(g^{-1}.m)) = (T(h)(f))(g^{-1}.m) = T(g)(T(h)f)(m) = (T(g)\circ T(h))(f)(m).$$

Falls G eine *abelsche* Gruppe ist, dann gilt insbesondere

$$T(g)\circ T(h) = T(gh) = T(hg) = T(h)\circ T(g),$$

d.h. die Endomorphismen $T(g)$ vertauschen miteinander.

Beispiel 6.3.30 (Translationsoperatoren auf endlichen Gruppen)**.** Sei G eine endliche Gruppe (z.B. $G = (\mathbb{Z}/n\mathbb{Z}, +)$). Dann definiert jedes $g \in G$ einen Endomorphismus

$$T(g) : \mathrm{Abb}(G, \mathbb{C}) \to \mathrm{Abb}(G, \mathbb{C}), \quad T(g)(f)(x) := f(g^{-1}x),$$

genannt den *Translationsoperator* von g. Ist G abelsch, so vertauschen diese Translationsoperatoren miteinander.

Im Folgenden bezeichne $T(G) = \{T(g) \mid g \in G\}$ die Menge der Translationsoperatoren. Man überlegt sich leicht, dass die Abbildung $G \to T(G)$, $g \mapsto T(g)$ injektiv ist. Es stellt sich nun heraus, dass simultane Eigenvektoren von $T(G)$ eine einfache algebraische Beschreibung besitzen:

Proposition 6.3.31 (Homomorphismen als simultane Eigenvektoren)**.** *Sei G eine endliche Gruppe, $\chi : G \to (\mathbb{C}^\times, \cdot)$ ein Gruppenhomomorphismus und*

$$\lambda_\chi : T(G) \to \mathbb{C}, \quad \lambda_\chi(T(g)) := \chi(g)^{-1}. \tag{6.3.3}$$

Dann ist λ_χ ein simultaner Eigenwert von $T(G)$, und der zugehörige Eigenraum ist gegeben durch

$$V_{\lambda_\chi}(\mathscr{A}) = \mathbb{C} \cdot \chi.$$

Beweis. Für alle $g, x \in G$ gilt

$$T(g)(\chi)(x) = \chi(g^{-1}x) = \chi(g)^{-1}\chi(x).$$

Folglich ist $\mathbb{C} \cdot \chi \subseteq V_{\lambda_\chi}(\mathscr{A})$, und λ_χ ein simultaner Eigenwert. Umgekehrt sei $\eta \in V_{\lambda_\chi}(\mathscr{A})$. Dann gilt für alle $x \in G$, dass

$$\eta(x) = \eta((x^{-1})^{-1}e) = T(x^{-1})(\eta)(e) = \lambda_\chi(T(x^{-1}))\eta(e) = \chi(x)\eta(e).$$

Folglich ist $\eta = \eta(e) \cdot \chi \in \mathbb{C}\chi$, und daher $V_{\lambda_\chi}(\mathscr{A}) = \mathbb{C} \cdot \chi$. □

Beispiel 6.3.32 (Zyklische Gruppen und Einheitswurzeln)**.** Es sei $G = (\mathbb{Z}/n\mathbb{Z}, +)$. Ist $\chi : G \to \mathbb{C}^\times$ ein Homomorphismus, so gilt

$$\chi([1])^n = \chi(n \cdot [1]) = \chi([0]) = 1,$$

d.h. $\chi([1])$ muss eine komplexe Zahl ζ mit $\zeta^n = 1$ sein. Solche Zahlen nennt man *nte Einheitswurzeln*, und es gibt genau n solche $n$ten Einheitswurzeln, nämlich

$$\zeta_k := e^{\frac{2\pi i k}{n}} = \cos(2\pi k/n) + i \sin(2\pi k/n) \quad (k \in \{0, \ldots, n-1\})$$

Geometrisch sind dies gerade die Ecken des im Einheitskreis einbeschriebenen regelmäßigen n-Ecks. Ist $\chi_k : G \to \mathbb{C}^\times$ ein Homomorphismus mit $\chi_k([1]) = \zeta_k$, so muss gelten

$$\chi_k([m]) = \chi_k(m \cdot [1]) = \chi([1])^m = \zeta_k^m. \tag{6.3.4}$$

Umgekehrt liefert die Formel (6.3.4) einen Homomorphismus $\chi_k : G \to \mathbb{C}^\times$. Es gilt also

$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^\times) = \{\chi_0, \ldots, \chi_{n-1}\}.$$

Wir haben daher n paarweise verschiedene simultane Eigenvektoren für $T(G)$ gefunden. Die zugehörigen simultanen Eigenwerte $\lambda_{\chi_0}, \ldots, \lambda_{\chi_{n-1}}$ sind dann ebenfalls paarweise verschieden, denn es gilt $\lambda_{\chi_i} = \lambda_{\chi_j} \iff \chi_i = \chi_j$. Daraus folgt nun mit Satz 6.3.13, dass $T(G)$ simultan diagonalisierbar mit eindimensionalen Eigenräumen $\mathbb{C}\chi_0$, $\mathbb{C}\chi_1$, $\ldots \mathbb{C}\chi_{n-1}$. Insbesondere ist dann $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^\times) = \{\chi_0, \ldots, \chi_{n-1}\}$ eine Basis von $\mathrm{Abb}(G, \mathbb{C})$, die aus simultanen Eigenfunktionen der Translationsoperatoren besteht.

Mit Korollar 6.3.23 folgt:

Korollar 6.3.33. *Es sei $G := \mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$ und $W := \mathrm{Abb}(G, \mathbb{C})$. Vertauscht $\Phi \in \mathrm{End}_{\mathbb{C}}(W)$ mit allen Translationsoperatoren $T(g)$, so ist Φ diagonalisierbar und $(\chi_0, \dots, \chi_{n-1})$ ist eine geordnete Basis von Eigenvektoren von Φ.*

Notation 6.3.34. Da $\{\chi_0, \dots, \chi_{n-1}\}$ eine Basis von W ist, können wir jede Funktion $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ darstellen als

$$f([m]) = \sum_{k=0}^{n-1} a_k \chi_k([m]) = \sum_{k=0}^{n-1} a_k e^{2\pi i k m/n} \quad \text{für gewisse } a_0, \dots, a_{n-1} \in \mathbb{C}.$$

Die Koeffizienten $a_0, \dots, a_{n-1}$ heißen die *Fourier-Koeffizienten* von f.

Bemerkung 6.3.35 (Verallgemeinerung auf nicht-zyklische Gruppen)**.** Die Aussage von Korollar 6.3.33 gilt für jede endliche abelsche Gruppe G mit $|\mathrm{Hom}(G, \mathbb{C}^\times)| = |G|$. Man kann zeigen, dass *jede* endliche abelsche Gruppe diese Eigenschaft hat – dies folgt aus der Tatsache, dass jede endliche abelsche Gruppe ein direktes Produkt von zyklischen Gruppen ist, die wir hier aber nicht beweisen wollen. Es gilt sogar für endliche abelsche Gruppen stets, dass $\mathrm{Hom}(G, \mathbb{C}^\times) \cong G$.

Wir nennen einen Endomorphismus Φ wie in Korollar 6.3.33 *translationsinvariant*. Es stellt sich heraus, dass der Laplace-Operator auf einem beliebigen Cayley-Graphen von G diese Eigenschaft hat:

Bemerkung 6.3.36 (Translationsinvarianz von Laplace-Operatoren auf Cayley-Graphen)**.** Es sei G eine beliebige Gruppe und S ein symmetrisches Erzeugendensystem von G. Wir behaupten, dass der Laplace-Operator Δ von $\mathrm{Cay}(G, S)$ translationsinvariant ist. Zum Beweis verwenden wir die Beobachtung, dass für alle Ecken $v \in G$ des Cayley-Graphs der Grad druch $|v| = |S|$ gegeben ist. Für $f \in \mathrm{Abb}(G, \mathbb{C})$ und $g, v \in G$ gilt daher

$$\begin{aligned}(T(g) \circ \Delta)(f)(v) &= \Delta(f)(g^{-1}v) = |S| f(g^{-1}v) - \sum_{s \in S} f(g^{-1}vs) \\ &= |S| T(g)(f)(v) - \sum_{s \in S} T(g)(f)(vs) = \Delta(T(g)(f))(v) = (\Delta \circ T(g))(f)(v),\end{aligned}$$

und daher $T(g) \circ \Delta = \Delta \circ T(g)$.

Gemeinsam mit Korollar 6.3.33 ergibt sich daraus:

Korollar 6.3.37. *Ist $G = (\mathbb{Z}/n\mathbb{Z}, +)$ und S ein beliebiges Erzeugendensystem von G, so ist der Laplace-Operator von $\mathrm{Cay}(G, S)$ diagonalisierbar mit Eigenfunktionen $\chi_0, \dots, \chi_{n-1}$ wie in Beispiel 6.3.32.*

Bemerkung 6.3.38 (Spektrum des Laplace-Operators)**.** Es sei weiterhin $G = (\mathbb{Z}/n\mathbb{Z}, +)$ und S ein beliebiges Erzeugendensystem von G. Nach Korollar 6.3.37 gilt dann

$$\mathrm{spec}_{\mathbb{C}}(\Delta) = \{\lambda_0, \dots, \lambda_{n-1}\}, \quad \text{wobei} \quad \Delta\chi_j = \lambda_j \chi_j.$$

Während die Eigenfunktionen nur von G abhängen, hängen die Eigenwerte von S ab. Um diese zu berechnen, können wir verwenden, dass

$$\chi_j([0]) = e^{2\pi i \cdot 0/n} = 1 \quad \text{für alle } j \in \{0, \dots, n-1\}$$

gilt. Wir erhalten dann

$$\lambda_j = \lambda_j \chi_j([0]) = \Delta\chi_j([0]) = |S|\chi_j([0]) - \sum_{s\in S} \chi_j(s) = |S| - \sum_{s\in S} \chi_j(s) = \sum_{s\in S} 1 - \chi_j(s),$$

also

$$\operatorname{spec}_{\mathbb{C}}(\Delta) = \left\{ \sum_{[s]\in S} 1 - e^{2\pi i s j/n} \mid j \in \{0,\dots,n-1\} \right\}.$$

Beispiel 6.3.39. Wir betrachten den orientierten und den unorientierten n-Zykel:

(i) Ist $G = \mathbb{Z}/n\mathbb{Z}$ und $S = \{[1]\}$, so gilt $\chi_j([1]) = e^{2\pi i j/n}$ und daher

$$\operatorname{spec}_{\mathbb{C}}(\Delta_{\mathrm{Cay}(G,S)}) = \{0, 1 - e^{2\pi i/n}, 1 - e^{4\pi i/n}, \dots, 1 - e^{2\pi i(n-1)/n}\}.$$

In diesem Fall gilt es n verschiedene komplexe Eigenwerte. Da 1 und -1 die einzigen reellen $n$ten Einheitswurzeln sind, gibt es maximal zwei reelle Eigenwerte. 0 ist immer ein reeller Eigenwert und der zugehörige Eigenraum ist der Raum der harmonischen Funktionen. Da dieser 1-dimensional ist, sind nur die konstanten Funktionen harmonisch. Falls n gerade ist, so ist auch $2 = 1 - e^{\pi i}$ ein reeller Eigenwert, und in diesem Fall sind die zugehörigen Eigenfunktionen gegeben durch

$$\chi_{n/2}([m]) = (-1)^m.$$

(ii) Ist $G = \mathbb{Z}/n\mathbb{Z}$ und $S = \{[1],[5]\}$, so gilt $\chi_j([1]) + \chi_j([n-1]) = e^{2\pi i j/n} + e^{-2\pi i j/n} = 2\cos(2\pi j/n)$ und daher

$$\operatorname{spec}_{\mathbb{C}}(\Delta_{\mathrm{Cay}(G,S)}) = \{0, 2(1-\cos(2\pi/n)), 2(1-\cos(4\pi/n)), \dots, 2(1-\cos(2(n-1)\pi/n))\}.$$

Im symmetrischen Fall sind also alle Eigenwerte reell und nicht-negativ. Beachte, dass

$$\cos(2(n-k)\pi/n) = \cos(-2(n-k)\pi/n) = \cos(2k\pi/n - 2\pi) = \cos(2k\pi/n),$$

d.h. χ_k und χ_{n-k} haben denselben Eigenwert. Wir erhalten daher

$$\operatorname{spec}_{\mathbb{C}}(\Delta_{\mathrm{Cay}(G,S)}) = \operatorname{spec}_{\mathbb{R}}(\Delta_{\mathrm{Cay}(G,S)}) = \begin{cases} \{2(1-\cos(2\pi k/n)) \mid 0 \le k \le n/2\}, & n \text{ gerade}, \\ \{2(1-\cos(2\pi k/n)) \mid 0 \le k \le (n-1)/2\}, & n \text{ ungerade}. \end{cases}$$

Der Laplace-Operator hat in diesem Fall also $(n+2)/2$ (falls n gerade) bzw. $(n+1)/2$ (falls n ungerade) positive reelle Eigenwerte. Obwohl fast alle Eigenwerte (mit höchstens zwei Ausnahmen) die algebraische Vielfachheit 2 haben, ist er diagonalisierbar. Wieder sind alle harmonischen Funktionen konstant.

Übung 6.3.40. Berechnen Sie das Spektrum des Laplace-Operators des Graphen (6.3.2). Für welche Erzeugendensystem S von $\mathbb{Z}/n\mathbb{Z}$ sind alle Eigenwerte des zugehörigen Laplace-Operators reell?

Bemerkung 6.3.41 (Fourierbild des Laplace-Operators)**.** Ist $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ eine beliebige Funktion mit Fourier-Koeffizienten $a_0, \dots, a_{n-1}$, so gilt

$$\Delta f([m]) = \Delta(\sum_{k=0}^{n-1} a_k \chi_k)([m]) = \sum_{k=0}^{n-1} \lambda_k a_k \chi_k([m]) = \sum_{k=0}^{n-1} \lambda_k a_k e^{2\pi i k m/n}.$$

Anwenden des Laplace-Operators multipliziert also den $k$ten Fourierkoeffizienten mit λ_k.

Zum Abschluss diskutieren wir eine physikalische Anwendung:

Bemerkung 6.3.42 (Wärmeleitung auf Graphen)**.** Wir diskutieren ein stark vereinfachtes Modell von Wärmeleitung in einem Netzwerk. Wir nehmen an, dass unser Netzwerk durch einen endlichen Graphen $\mathcal{G} = (V, E)$ modelliert ist. Da Wärmeleitung ungerichtet ist, nehmen wir weiter an, dass (v_1, v_2) genau dann eine Kante des Graphen ist, wenn (v_2, v_1) eine Kante ist, wie dies etwa im Fall des unorientierten Zykels der Fall ist. Für eine Ecke $x \in V$ bezeichne $f(t,x)$ die Temperatur an der Ecke x zum Zeitpunkt t. Dies definiert eine Funktion $f : \mathbb{R} \times V \to \mathbb{R}$.

Wir nehmen an, dass für jede feste Ecke x die Funktion $t \mapsto f(t,x)$ stetig differenzierbar ist und schreiben

$$\partial_t f(t,x) := \lim_{h \to 0} \frac{f(t+h,x) - f(t,x)}{h}.$$

Weiterhin bezeichne $f_0(x) := f(0,x)$ die Ausgangstemperatur an der Ecke $x \in V$ zur Zeit $t = 0$. Es gilt dann näherungsweise die *diskrete Wärmeleitungsgleichung*[9]

$$\begin{cases} \partial_t f(t,x) = -\Delta_{\mathcal{G}} f(t,x) \\ f(0,x) = f_0(x) \end{cases} \tag{6.3.5}$$

mit Anfangswertbedingung $f(0,x) = f_0(x)$.

Beispiel 6.3.43 (Wärmeleitung im n-Zykel)**.** Es sei $\mathcal{G} = \mathrm{Cay}(\mathbb{Z}/n\mathbb{Z}, \{[1], [n-1]\})$ der unorientierte n-Zykel. Wir geben uns eine beliebige Wärmeverteilung $f_0 : \mathbb{Z}/n\mathbb{Z} \to \mathbb{R}$ vor und bezeichnen mit $a_0, \dots, a_{n-1}$ die Fourierkoeffizienten von f_0. Es sei nun $f : \mathbb{R} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{R}$ eine Funktion, die (6.3.5) erfüllt und es seien $a_0(t), \dots, a_{n-1}(t)$ die Fourierkoeffizienten der Funktion $x \mapsto f(t,x)$. Es gilt dann

$$f(t,x) = \sum_{k=0}^{n-1} a_k(t) \chi_k(x),$$

und daher

$$\partial_t f(t,x) = \sum_{k=0}^{n-1} a_k'(t) \chi_k(x) \quad \text{und} \quad -\Delta_{\mathcal{G}} f(t,x) = -\sum_{k=0}^{n-1} a_k(t) \Delta_{\mathcal{G}} \chi_k(x) = -\sum_{k=0}^{n-1} \lambda_k a_k(t) \chi_k(x).$$

Da die Funktionen $\chi_0, \dots, \chi_{k-1}$ linear unabhängig sind, ist (6.3.5) dann äquivalent zum System

$$\begin{cases} a_k'(t) = -\lambda_k a_k(t) & (k \in \{0, \dots, n-1\}), \\ a_k(0) = a_k & (k \in \{0, \dots, n-1\}). \end{cases} \tag{6.3.6}$$

Dieses System kann man mit Methoden der ANALYSIS I explizit lösen. Dazu beobachtet man zunächst, dass die Funktion $f : \mathbb{R} \to \mathbb{R}$, $f(t) = e^{-\lambda t}$ eine Lösung der Differentialgleichung $f'(t) = -\lambda f(t)$ ist. Ist $g : \mathbb{R} \to \mathbb{R}$ eine andere Lösung dieser Differentialgleichung, so folgt aus der Produktregel, dass

$$(g(t)e^{\lambda t})' = g'(t)e^{\lambda t} + g(t)\lambda e^{\lambda t} = -\lambda g(t)e^{\lambda t} + g(t)\lambda e^{\lambda t} = 0,$$

also ist $g(t)e^{\lambda t}$ konstant. Dies bedeutet, dass $g(t) = Ce^{-\lambda t}$ für ein $C \in \mathbb{R}$ gilt, und setzt man $t = 0$ ein, so erhält man $C = g(0)$. Es gilt also

$$\left\{ \begin{array}{l} f'(t) = -\lambda f(t) \\ f(0) = C \end{array} \right\} \iff f(t) = Ce^{-\lambda t}.$$

[9] Der Laplace-Operator in der Graphentheorie hat aus historischen Gründen das umgekehrte Vorzeichen wie in der Analysis, daher das Minuszeichen.

Das System (6.3.6) besitzt daher die eindeutige Lösung

$$a_k(t) = a_k e^{-\lambda_k t} \quad (k \in \{0, \dots, n-1\}),$$

und (6.3.5) besitzt die eindeutige Lösung

$$f(t,[m]) = \sum_{k=0}^{n-1} a_k e^{-\lambda_k t} e^{2\pi i k m/n}. \tag{6.3.7}$$

Wegen $\lambda_0 = 0$ und $\lambda_k > 0$ für alle $k \geq 1$ erhalten wir für alle $[m] \in \mathbb{Z}/n\mathbb{Z}$ den Grenzwert

$$\lim_{t\to\infty} f(t,[m]) = a_0,$$

und dieser Grenzwert ist unabhängig von $[m]$. Mit der Zeit gleicht sich die Temperatur in den verschiedenen Ecken also immer mehr an.

Zusammenfassung von Abschnitt 6.3

(1) Diagonalisierbare Endomorphismen/Matrizen sind genau dann simultan diagonalisierbar, wenn sie miteinander vertauschen.

(2) Jede simultan diagonalisierbare Menge von Endomorphismen/Matrizen ist in einer maximalen toralen Unteralgebra enthalten, und alle maximalen toralen Unteralgebren sind konjugiert zueinander.

(3) Maximal torale Unteralgebren sind gerade die Zentralisatoren von Endomorphismen/Matrizen ohne mehrfache Eigenwerte.

(4) Man kann die Diagonalisierbarkeit eines Endomorphismen Φ nachweisen (und sogar seine Eigenfunktionen bestimmen), indem man genügend viele diagonalisierbare Endomorphismen findet, die mit Φ vertauschen. Dies hat zahlreiche Anwendungen, z.B. in der harmonischen Analyse.

[16.02.24]

6.4 Die Koeffizienten des charakteristischen Polynoms

In diesem Abschnitt sei $\mathbb{K}$ ein Körper, $A = (a_{ij}) \in \mathbb{K}^{n\times n}$ eine Matrix und $\mathbb{L}$ eine Körperweiterung von $\mathbb{K}$, so dass χ_A über $\mathbb{L}$ in Linearfaktoren zerfällt. Ist z.B. $\mathbb{K} = \mathbb{R}$, so können wir stets $\mathbb{L} := \mathbb{C}$ wählen. Es existieren dann Koeffizienten $c_0(A), \dots, c_{n-1}(A) \in \mathbb{K}$, so dass

$$\chi_A = X^n + c_{n-1}(A)X^{n-1} + \dots c_1(A)X + c_0(A).$$

Ist B eine zu A ähnliche Matrix, so gilt $\chi_B = \chi_A$ und daher $c_k(A) = c_k(B)$ für alle $k \in \{0, \dots, n\}$, d.h. die Koeffizienten sind Ähnlichkeitsinvarianten.

Bemerkung 6.4.1 (1. Formel für die Koeffizienten)**.** Nach der Leibnizformel gilt

$$\chi_A = \sum_{\sigma\in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} (X \cdot \delta_{i\sigma(i)} - a_{i\sigma(i)}), \tag{6.4.1}$$

wobei δ_{ij} das Kronecker-Symbol

$$\delta_{ij} := \begin{cases} 1, & i = j, \\ 0 & i \neq j. \end{cases}$$

bezeichnet. Ausmultiplizieren liefert eine Formel für die $c_k(A)$ als vorzeichenbehaftete Summen von Produkten der Matrixeinträge von A. Die entsprechenden Summen sind dann Ähnlichkeitsinvarianten!

Bemerkung 6.4.2 (2. Formel für die Koeffizienten)**.** Über dem größeren Körper $\mathbb{L}$ zerfällt χ_A als

$$\chi_A(X) = \prod_{j=1}^{n} (X - \lambda_j) \tag{6.4.2}$$

für gewisse $\lambda_1, \dots, \lambda_n \in \mathbb{L}$. Es gilt dann $\mathrm{spec}_{\mathbb{L}}(A) = \{\lambda_1, \dots, \lambda_n\}$, und jeder Eigenwert tritt gemäß seiner algebraischen Vielfachheit (also u.U. mehrfach) auf. Ausmultiplizieren liefert eine Formel für die $c_k(A)$ als vorzeichenbehaftete Summen von Produkten der Eigenwerte von A in $\mathbb{L}$. Die entsprechenden Summen haben dann gleich drei bemerkenswerte Eigenschaften:

(i) Sie liegen in $\mathbb{K}$ (obwohl die Eigenwerte in $\mathbb{L}$ liegen)!

(ii) Sie sind Ähnlichkeitsinvarianten!

(iii) Sie stimmen mit den Ausdrücken aus der 1. Formel überein!

Wir schauen uns die beiden Formel zunächst für kleine Werte von n an.

Beispiel 6.4.3 ((2×2)-Matrizen)**.** Sei $n = 2$. Die erste Formel liefert

$$\chi_A = (X - a_{11})(X - a_{22}) + (-1)(-a_{12})(-a_{21}) = X^2 - (a_{11} + a_{22})X + (a_{11}a_{22} - a_{12}a_{21}),$$

und die zweite Formel liefert

$$\chi_A(X) = (X - \lambda_1)(X - \lambda_2) = X^2 - (\lambda_1 + \lambda_2)X + \lambda_1\lambda_2.$$

Die beiden resultierenden Ähnlichkeitsinvarianten von (2×2)-Matrizen sind also

$$c_0(A) = a_{11}a_{22} - a_{12}a_{21} = \lambda_1\lambda_2 \quad \text{und} \quad c_1(A) = -(a_{11} + a_{22}) = -(\lambda_1 + \lambda_2).$$

Die Ähnlichkeitsnvariante $c_0(A)$ ist gerade die *Determinante* von A, und wir sehen, dass sich diese stets als *Produkt der Eigenwerte* (über dem größeren Körper $\mathbb{L}$, mit algebraischen Vielfachheiten) geschrieben werden kann. Die Ähnlichkeitsinvariante $c_1(A)$ ist das Negative der aus den Übungen bekannten Spur (engl. „trace“) $\operatorname{tr}(A) := a_{11} + a_{22}$, welche überraschenderweise als *Summe der Eigenwerte* (über dem größeren Körper $\mathbb{L}$, mit algebraischen Vielfachheiten) geschrieben werden kann. Insbesondere liegen Summe und Produkt der Eigenwerte (im obigen Sinne) stets in $\mathbb{K}$, auch wenn die Eigenwerte Elemente von $\mathbb{L}$ sind.

Beispiel 6.4.4 ((3×3)-Matrizen)**.** Sei $n = 3$. Die erste Formel liefert

$$\begin{aligned}\chi_A &= (X - a_{11})(X - a_{22})(X - a_{33}) - a_{12}a_{23}a_{31} - a_{13}a_{21}a_{32} \\ &\quad -a_{13}(X - a_{22})a_{31} - (X - a_{11})a_{23}a_{32} - a_{12}a_{21}(X - a_{33}) \\ &= X^3 + (a_{11} + a_{22} + a_{33})X^2 - (a_{11}a_{22} + a_{11}a_{33} + a_{22}a_{33} - a_{13}a_{31} - a_{23}a_{32} - a_{12}a_{21})X \\ &\quad -(a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}).\end{aligned}$$

und die zweite Formel liefert

$$\begin{aligned}\chi_A(X) &= (X - \lambda_1)(X - \lambda_2)(X - \lambda_3) \\ &= X^3 + (\lambda_1 + \lambda_2 + \lambda_3)X^2 - (\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3)X + \lambda_1\lambda_2\lambda_3.\end{aligned}$$

Wir erhalten also drei Ähnlichkeitsinvarianten von (3×3)-Matrizen. Zwei davon sind

$$c_0(A) = -\det(A) = -\lambda_1\lambda_2\lambda_3 \quad \text{und} \quad c_2(A) = \operatorname{tr}(A) = \lambda_1 + \lambda_2 + \lambda_3,$$

also bis auf Vorzeichen wieder die Determinante und die Spur, die man wieder als Produkt bzw. Summe der Eigenwerte darstellen kann. Interessant ist die dritte Invariante $c_1(A)$. Wir können diese schreiben als

$$c_1(A) = -\left(\det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \det\begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix} + \det\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}\right) = -(\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3).$$

Wir erinnern an unsere Notation für Minoren (vgl. Notation 4.4.1): Sind $I = \{i_1, \ldots, i_k\}$ und $J = \{j_1, \ldots, j_k\}$ mit $1 \le i_1 < \cdots < i_k \le n$ und $1 \le j_1 < \cdots < j_k \le n$, so schreiben wir

$$A_{IJ} := (a_{i_r, j_s})_{r,s \in \{1,\ldots,k\}} \in \mathbb{K}^{k \times k} \quad \text{und} \quad \det_{IJ}(A) := \det(A_{IJ}).$$

Mit dieser Notation haben wir also gezeigt, dass die Minorensumme

$$\sum_{\substack{I \subseteq \{1,2,3\} \\ |I| = 2}} \det_{II}(A) = \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3$$

eine Ähnlichkeitsinvariante ist, die mit der Summe der Produkte von je zwei Eigenwerten übereinstimmt.

Das ist natürlich nur die Spitze des Eisbergs. Für allgemeine n können wir die Koeffizienten $c_k(A)$ stets einerseits als Summen spezieller Minoren von A ausdrücken (1. Formel) und andererseits als spezielle Funktionen in den Eigenwerten (2. Formel).

Notation 6.4.5. Für $k \in \{1,\dots,n\}$ heißt die Funktion

$$\sigma_k^{(n)} : \mathbb{L}^n \to \mathbb{L}, \quad \sigma_k^{(n)}(\lambda_1,\dots,\lambda_n) := \sum_{1\le i_1<\dots<i_k\le n} \prod_{j=1}^{k} \lambda_{i_j}$$

heißt die *kte elementarsymmetrische Polynomfunktion* in n Variablen über $\mathbb{K}$.

Beispiel 6.4.6. Für $n = 4$ lauten die elementrasymmetrischen Polynomfunktionen

$$\begin{aligned}
\sigma_1^{(4)}(\lambda_1,\lambda_2,\lambda_3,\lambda_4) &= \lambda_1+\lambda_2+\lambda_3+\lambda_4,\\
\sigma_2^{(4)}(\lambda_1,\lambda_2,\lambda_3,\lambda_4) &= \lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_1\lambda_4+\lambda_2\lambda_3+\lambda_2\lambda_4+\lambda_3\lambda_4,\\
\sigma_3^{(4)}(\lambda_1,\lambda_2,\lambda_3,\lambda_4) &= \lambda_1\lambda_2\lambda_3+\lambda_1\lambda_2\lambda_4+\lambda_1\lambda_3\lambda_4+\lambda_2\lambda_3\lambda_4,\\
\sigma_4^{(4)}(\lambda_1,\lambda_2,\lambda_3,\lambda_4) &= \lambda_1\lambda_2\lambda_3\lambda_4.
\end{aligned}$$

Wie im (2×2)-Fall nennen wir auch für $A \in \mathbb{K}^{n\times n}$ die Summe $\operatorname{tr}(A) := a_{11}+\dots+a_{nn}$ der Diagonaleinträge von A wieder die *Spur* von A.

Satz 6.4.7 (Koeffizientenformeln)**.** *Für $A \in \mathbb{K}^{n\times n}$ sind die Koeffizienten $c_0(A),\dots,c_{n-1}(A)$ von χ_A wie folgt gegeben.*

(i) Für alle $k \in \{0,\dots,n-1\}$ gilt

$$c_k(A) = (-1)^{n-k} \sum_{\substack{I\subseteq\{1,\dots,n\}\\ |I|=n-k}} \det_{II}(A).$$

Speziell gilt $c_0(A) = (-1)^n \det(A)$ und $c_{n-1}(A) = -\operatorname{tr}(A)$.

(ii) Für alle $k \in \{0,\dots,n-1\}$ gilt

$$c_k(A) = (-1)^{n-k}\sigma_{n-k}^{(n)}(\lambda_1,\dots,\lambda_n).$$

Speziell gilt $c_0(A) = (-1)^n\lambda_1\cdots\lambda_n$ und $c_{n-1}(A) = -(\lambda_1+\dots+\lambda_n)$.

Beweis. (i) Es seien $s_1,\dots,s_n$ die Spalten von A. Unter Ausnutzung der Mulilinearität der Determinantenform erhalten wir

$$\begin{aligned}
\chi_A &= \operatorname{Det}(X\cdot e_1-s_1,\dots,X\cdot e_n-s_n) = \operatorname{Det}(-s_1,\dots,X\cdot e_n-s_n)+\operatorname{Det}(X\cdot e_1,\dots,X\cdot e_n-s_n)\\
&= \operatorname{Det}(-s_1,-s_2,\dots,X\cdot e_n-s_n)+\operatorname{Det}(-s_1,X\cdot e_2)\\
&\quad +\operatorname{Det}(X\cdot e_1,-s_2,\dots,X\cdot e_n-s_n)+\operatorname{Det}(X\cdot e_1,X\cdot e_2,\dots,X\cdot e_n-s_n)\\
&= \dots\\
&= \operatorname{Det}(-s_1,\dots,-s_n)+\sum_{i=1}^{n}\operatorname{Det}(-s_1,\dots,X\cdot e_i,\dots,-s_n)\\
&\quad +\sum_{1\le i<j\le n}\operatorname{Det}(-s_1,\dots,X\cdot e_i,\dots,X\cdot e_j,\dots,-s_n)+\dots+\operatorname{Det}(X\cdot e_1,\dots,X\cdot e_n)\\
&= \sum_{k=0}^{n} X^k(-1)^{n-k}\sum_{1\le i_1<\dots<i_k\le n}\operatorname{Det}(s_1,\dots,e_{i_1},\dots,e_{i_k},\dots,s_n).
\end{aligned}$$

Wir entwicklen nun diese Determinanten nacheindander nach den Spalten mit den Nummern $i_1,\dots,i_k$. Ist $I := \{1,\dots n\}\setminus\{i_1,\dots,i_k\}$, so erhalten wir

$$\operatorname{Det}(s_1,\dots,e_{i_1},\dots,e_{i_k},\dots,s_n) = \det_{II}(A).$$

Es gilt also

$$\chi_A = \sum_{k=0}^{n} X^k (-1)^{n-k} \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=n-k}} \det_{II}(A),$$

woraus die Behauptung folgt.

(ii) Wir multiplizieren $(X-\lambda_1)\cdots(X-\lambda_n)$ aus. Wir erhalten eine Summe von Produkten von jeweils n Faktoren, wobei jeder Faktor entweder X oder $-\lambda_j$ ist. Ein solcher Faktor ist genau dann ein skalares Vielfaches von X^k, wenn man k mal ein X und $(n-k)$ mal ein $-\lambda_j$ wählt. Daher ist der Vorfaktor von X^k durch $(-1)^{n-k} \cdot \sigma^{(n)}_{n-k}(\lambda_1,\dots,\lambda_n)$ gegeben. □

Korollar 6.4.8 (Eigenwertformeln für Minorensummen)**.** *Sei $A \in \mathbb{K}^{n\times n}$ und $\lambda_1,\dots,\lambda_n$ die Eigenwerte von A in $\mathbb{L}$ (gezählt mit algebraischer Vielfachheit).*

(i) Für alle $k \in \{0,\dots,n-1\}$ gilt

$$\sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=n-k}} \det_{II}(A) = \sigma^{(n)}_{n-k}(\lambda_1,\dots,\lambda_n).$$

Speziell gilt $\det(A) = \lambda_1 \cdots \lambda_n$ *und* $\operatorname{tr}(A) = \lambda_1 + \cdots + \lambda_n$.

(ii) Für alle $k \in \{0,\dots,n-1\}$ gilt $\sigma^{(n)}_{n-k}(\lambda_1,\dots,\lambda_n) \in \mathbb{K}$, speziell $\lambda_1 \cdots \lambda_n \in \mathbb{K}$ und $\lambda_1 + \cdots + \lambda_n \in \mathbb{K}$. □

Beispiel 6.4.9. Für $n = 4$ und $k = 2$ erhalten wir die denkwürdige Formel

$$\begin{aligned} & a_{11}a_{22} + a_{11}a_{33} + a_{11}a_{44} - a_{12}a_{21} - a_{13}a_{31} - a_{14}a_{41} \\ & + a_{22}a_{33} + a_{22}a_{44} - a_{23}a_{32} - a_{24}a_{42} - a_{33}a_{44} - a_{34}a_{43} \\ = \; & \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_1\lambda_4 + \lambda_2\lambda_3 + \lambda_2\lambda_4 + \lambda_3\lambda_4, \end{aligned}$$

Eine solche Formel zu beweisen, ist mit der richtigen Idee nicht besonders schwierig, aber man muss erstmal auf so eine Formel kommen!

Von den Koeffizienten des charakteristischen Polynoms sind die Determinante und die Spur die mit Abstand wichtigsten in Anwendungen. Über die Eigenschaften der Determinante haben wir bereits einiges gelernt. Wir tragen nun noch einige wichtige Eigenschaften der Spur zusammen.

Proposition 6.4.10 (Eigenschaften der Spur)**.** *Es sei $\operatorname{tr} : \mathbb{K}^{n\times n} \to \mathbb{K}$ die Spurabbildung.*

(i) Die Spurabbildung ist linear.

(ii) Es gilt die Spuridentität $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ für alle $A, B \in \mathbb{K}^{n\times n}$.

(iii) Sind $\lambda_1,\dots,\lambda_n$ die Eigenwerte von A in $\mathbb{L}$ (mit algebraischer Multiplizität), so gilt $\operatorname{tr}(A^k) = \lambda_1^k + \cdots + \lambda_n^k$ für alle $k \in \mathbb{N}$.

Beweis. (i) Sind $A = (a_{ij}), B = (b_{ij}) \in \mathbb{K}^{n\times n}$ und $\lambda, \mu \in \mathbb{K}$, so ist

$$\operatorname{tr}(\lambda A + \mu B) = \operatorname{tr}(\lambda a_{ij} + \mu b_{ij}) = (\lambda a_{11} + \mu b_{11}) + \cdots + (\lambda a_{nn} + \mu b_{nn}) = \lambda \operatorname{tr}(A) + \mu \operatorname{tr}(B).$$

(ii) Sind $A=(a_{ij}), B=(b_{ij}) \in \mathbb{K}^{n\times n}$ und $AB=(c_{ij})$, so gilt

$$\operatorname{tr}(AB)=\sum_{i=1}^{n} c_{ii}=\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji}.$$

Analog erhält man

$$\operatorname{tr}(BA)=\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}a_{ji}=\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ji}b_{ij}.$$

Benennt man nun den Summationsindex i in j um und umgekehrt, so sieht man, dass beide Ausdrücke gleich sind.

(iii) Aus dem spektralen Abbildungssatz, folgt dass $\operatorname{spec}_{\mathbb{L}}(A^k)=\{\lambda_1^k,\dots,\lambda_n^k\}$, und der Beweis des spektralen Abbildungssatzes zeigt, dass auch die algebraische Multiplizität von λ_j^n mit der von λ_j übereinstimmt (Übung!). Dann folgt die Behauptung aus Korollar 6.4.8.(i). □

Die letzte Eigenschaft der Spur hat eine wichtige Anwendung in der Graphentheorie.

Bemerkung 6.4.11 (Geschlossene Pfade zählen)**.** Sei $\mathcal{G}=(V,E)$ ein einfacher gerichteter Graph mit Eckenmenge $\{v_1,\dots,v_n\}$ und Adjazenzmatrix A. Ist $A^k=(a_{ij}^{(k)})$, so ist $a_{ij}^{(k)}$ bekanntlich gerade die Anzahl der Pfade der Länge k von Ecke i zu Ecke j. Wir nennen einen Pfad in $\mathcal{G}$ *geschlossen*, wenn er an derselben Ecke startet und endet. Die Anzahl der geschlossenen Pfade der Länge $k\in\mathcal{G}$ ist dann gegeben durch

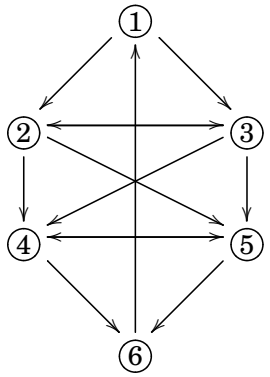
$$a_{11}^{(k)}+\cdots+a_{nn}^{(k)}=\operatorname{tr}(A^k).$$

Sind also $\lambda_1,\dots,\lambda_n$ die komplexen Eigenwerte der Adjazenzmatrix, so ist die Anzahl der geschlossenen Pfade der Länge k gerade

$$a_{11}^{(k)}+\cdots+a_{nn}^{(k)}=\lambda_1^k+\cdots+\lambda_n^k.$$

Obwohl $\lambda_1,\dots,\lambda_n$ komplexe Zahlen sind, ist dies stets eine nicht-negative ganze Zahl!

Beispiel 6.4.12. Wie betrachten den einfachen gerichteten Graphen



mit Adjazenzmatrix

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

Es gilt dann

$$\chi_A = (X+1)^3(X-2)(X^2-X+2).$$

In der Tat rechnet man nach, dass

$$\begin{aligned}
\chi_A &= \left|\begin{pmatrix} X & -1 & -1 & 0 & 0 & 0 \\ 0 & X & -1 & -1 & -1 & 0 \\ 0 & -1 & X & -1 & -1 & 0 \\ 0 & 0 & 0 & X & -1 & -1 \\ 0 & 0 & 0 & -1 & X & -1 \\ -1 & 0 & 0 & 0 & 0 & X \end{pmatrix}\right| = \left|\begin{pmatrix} 0 & -1 & -1 & 0 & 0 & X^2 \\ 0 & X & -1 & -1 & -1 & 0 \\ 0 & -1 & X & -1 & -1 & 0 \\ 0 & 0 & 0 & X & -1 & -1 \\ 0 & 0 & 0 & -1 & X & -1 \\ -1 & 0 & 0 & 0 & 0 & X \end{pmatrix}\right| \\
&= -(-1)\left|\begin{pmatrix} -1 & -1 & 0 & 0 & X^2 \\ X & -1 & -1 & -1 & 0 \\ -1 & X & -1 & -1 & 0 \\ 0 & 0 & X & -1 & -1 \\ 0 & 0 & -1 & X & -1 \end{pmatrix}\right| = \left|\begin{pmatrix} -1 & -1 & -X^2 & X^3 & 0 \\ X & -1 & -1 & -1 & 0 \\ -1 & X & -1 & -1 & 0 \\ 0 & 0 & X+1 & -X-1 & 0 \\ 0 & 0 & -1 & X & -1 \end{pmatrix}\right| \\
&= (-1)\left|\begin{pmatrix} -1 & -1 & -X^2 & X^3 \\ X & -1 & -1 & -1 \\ -1 & X & -1 & -1 \\ 0 & 0 & X+1 & -X-1 \end{pmatrix}\right| = \left|\begin{pmatrix} 1 & 1 & X^2 & -X^3 \\ 0 & -X-1 & -X^3-1 & X^4-1 \\ 0 & X+1 & X^2-1 & -X^3-1 \\ 0 & 0 & X+1 & -X-1 \end{pmatrix}\right| \\
&= \left|\begin{pmatrix} -X-1 & -X^3-1 & X^4-1 \\ X+1 & X^2-1 & -X^3-1 \\ 0 & X+1 & -X-1 \end{pmatrix}\right| = \left|\begin{pmatrix} -X-1 & -X^3-1 & X^4-1 \\ 0 & -X^3+X^2-2 & X^4-X^3-2 \\ 0 & X+1 & -X-1 \end{pmatrix}\right| \\
&= (-X-1)\cdot\left|\begin{pmatrix} -X^3+X^2-2 & X^4-X^3-2 \\ X+1 & -X-1 \end{pmatrix}\right| \\
&= -(X+1)((-X^3+X^2-2)(-X-1)-(X^4-X^3-2)(X+1)) \\
&= (X+1)^2((-X^3+X^2-2)+(X^4-X^3-2)) \\
&= (X+1)^2(X^4-2X^3+X^2-4) = (X+1)^3(X-2)(X^2-X+2).
\end{aligned}$$

Über $\mathbb{Q}$ oder $\mathbb{R}$ ist der quadratische Faktor irreduzibel; arbeiten wir hingegen über den komplexen Zahlen, so erhalten wir die Zerlegung

$$\chi_A(X) = (X+1)^3(X-2)\left(X-\frac{1-i\sqrt{7}}{2}\right)\left(X-\frac{1+i\sqrt{7}}{2}\right)$$

Die Anzahl der geschlossenen Pfade der Länge k ist daher gegeben durch

$$\operatorname{tr}(A^k) = (-1)^k + (-1)^k + (-1)^k + 2^k + \left(\frac{1-i\sqrt{7}}{2}\right)^k + \left(\frac{1+i\sqrt{7}}{2}\right)^k.$$

Auch wenn man es der Formel nicht sofort ansieht, ist dies stets eine ganze Zahl. Für kleine Werte von k erhalten wir

$$0,4,0,20,40,76,112,228,504,1084,2112,\ldots$$

geschlossene Pfade. Es gibt also 1084 geschlossene Pfade der Länge 10, und wir konnten diese Zahl allein aus den Eigenwerten von A bestimmen ohne die zugehörigen Eigenvektoren zu berechnen.

Zusammenfassung von Abschnitt 6.4

(1) Die Koeffizienten des charakteristischen Polynoms sind Ähnlichkeitsinvarianten. Die zwei wichtigsten Beispiele sind (bis auf Vorzeichen) die Spur und die Determinante.

(2) Die Koeffizienten sind (bis auf Vorzeichen) Summen von Determinanten von speziellen Untermatrizen und zugleich elementarsymmetrische Polynomfunktionen in den Eigenwerten (über einer hinreichend großen Körpererweiterung, gezählt mit algebraischen Vielfachheiten).

(3) Spur und Determinante sind gegeben durch Summe bzw. Produkt der Eigenwerte (über einer hinreichend großen Körpererweiterung, gezählt mit algebraischen Vielfachheiten).

(4) Die Spur der Potenz einer Matrix ist die Summe der entsprechenden Potenzen der Eigenwerte (über einer hinreichend großen Körpererweiterung, gezählt mit algebraischen Vielfachheiten). Dies kann zum Zählen geschlossener Pfade in Netzwerken verwendet werden.

[17.04.24]

6.5 Normalform nilpotenter Endomorphismen

In diesem Abschnitt sei $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum der Dimension n und $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ ein nilpotenter Endomorphismus.

Bemerkung 6.5.1 (Erinnerung: Nilpotente Endomorphismen)**.** Wir erinnern daran, dass Φ *nilpotent* heißt, falls $\Phi^N = 0$ für ein $N \in \mathbb{N}$ gilt. In diesem Fall ist das Minimalpolynom μ_Φ von Φ ein Teiler von X^N. Daraus folgern wir:

(1) $\mu_\Phi = X^k$ für ein $k \leq N$. Insbesondere zerfällt μ_Φ in Linearfaktoren und Φ ist trigonalisierbar.

(2) Das charakteristische Polynom χ_Φ hat (über einem geeigneten Erweiterungskörper) dieselben Nullstellen wie μ_Φ, also muss $\chi_\Phi = X^n$ gelten. Mit dem Satz von Cayley–Hamilton folgt daher $k \leq n$.

(3) Ist $k = 1$ so gilt nach Definition $\Phi = 0$. Andernfalls ist Φ nach dem 4. Diagonalisierbarkeitskriterium (Satz 6.2.13) nicht diagonalisierbar.

Wenn wir annehmen, dass $\Phi \neq 0$ gilt, so ist Φ also trigonalisierbar, aber nicht diagonalisierbar. Es stellt sich nun die Frage, wie wir eine möglichst einfache Normalform für solche Endomorphismen finden können.

Definition 6.5.2. Ist $\mu_\Phi = X^k$, so sagen wir, Φ sei *nilpotent vom Grad k*.

Notation 6.5.3. Ab jetzt sei Φ nilpotent vom Grad k. Für $j \in \{0,\dots,k\}$ setzen wir

$$K_j := \ker(\Phi^j), \quad d_j := \dim K_j = \mathrm{def}(\Phi^j), \quad r_j := n - d_j = \mathrm{rk}(\Phi^j).$$

Wir setzen zusätzlich noch $K_{-1} := \{0\}$.

Lemma 6.5.4. *Es sei $j \in \{1,\dots,k\}$.*

(i) Für $j \in \{1,\dots,k\}$ gilt $K_{j-1} \subseteq K_j$ und $\Phi[K_j] \subseteq K_{j-1}$.

(ii) Φ induziert lineare Abbildungen

$$\Phi_j : K_j \to K_{j-1} \quad \text{und} \quad \bar{\Phi}_j : K_j/K_{j-1} \to K_{j-1}/K_{j-2}.$$

(iii) Für $j \geq 2$ ist die lineare Abbildung $\bar{\Phi}_j$ injektiv, insbesondere gilt $d_j - d_{j-1} \leq d_{j-1} - d_{j-2}$.

(iv) Es gilt $d_1 < d_2 < \cdots < d_k$ und folglich $K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_k$.

Beweis. (i) Ist $v \in K_{j-1}$, so ist $\Phi^j(v) = \Phi(\Phi^{j-1}(v)) = \Phi(0) = 0$, also $v \in K_j$. Ist umgekehrt $v \in K_j$, dann gilt $\Phi^{j-1}(\Phi(v)) = \Phi^j(v) = 0$, also $\Phi(v) \in K_{j-1}$.

(ii) Dies folgt sofort aus (i).

(iii) Es sei $j \geq 2$ und $v \in K_j$. Dann gilt

$$\begin{aligned}\bar{\Phi}_j(v + K_{j-1}) = 0 + K_{j-2} &\iff \Phi(v) \in K_{j-2} \iff \Phi^{j-2}(\Phi(v)) = 0 \\ &\iff \Phi^{j-1}(v) = 0 \iff v \in K_{j-1} \iff v + K_{j-1} = 0 + K_{j-1}.\end{aligned}$$

Die erste Behauptung folgt daher aus dem Injektivitätskriterium, und sie impliziert

$$d_j - d_{j-1} = \dim K_j/K_{j-1} \leq \dim K_{j-1}/K_{j-2} = d_{j-1} - d_{j-2}.$$

(iv) Da k minimal ist mit $\Phi^k = 0$ gilt $\Phi^{k-1} \neq 0$ und daher $K_{k-1} = \ker(\Phi^{k-1}) \subsetneq V = K_k$. Dies impliziert $d_k - d_{k-1} > 0$ und durch sukzessives Anwenden von (iii) folgt daraus nach und nach $d_{k-1} - d_{k-2} > 0, \ldots, d_2 - d_1 > 0$ und $d_1 - d_0 > 0$. □

Bemerkung 6.5.5 (Kanonische Fahne)**.** Aus Lemma 6.5.4 folgt, dass $K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_{k-1} \subsetneq K_k$ eine Φ-invariante echte Fahne ist. Diese heißt auch die *kanonische Fahne* zu Φ. Nach Lemma 6.5.4.(i) wirkt Φ auf seiner kanonischen Fahne durch „Runterschieben“:

$$\{0\} = K_0 \underset{\Phi_1}{\subsetneq} K_1 \underset{\Phi_2}{\subsetneq} \cdots \underset{\Phi_{k-1}}{\subsetneq} K_{k-1} \underset{\Phi_k}{\subsetneq} K_k = V$$

Bemerkung 6.5.6 (Ketten)**.** Ist $v \in V$, so definieren wir den Φ-*Grad* von v als

$$\deg(v) = \min\{j \in \mathbb{N} \mid \Phi^j(v) = 0\}.$$

Nach Definition gilt für alle $j \in \{0, \ldots, k\}$, dass

$$K_j = \{v \in V \mid \deg(v) \leq j\}.$$

Ist $v \neq 0$, so senkt Anwenden von Φ den Φ-Grad um 1. In diesem Fall definieren wir die von v erzeugte Φ-*Kette* als $\{v, \Phi(v), \ldots, \Phi^{\deg(v)-1}(v)\}$. Wir nennen $\deg(v)$ die *Länge*[10] dieser Kette. Beachte, dass die Elemente $v, \Phi(v), \ldots, \Phi^{\deg(v)-1}(v)$ paarweise verschieden (und alle nicht 0) sind, da sie paarweise (und von 0) verschiedenen Grad haben.

Beispiel 6.5.7 (Eine Kettenbasis)**.** Wir betrachten den Endomorphismus $\Phi : \mathbb{Q}^4 \to \mathbb{Q}^4$ mit darstellender Matrix (bzgl. Standardbasis)

$$A := \begin{pmatrix} -2 & 4 & 4 & 0 \\ 4 & -2 & -4 & -1 \\ -5 & 4 & 6 & 1 \\ 4 & 4 & 0 & -2 \end{pmatrix}.$$

Es gilt dann $A^2 = 0$ und $A \neq 0$, also ist Φ nilpotent vom Grad 2. Der Kern von A lässt sich durch elementare Zeilenumformungen wie gewohnt bestimmen:

$$\begin{pmatrix} -2 & 4 & 4 & 0 \\ 4 & -2 & -4 & -1 \\ -5 & 4 & 6 & 1 \\ 4 & 4 & 0 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -2 & -2 & 0 \\ 4 & -2 & -4 & -1 \\ -5 & 4 & 6 & 1 \\ 4 & 4 & 0 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -2 & -2 & 0 \\ 0 & 6 & 4 & -1 \\ 0 & -6 & -4 & 1 \\ 0 & 12 & 8 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -2 & -2 & 0 \\ 0 & 6 & 4 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Es gilt daher

$$\ker(A) = \ker\left(\begin{pmatrix} 1 & -2 & -2 & 0 \\ 0 & 6 & 4 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\right) = \left\langle \begin{pmatrix} 2 \\ -2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 6 \end{pmatrix} \right\rangle.$$

Die kanonische Fahne von Φ ist daher gegeben durch

$$K_0 = \{0\} \quad \subseteq \quad K_1 = \left\langle \begin{pmatrix} 2 \\ -2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 6 \end{pmatrix} \right\rangle \quad \subseteq \quad K_2 = \mathbb{Q}^4.$$

[10] Manche Autoren nennen $\deg(v) - 1$ die Länge der Kette; in meinem alten Skript bin ich dieser Konvention gefolgt.

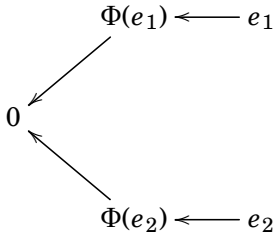
Die beiden Standardbasisvektoren e_1 und e_2 liegen nicht in K_1 und haben daher Φ-Grad 2. Die zugehörigen Φ-Ketten sind gegeben durch

$$\{e_1, \Phi(e_1)\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 4 \\ -5 \\ 4 \end{pmatrix} \right\} \quad \text{und} \quad \{e_2, \Phi(e_2)\} = \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ -2 \\ 4 \\ 4 \end{pmatrix} \right\}$$

Diese beiden Ketten bilden zusammengenommen eine Basis von $\mathbb{Q}^4$, denn es gilt

$$\det \begin{pmatrix} 1 & -2 & 0 & 4 \\ 0 & 4 & 1 & -2 \\ 0 & -5 & 0 & 4 \\ 0 & 4 & 0 & 4 \end{pmatrix} = -\det \begin{pmatrix} 1 & 0 & -2 & 4 \\ 0 & 1 & 4 & -2 \\ 0 & 0 & -5 & 4 \\ 0 & 0 & 4 & 4 \end{pmatrix} = -\det \begin{pmatrix} -5 & 4 \\ 4 & 4 \end{pmatrix} = 36 \neq 0.$$

Bzgl. dieser Basis können wir uns die Wirkung von Φ schematisch so vorstellen:



Im obigen Beispiel haben wir einfach zwei zufällig gewählte Ketten von maximaler Länge genommen und so eine Basis gefunden, in der sich die Wirkung von Φ einfach beschreiben lässt. Kann man das immer machen? Dazu betrachten wir ein weiteres Beispiel:

Beispiel 6.5.8. Wir betrachten $\Phi : \mathbb{Q}^3 \to \mathbb{Q}^3$ mit darstellender Matrix (bzgl. Standardbasis)

$$B := \begin{pmatrix} 0 & -1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Es gilt dann $B^2 = 0$ und

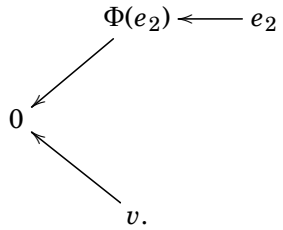
$$K_0 = \{0\} \quad \subseteq \quad K_1 = \ker(B) = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} \right\rangle \quad \subseteq \quad K_2 = \mathbb{Q}^3.$$

Nehmen wir einen Vektor aus $K_2 \setminus K_1$, so erhalten wir eine Kette von maximaler Länge (nämlich 2), z.B.

$$\{e_2, \Phi(e_2)\} = \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

Es kann keine von dieser Kette linear unabhängige Kette der Länge 2 geben, denn wegen $\dim \mathbb{Q}^3 = 3$ ist dafür schlicht kein Platz. Es ist aber noch Platz für eine kürzere Kette, wir versuchen es also mit einem Element von K_1. Der Vektor $e_1 \in K_1$ ist von den Elementen der vorigen Kette linear abhängig, aber der Vektor $v := (0,2,1)^\top$ ist linear unabhängig. Wir erhalten also

eine „Kettenbasis“ $(e_2, \Phi(e_2), v)$, und bzgl. dieser ist die Wirkung von Φ schematisch gegeben durch



Das Rezept zum Finden einer guten Basis scheint also grob gesagt das Folgende zu sein: Man wählt so viele linear unabhängige Ketten von maximaler Länge wie möglich. Dann wählt man so viele linear unabhängige Ketten von der nächst kürzeren Länge wie möglich usw. Dabei hat man natürlich sehr viele Wahlmöglichkeiten, uns es ist erstmal nicht klar, dass dieses Vorgehen auf eine kanonische Normalform führt, aber darum kümmern wir uns später. Zunächst machen wir die hier angedeutete Konstruktion formal präzise.

Notation 6.5.9. Für $j \in \{0, \dots, k\}$ schreiben wir $\overline{K}_j := K_j/K_{j-1}$ und bezeichnen mit $\pi_j : K_j \to \overline{K}_j$, $v \mapsto \bar{v}$ die kanonischen Projektionen. Wir sagen, dass Vektoren in K_j *linear unabhängig modulo* K_{j-1} sind, wenn ihre Bilder unter π_j linear unabhängig sind. Nach Lemma 6.5.4 haben wir ein kommutatives Diagramm

$$\begin{array}{ccccccccc} K_1 & \xleftarrow{\Phi_2} & K_2 & \xleftarrow{\Phi_3} & \dots & \xleftarrow{\Phi_{k-1}} & K_{k-1} & \xleftarrow{\Phi_k} & K_k \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} & & & & \downarrow{\scriptstyle \pi_{k-1}} & & \downarrow{\scriptstyle \pi_k} \\ \overline{K}_1 & \xleftarrow{\overline{\Phi}_2} & \overline{K}_2 & \xleftarrow{\overline{\Phi}_3} & \dots & \xleftarrow{\overline{\Phi}_{k-1}} & \overline{K}_{k-1} & \xleftarrow{\overline{\Phi}_k} & \overline{K}_k, \end{array} \tag{6.5.1}$$

wobei die Abbildungen der unteren Zeile alle injektiv sind.

Übung 6.5.10. Sei $j \in \{0, \dots, k\}$ und $v \in K_j$. Zeigen Sie, dass

$$\deg(v) = j \iff v \notin K_{j-1} \iff \pi_j(v) \neq 0.$$

Konstruktion 6.5.11 (Konstruktion von Kettenbasen)**.** Wir wollen nun so viele und lange linear unabhängige Ketten wie möglich konstruieren. Dazu gehen wir wie folgt vor:

- Wir wählen zunächst eine Basis $\overline{\mathscr{B}}_k$ von $\overline{K}_k$.
- Da $\overline{\Phi}_k$ injektiv ist, ist $\overline{\Phi}_k[\overline{\mathscr{B}}_k]$ linear unabhängig. Wir ergänzen diese Menge nun mittels Basisergänzungssatz zu einer Basis $\overline{\Phi}_k[\overline{\mathscr{B}}_k] \sqcup \overline{\mathscr{B}}_{k-1}$ von $\overline{K}_{k-1}$.
- Nach und nach finden wir so – durch wiederholtes Anwenden von Lemma 6.5.4 und des Basisergänzungssatzes – Teilmengen $\overline{\mathscr{B}}_j \subseteq \overline{K}_j$ mit den folgenden Eigenschaften:

$$\begin{aligned} \overline{\mathscr{B}}_k &\quad \text{ist Basis von} \quad \overline{K}_k \\ \overline{\Phi}_k[\overline{\mathscr{B}}_k] \sqcup \overline{\mathscr{B}}_{k-1} &\quad \text{ist Basis von} \quad \overline{K}_{k-1} \\ \overline{\Phi}_{k-1}[\overline{\Phi}_k[\overline{\mathscr{B}}_k]] \sqcup \overline{\Phi}_{k-1}[\overline{\mathscr{B}}_{k-1}] \sqcup \overline{\mathscr{B}}_{k-2} &\quad \text{ist Basis von} \quad \overline{K}_{k-2} \\ &\dots \\ \overline{\Phi}_2[\cdots[\overline{\Phi}_k[\overline{\mathscr{B}}_k]]] \sqcup \cdots \sqcup \overline{\Phi}_2[\overline{\mathscr{B}}_2] \sqcup \overline{\mathscr{B}}_1 &\quad \text{ist Basis von} \quad \overline{K}_1 \end{aligned}$$

- Für $j \in \{1,\dots,k\}$ wählen wir nun eine Teilmenge $\mathscr{B}_j \subseteq K_j$, so dass $\mathscr{B}_j$ unter der kanonischen Projektikon $\pi_j : K_j \to \overline{K}_j$ bijektiv auf $\overline{\mathscr{B}}_j$ abgebildet wird. (Man nennt die Menge $\mathscr{B}_j$ eine *Hochhebung* (engl. *lift*) der Menge $\overline{\mathscr{B}}_j$.) Wegen $0 \notin \overline{\mathscr{B}}_j$ haben die Elemente von $\mathscr{B}_j$ nach Übung 6.5.10 stets den Grad j, und nach Konstruktion ist $\mathscr{B}_j$ linear unabhängig modulo K_{j-1}.
- Wir setzen nun $\mathscr{B} := \mathscr{B}_1 \cup \dots \cup \mathscr{B}_k$ und schreiben $\mathscr{B}_*$ für die Vereinigung der Φ-Ketten von Elementen aus $\mathscr{B}$. Die Elemente vom Grad k in $\mathscr{B}_*$ sind genau die Elemente von $\mathscr{B}_k$. Die Elemente vom Grad $k-1$ sind genau die Elemente von $\mathscr{B}_{k-1} \cup \Phi[\mathscr{B}_k]$, und diese sind linear unabhängig modulo K_{k-2}, insbesondere paarweise verschieden. Insgesamt erhalten wir eine disjunkte Vereinigung

$$\mathscr{B}_* := \underbrace{\mathscr{B}_k}_{\deg k} \sqcup \underbrace{\Phi[\mathscr{B}_k] \sqcup \mathscr{B}_{k-1}}_{\deg k-1} \sqcup \dots \sqcup \underbrace{\Phi^{k-1}[\mathscr{B}_k] \sqcup \Phi^{k-2}[\mathscr{B}_{k-1}] \sqcup \dots \sqcup \Phi[\mathscr{B}_2] \sqcup \mathscr{B}_1}_{\deg 1}.$$

Wir zählen nun durch, wie viele Elemente von V wir konstruiert haben:

Lemma 6.5.12. *Sei $j \in \{1,\dots,k\}$.*

(i) $|\mathscr{B}_j| + \dots + |\mathscr{B}_k| = d_j - d_{j-1}$.

(ii) Es gilt $|\mathscr{B}_k| = c_k := d_k - d_{k-1}$ *und für* $j < k$ *gilt* $|\mathscr{B}_j| = c_j := -d_{j+1} + 2d_j - d_{j-1}$.

(iii) Es gilt $|\mathscr{B}_*| = n = \dim V$.

Beweis. (i) Da $\overline{\mathscr{B}}_k$ eine Basis von $\overline{F}_k$ ist, gilt

$$d_k - d_{k-1} = \dim \overline{F}_k = |\overline{\mathscr{B}}_k| = |\mathscr{B}_k|.$$

Dies zeigt (i) für $j = k$. Für $j = k-1$ rechnet man

$$d_{k-1} - d_{k-2} = \dim \overline{F}_{k-1} = |\overline{\mathscr{B}}_{k-1}| + |\overline{\Phi}_k[\overline{\mathscr{B}}_k]| = |\overline{\mathscr{B}}_{k-1}| + |\overline{\mathscr{B}}_k| = |\mathscr{B}_{k-1}| + |\mathscr{B}_k|,$$

und analog argumentiert man für $j < k-1$.

(ii) Für $j = k$ folgt die Behauptung direkt aus (i). Für $j < k$ folgt aus (i), dass

$$|\mathscr{B}_j| = (|\mathscr{B}_j| + \dots + |\mathscr{B}_k|) - (|\mathscr{B}_{j+1}| + \dots + |\mathscr{B}_k|) = (d_j - d_{j-1}) - (d_{j+1} - d_j) = -d_{j+1} + 2d_j - d_{j-1} = c_j.$$

(iii) Zählt man zuerst die Elemente von Grad k, dann die Elemente von Grad $k-1$ usw., so erhält man

$$|\mathscr{B}_*| = |\mathscr{B}_k| + (|\mathscr{B}_{k-1}| + |\mathscr{B}_k|) + \dots + (|\mathscr{B}_1| + \dots + |\mathscr{B}_k|).$$

Wegen (i) erhalten wir also eine Teleskopsumme

$$|\mathscr{B}_*| = (d_k - d_{k-1}) + (d_{k-1} - d_{k-2}) + \dots + (d_1 - d_0) = d_k - d_0 = n - 0 = n. \qquad \square$$

Bemerkung 6.5.13. Im Folgenden sei stets c_j wie in Lemma 6.5.12 definiert. Wegen $r_j = n - d_j$ gilt dann

$$c_j = r_{j-1} - 2r_j + r_{j+1} \tag{6.5.2}$$

für alle $j \in \{1,\dots,k-1\}$. Setzen wir $r_{k+1} := \mathrm{rk}(\Phi^{k+1}) = 0$, so gilt diese Formel auch für $j = k$.

Satz 6.5.14 (Kettenbasissatz)**.** *Die Menge $\mathscr{B}_*$ aus Konstruktion 6.5.11 ist eine Basis von V. Insbesondere besitzt V eine Basis, die eine disjunkte Vereinigung von Φ-Ketten ist, und die Anzahl der Ketten der Länge j in dieser Basis ist c_j.*

Beweis. Wir zeigen, dass $\mathscr{B}_*$ ein Erzeugendensystem ist; wegen $|\mathscr{B}_*| = \dim V$ folgt daraus die Behauptung.

Es sei $v \in V = K_k$ beliebig; wir betrachten den Vektor $\pi_k(v) \in \overline{K}_k$. Da $\pi_k(\mathscr{B}_*)$ eine Basis von $\overline{K}_k$ (nämlich $\overline{\mathscr{B}}_k$) enthält, existieren $v_1,\dots,v_t \in \mathscr{B}_*$ und $\lambda_1,\dots,\lambda_t \in \mathbb{K}$ mit

$$\pi_k(v) = \sum_{j=1}^{t} \lambda_j \pi_k(v_j) \quad\Longrightarrow\quad \pi_k\left(v - \sum_{j=1}^{t} \lambda_j v_j\right) = 0 \quad\Longrightarrow\quad v - \sum_{j=1}^{t} \lambda_j v_j \in \ker(\pi_k) = K_{k-1}.$$

Es existiert also $w_k \in \langle \mathscr{B}_* \rangle$ mit $v - w_k \in K_{k-1}$.

Nun betrachten wir $\pi_{k-1}(v - w_k) \in \overline{K}_{k-1}$. Da $\pi_{k-1}(\mathscr{B}_* \cap K_{k-1})$ eine Basis von $\overline{K}_{k-1}$ (nämlich $\overline{\Phi}_k[\overline{\mathscr{B}}_k] \sqcup \overline{\mathscr{B}}_{k-1}$) enthält, finden wir $u_1,\dots,u_s \in \mathscr{B}_* \cap K_{k-1}$ und $\mu_1,\dots,\mu_s \in \mathbb{K}$ mit

$$\pi_{k-1}(v - w_k) = \sum_{j=1}^{s} \mu_j \pi_k(u_j) \quad\Longrightarrow\quad \pi_{k-1}\left(v - w_k - \sum_{j=1}^{s} \mu_j u_j\right) = 0 \quad\Longrightarrow\quad v - \sum_{j=1}^{s} \mu_j u_j \in K_{k-2}.$$

Es existiert also $w_{k-1} \in \langle \mathscr{B}_* \langle$ mit $v - w_k - w_{k-1} \in K_{k-2}$.

Sukzessive finden wir nun für Elemente $w_{k-2},\dots,w_1 \in \langle \mathscr{B}_* \rangle$, so dass $v - w_k - \dots - w_j \in K_{j-1}$ für alle $j \in \{1,\dots,k\}$. Speziell gilt dann $v - w_k - \dots - w_1 \in K_0 = \{0\}$, und folglich ist $v = w_1 + \dots + w_k \in \langle \mathscr{B}_* \rangle$. □

Beispiel 6.5.15. Wir betrachten zwei konkrete Beispiele (vgl. Beispiel 6.5.7 und Beispiel 6.5.8) und ein abstraktes Beispiel.

(i) Sei Φ wie in Beispiel 6.5.7. Es gilt dann $k = 2$, also $\Phi^2 = 0$ und $r_2 = 0$. Außerdem gilt $r_0 = \mathrm{rk}(\Phi^0) = 4$ und $r_1 = \mathrm{rk}(\Phi^1) = 2$. Formel (6.5.2) liefert

$$c_2 = r_1 - r_2 = 2 - 0 = 2 \quad \text{und} \quad c_1 = r_0 - 2r_1 + r_2 = 4 - 2\cdot 2 + 0 = 0,$$

also gibt es eine Kettenbasis bestehen aus 2 Ketten der Länge 2. Dies stimmt mit unserer konkreten Rechnung überein.

Wie findet man nun diese beide Ketten? Dazu muss man zwei Vektoren aus K_2 wählen, die linear unabhängig modulo K_1 sind. Nun gilt $K_2 = \mathbb{Q}^4$, und eine geordnete Basis von K_1 ist gegeben durch

$$\left(\begin{pmatrix} 2 \\ -2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 6 \end{pmatrix}\right).$$

Wir können also beliebige Vektoren $v, w \in \mathbb{Q}^4$ wählen mit der Eigenschaft, dass

$$\mathrm{Det}\left(\begin{pmatrix} 2 \\ -2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 6 \end{pmatrix}, v, w\right) \neq 0.$$

Eine mögliche Wahl ist z.B. $v := e_1$ und $w := e_2$. Diese spezielle Wahl führt dann genau auf die beiden Ketten, die wir in Beispiel 6.5.7. betrachtet haben. Es gibt aber auch (unendlich viele) andere Wahlen für v und w, und für jede solche Wahl kann man dann $\Phi(v)$ und $\Phi(w)$ entsprechend bestimmen.

(ii) Sei nun Φ wie in Beispiel 6.5.8. Es gilt dann $k = 2$, also $\Phi^2 = 0$. Weiterhin sind $r_0 = 3$, $r_1 = 1$ und $r_2 = 0$ Dies liefert

$$c_2 = r_1 - r_2 = 1 - 0 = 1 \quad \text{und} \quad c_1 = r_0 - 2r_1 + r_2 = 3 - 2 \cdot 1 + 0 = 1.$$

Es gibt also eine Kettenbasis mit je einer Kette der Länge 2 bzw. 1. Als Erzeuger der Kette der Länge 2 können wir einen beliebigen Vektor im Komplement von $\left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\1\end{pmatrix} \right\rangle \subseteq \mathbb{Q}^3$ wählen. Eine mögliche Wahl ist e_2, und der zweite Eintrag unserer Kettenbasis ist in diesem Fall $\Phi(e_2) = -e_1$. Um den dritten und letzten Vektor unserer Kettenbasis zu finden, muss man nun noch $-e_1$ zu einer Basis von K_1 ergänzen. In Beispiel 6.5.8 haben wir den Vektor $(0,2,1)^\top$ gewählt, aber andere Wahlen sind natürlich möglich.

(iii) Wenn wir nur wissen wollen, wieviele Ketten von welcher Länge es in einer Kettenbasis gibt, so müssen wir dazu lediglich den Rang der Potenzen von Φ bestimmen, aber nicht die Kerne explizit berechnen. Sei z.B. $\Phi \in \mathrm{End}_{\mathbb{K}}(\mathbb{K}^{12})$ mit $r_1 = 8$, $r_2 = 5$, $r_3 = 2$ und $\Phi^4 = 0$. Dann gilt $r_0 = 12$ und $r_4 = 0$, also

$$c_4 = r_3 - r_4 = 2, \quad c_3 = r_2 - 2r_3 + r_4 = 5 - 2 \cdot 2 + 0 = 1,$$

$$c_2 = r_1 - 2r_2 + r_3 = 8 - 2 \cdot 5 + 2 = 0, \quad c_1 = r_0 - 2r_1 + r_2 = 12 - 2 \cdot 8 + 5 = 1.$$

Es gibt daher eine Kettenbasis bestehend aus 2 Ketten der Länge 4 und je einer Kette der Länge 3 bzw. 1.

Wie sieht die darstellende Matrix eines nilpotenten Endomorphismus bzgl. einer Kettenbasis aus? Wir betrachten zunächst einen Spezialfall.

Beispiel 6.5.16 (Nilpotente Jordan-Blöcke)**.** Wir nehmen zunächst an, V besitzt eine Basis, die aus einer einzigen Ketten $\{v, \Phi(v), \ldots, \Phi^{n-1}(v)\}$ besteht. Dann hat Φ bzgl. der geordnete Basen $\mathscr{B}_- := (v, \Phi(v), \Phi^2(v), \ldots, \Phi^{n-1}(v))$ bzw. $\mathscr{B}_+ := (\Phi^{n-1}(v), \ldots, \Phi^2(v), \Phi(v), v)$ die Darstellungsmatrizen

$$D_{\mathscr{B}_-}(\Phi) = J_-[n] := \begin{pmatrix} 0 & \ldots & \ldots & \ldots & 0 \\ 1 & 0 & & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 0 \end{pmatrix} \quad \text{bzw.} \quad D_{\mathscr{B}_+}(\Phi) = J_+[n] := \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & 1 & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \ldots & \ldots & \ldots & 0 \end{pmatrix}.$$

Im ersten Fall gilt nämlich

$$\begin{aligned} \Phi(v) &= 0 \cdot v + 1 \cdot \Phi(v) + 0 \cdot \Phi^2(v) + \cdots + 0 \cdot \Phi^{n-1}(v), \\ \Phi(\Phi(v)) &= 0 \cdot v + 0 \cdot \Phi(v) + 1 \cdot \Phi^2(v) + \cdots + 0 \cdot \Phi^{n-1}(v), \\ &\cdots \\ \Phi(\Phi^{n-2}(v)) &= 0 \cdot v + 0 \cdot \Phi(v) + 0 \cdot \Phi^2(v) + \cdots + 1 \cdot \Phi^{n-1}(v), \\ \Phi(\Phi^{n-1}(v)) &= 0 \cdot v + 0 \cdot \Phi(v) + 0 \cdot \Phi^2(v) + \cdots + 0 \cdot \Phi^{n-1}(v), \end{aligned}$$

und den zweiten Fall behandelt man analog. Die Matrizen $J_-[n]$ bzw. $J_+[n]$ heißen *unterer* bzw. *oberer nilpotenter Jordan[11]-Block der Größe n*. Es gilt $J_\pm[n]^{n-1} \neq 0 = J_\pm[n]^n$, d.h. die Matrizen $J_\pm[n]$ sind nilpotent vom Grad n.

[11] nach CAMILLE JORDAN (1838-1922), frz. Mathematiker

[19.04.24]

Was für eine darstellende Matrix kann man finden, wenn die Kettenbasis aus mehr als einer Kette besteht?

Notation 6.5.17. Es seien $n_1,\dots,n_\ell \in \mathbb{N}$. Ist $n = n_1 + \cdots + n_\ell$ so nennen wir $(n_1,\dots,n_\ell)$ eine *Partition* von n. Wir definieren dann $(n \times n)$-Matrizen

$$J_\pm[n_1,\dots,n_k] := \begin{pmatrix} J_\pm[n_1] & 0 & \dots & 0 \\ 0 & J_\pm[n_2] & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & J_\pm[n_\ell] \end{pmatrix}$$

und nennen $J_-[n_1,\dots,n_\ell]$ bzw. $J_+[n_1,\dots,n_\ell]$ eine *Matrix in unterer bzw. oberer nilpotenter Normalform* mit *Blockgrößen* $n_1,\dots,n_\ell$.

Bemerkung 6.5.18 (Darstellende Matrix bzgl. Kettenbasis)**.** Es sei $\mathscr{B}_*$ eine Kettenbasis für Φ. Wir ordnen diese Basis so an, dass wir zuerst die erste Kette in aufsteigender (bzw. absteigender) Reihenfolge nehmen, dann die zweite Kette usw. Sind $n_1,\dots,n_\ell$ die entsprechenden Kettenlängen, so ist die zugehörige darstellende Matrix durch $J_-[n_1,\dots,n_\ell]$ (bzw. $J_+[n_1,\dots,n_\ell]$) gegeben. Insbesondere besitzt jeder nilpotente Endomorphismus eine darstellende Matrix in unterer bzw. oberer nilpotenter Normalform. Beachte, dass eine solche Matrix nicht ganz eindeutig ist, weil man z.B. durch Umsortieren der Basis die Reihenfolge der Blöcke vertauschen kann.

Wir können nun unsere bisherigen Ergebnisse wie folgt zusammenfassen:

Korollar 6.5.19 (Nilpotente Normalform)**.** *Ist Φ nilpotent vom Grad k, so besitzt Φ eine darstellende Matrix in unterer/oberer nilpotenter Normalform mit genau* $\operatorname{rk}(\Phi^{j-1}) - 2\operatorname{rk}(\Phi^j) + \operatorname{rk}(\Phi^{j+1})$ *Jordanblöcken der Größe j für $j \in \{1,\dots,k\}$.*

Bemerkung 6.5.20 (Konventionen)**.** Man kann nilpotente Endomorphismen durch Matrizen in oberer oder unterer nilpotenter Normalform darstellen, und man kann die Blöcke beliebig, z.B. der Größe nach aufsteigend oder absteigend ordnen. Diese Wahlfreiheiten gibt es, und verschiedene Autoren verwenden verschiedene Konventionen. Die Mehrheitskonvention, der auch wir hier folgen wollen, ist es, die *obere* Normalform zu verwenden und die Blöcke nach *absteigender* Größe anzuordnen (d.h. $n_1 \geq n_2 \geq \cdots \geq n_\ell$). Das bedeutet, dass man die Ketten *rückwärts* in die Basis schreibt und mit der *längsten Kette* anfängt.

Wir können Korollar 6.5.19 auch in Matrizensprache formulieren. Wir nennen eine Partition $(n_1,\dots,n_\ell)$ von n *normalisiert*, falls $n_1 \geq \cdots \geq n_\ell$ gilt.

Korollar 6.5.21. *ist $A \in \mathbb{K}^{n\times n}$ nilpotent vom Grad k, so existiert eine normalisierte Partition $(n_1,\dots,n_\ell)$ von n und eine Matrix $S \in \mathrm{GL}_n(\mathbb{K})$, so dass*

$$A = SJ_+(n_1,\dots,n_\ell)S^{-1} \quad \text{und} \quad \forall j \in \{1,\dots,k\} : |\{i \in \{1,\dots,l\} \mid n_i = j\}| = \operatorname{rk}(A^{j-1}) - 2\operatorname{rk}(A^j) + \operatorname{rk}(A^{j+1})$$

Wir werden in Satz 6.5.28 sehen, dass die normalisierte Partition $(n_1,\dots,n_\ell)$ durch A eindeutig bestimmt ist, aber das ist an dieser Stelle noch alles andere als klar. Schauen wir uns nun an, was Korollar 6.5.19 in unseren Beispielen bedeutet:

Beispiel 6.5.22. Wie sehen die Normalformen in den konkreten Fällen aus Beispiel 6.5.15 aus?

(i) Sei Φ wie in Beispiel 6.5.7. Setzen wir $\mathscr{B} := (\Phi(e_1), e_1, \Phi(e_2), e_2)$, so besteht

$$D_{\mathscr{B}}(\Phi) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

aus 2 oberen Jordanblöcken der Größe 2. Beachte, dass wir die beiden Ketten rückwärts durchlaufen. In Matrizensprache haben wir gezeigt, dass

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

Links steht hier die darstellende Matrix von Φ bzgl. der Standardbasis, rechts in der Mitte die Matrix in nilpotenter Normalform, und wir konjugieren mit der Matrix, deren Spalten durch die Kettenbasis gegeben sind, wobei wir die Ketten rückwärts(!) durchlaufen.

(ii) Sei nun Φ wie in Beispiel 6.5.8. Wählen wir die (rückwärts) geordnete Kettenbasis

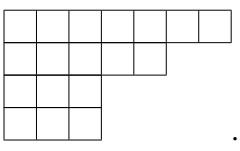
$$\mathscr{B} := \left(\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} \right),$$

so hat die darstellende Matrix zwei Jordanblöcke der Größe 2 bzw. 1, also gilt insbesondere

$$\begin{pmatrix} 0 & -1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{=:D_{\mathscr{B}}(\Phi)} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}^{-1}.$$

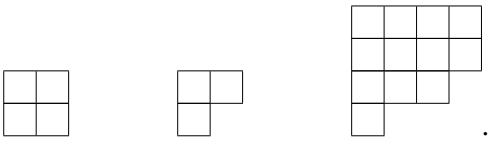
(iii) Schließlich sei $\Phi \in \mathrm{End}_{\mathbb{K}}(\mathbb{K}^{12})$ mit $\mathrm{rk}(\Phi) = 8$, $\mathrm{rk}(\Phi^2) = 5$, $\mathrm{rk}(\Phi^3) = 2$ und $\Phi^4 = 0$. Aufgrund unserer Rechnung in Beispiel 6.5.15.(iii) existiert dann eine darstellende Matrix von Φ in Jordannormalform mit 2 Blöcken der Größe 4, einem Block der Größe 3 und einem Block der Größe 1.

Bemerkung 6.5.23 (Veranschaulichung mittels Tableaus)**.** Man kann sich eine normalisierte Partition $(n_1, \ldots, n_\ell)$ von n durch ein sogenanntes *Tableau* mit ℓ Zeilen veranschaulichen. Dies ist eine linksbündige Anordnung von n quadratischen Kästchen, wobei die erste Zeile n_1 Kästchen enthält, die zweite Zeile n_2 Kästchen usw. Z.B. entspricht die normalisierte Partition (7,5,3,3) von 18 dem Tableau



.

Jedes Tableau definiert eine normalisierte Partition $(n_1,\dots,n_k)$ und damit eine nilpotente Matrix $J_+(n_1,\dots,n_k)$. Die drei Darstellungsmatrizen in Normalform aus Beispiel 6.5.22 werden z.B. durch die folgenden Tableaus beschrieben:



Bemerkung 6.5.24 (Bedeutung des Tableaus)**.** Angenommen der nilpotente Endomorphismus $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ besitzt eine Darstellungsmatrix der Form $J_+(n_1,\dots,n_k)$ bzgl. einer Basis $\mathscr{B}$ (die dann automatisch eine Kettenbasis ist). Die folgenden Eigenschaften von Φ kann man direkt aus dem zugehörigen Tableau ablesen:

(i) Die Anzahl der Kästchen des Tableaus ist die Dimension von V.

(ii) Die Anzahl der Zeilen ist die Anzahl der Ketten in $\mathscr{B}$.

(iii) Die Anzahl der Spalten (bzw. die Anzahl der Kästchen in der ersten Zeile) ist der Nilpotenz-Grad von Φ.

(iv) Die Anzahl der Kästchen in der $j$ten Spalte ist die Anzahl der Elemente vom Φ-Grad j in $\mathscr{B}$.

(v) Die Anzahl der Kästchen in der erste Spalte ist der Defekt von Φ.

(vi) Allgemeiner ist die Anzahl der Kästchen in den ersten j Spalten der Defekt von Φ^j. Die Anzahl der Kästchen in der $j$ten Spalte ist daher $\mathrm{def}(\Phi^j) - \mathrm{def}(\Phi^{j-1})$.

Übung 6.5.25. Beweise Sie die Behauptungen aus Bemerkung 6.5.24!

Mittels der nilpotenten Normalform können wir nun das Normalformenproblem für nilpotente Endomorphismen lösen.

Proposition 6.5.26. *Es sei $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ nilpotent vom Grad k und $\Psi \in \mathrm{End}_{\mathbb{K}}(V)$ beliebig. Sind Φ und Ψ ähnlich, so ist auch Ψ nilpotent vom Grad k.*

Beweis. Sind A und B darstellende Matrizen von Φ und Ψ, so existiert $S \in \mathrm{GL}(V)$ mit $B = SAS^{-1}$. Es gilt dann $B^k = SA^kS^{-1}$ und daher $A^k = 0$ genau dann, wenn $B^k = 0$. □

Proposition 6.5.27. *Seien Φ und Ψ nilpotente Endomorphismen vom Grad k. Dann sind die folgenden Aussagen äquivalent:*

(i) *Φ und Ψ sind ähnlich zueinander.*

(ii) $\mathrm{def}(\Phi^j) = \mathrm{def}(\Psi^j)$ *für alle* $j \in \{0,\dots,k-1\}$.

(iii) $\mathrm{rk}(\Phi^j) = \mathrm{rk}(\Psi^j)$ *für alle* $j \in \{0,\dots,k-1\}$.

(iv) *Φ und Ψ haben eine darstellende Matrix in nilpotenter Normalform mit der gleichen Anzahl Blöcke von jeder Größe.*

Beweis. (i) $\Longrightarrow$ (ii): Sind Φ und Ψ ähnlich, so auch Φ^j und Ψ^j für jedes $j \in \{0,\dots,k-1\}$. Die Behauptung folgt dann aus der Beobachtung, dass der Defekt eine Ähnlichkeitsinvariante ist.

(ii) $\Longrightarrow$ (iii): Dies folgt aus der Rang-Defekt-Formel.

(iii) $\Longrightarrow$ (iv): Dies folgt aus Korollar 6.5.19.

(iv) $\Longrightarrow$ (i): Sind $\mathscr{B}$ und $\mathscr{B}'$ geordnete Basen, so dass $D_{\mathscr{B}}(\Phi)$ und $D_{\mathscr{B}'}(\Psi)$ in oberer nilpotenter Normalform mit der gleichen Anzahl Blöcke von jeder Größe sind, so kann man die Basis $\mathscr{B}'$ so umordnen, dass die beiden darstellenden Matrizen gleich sind. □

Im folgenden bezeichne $\mathrm{Part}^0(n)$ die Menge der normalisierten Partitionen von n. Wir schreiben $\mathrm{Nil}_n(\mathbb{K}) \subseteq \mathbb{K}^{n\times n}$ für die Teilmenge der nilpotenten Matrizen und $\mathrm{Nil}_n(\mathbb{K})/\sim$ für die Menge der Ähnlichkeitsklassen solcher Matrizen

Satz 6.5.28 (Klassifikation der nilpotenten Ähnlichkeitsklassen)**.** *Die Abbildung*

$$\mathrm{Part}^0(n) \to \mathrm{Nil}_n(\mathbb{K})/\sim, \quad (n_1,\dots,n_\ell) \mapsto [J_+(n_1,\dots,n_\ell)].$$

ist eine Bijektion.

Beweis. Surjektivität folgt aus Korollar 6.5.21. Wir behaupten nun, dass man $(n_1,\dots,n_\ell) \in \mathrm{Part}^0(n)$ aus $[J_+(n_1,\dots,n_\ell)]$ zurückgewinnen kann: Wenn wir $[J_+(n_1,\dots,n_\ell)]$ kennen, dann kennen wir insbespondere $\mathrm{def}(J_+(n_1,\dots,n_\ell)^j)$ für alle $j > 0$. Damit können wir aber mittels Bemerkung 6.5.24.(vi) die Anzahl der Kästchen in jeder Spalte des Tableaus von $(n_1,\dots,n_\ell)$ und daher das gesamte Tableau rekonstruieren. □

Es gibt also insbesondere stets nur *endlich viele* Ähnlichkeitsklassen nilpotenter Endomorphismen eines gegebenen Vektorraums, und die genaue Anzahl hängt nur von der Dimension des Vektorraums ab, aber nicht vom Grundkörper!

Zusammenfassung von Abschnitt 6.5

(1) Jeder nilpotente Endomorphismus besitzt eine Kettenbasis und die zugehörige darstellende Matrix ist in (unterer oder oberer) nilpotenter Normalform.

(2) Jede nilpotente Matrix ist ähnlich zu einer bis auf Reihenfolge der Blöcke eindeutig bestimmten Matrix in oberer nilpotenter Normalform. Ähnlichkeitsklassen nilpotenter Endomorphismen/Matrizen werden daher durch normalisierte Partitionen (bzw. Tableaus) parametrisiert.

(3) Zwei nilpotente Endomorphismen sind genau dann ähnlich, wenn ihre Potenzen dieselben Ränge (bzw. Defekte) besitzen. Die zugehörige Partition lässt sich direkt aus diesen Rängen berechnen.

6.6 Fitting–Zerlegung und Jordannormalform

Im letzten Abschnitt haben wir nilpotente Endomorphismen bis auf Ähnlichkeit klassifiziert und in diesem Sinne „vollständig verstanden“. Man kann nun die nilpotente Theorie verwenden, um allgemeinere trigonalisierbare Endomorphismen bis auf Ähnlichkeit zu klassifizieren. Hierzu gibt es verschiedene Zugänge; wir präsentieren hier einen Zugang von HANS FITTING[12],

[12] dt. Mathematiker, 1906–1938, Schüler von Emmy Noether, der in seinen wenigen Lebensjahren mehrere Durchbrüche in der Gruppentheorie und der Theorie der Moduln erzielte

der auf der Abspaltung eines maximal nilpotenten Teils eines Endomorphismus basiert und der in vielen Teilgebieten der Algebra nützlich ist. Es sei stets $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum mit $n := \dim_{\mathbb{K}}(V) < \infty$ und $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$.

Konstruktion 6.6.1 (Stabiler Kern und stabiles Bild)**.** Die Kerne bzw. die Bilder der Potenzen von Φ bilden eine aufsteigende bzw. absteigende Fahne der Form

$$\{0\} \subseteq \ker(\Phi) \subseteq \ker(\Phi^2) \subseteq \ker(\Phi^3) \subseteq \ldots \subseteq V \quad \text{und} \quad V \supseteq \mathrm{Bild}(\Phi) \supseteq \mathrm{Bild}(\Phi^2) \supseteq \mathrm{Bild}(\Phi^3) \supseteq \cdots \supseteq \{0\},$$

und da Dimension monton bzgl. Inklusion von Unterräumen ist gilt, folgt

$$0 \leq \dim\ker(\Phi) \leq \dim\ker(\Phi^2) \leq \cdots \leq n \quad \text{und} \quad n \geq \dim\mathrm{Bild}(\Phi) \geq \dim\mathrm{Bild}(\Phi^2) \geq \cdots \geq 0.$$

Eine beschränkte monotone Folge natürlicher Zahlen muss aber ab irgendeinem Punkt konstant werden, daher existiert ein $t \in \mathbb{N}$ mit

$$\dim\ker(\Phi^t) = \dim\ker(\Phi^{t+1}) = \dim\ker(\Phi^{t+2}) = \ldots \quad \text{und} \quad \dim\mathrm{Bild}(\Phi^t) = \dim\mathrm{Bild}(\Phi^{t+1}) = \ldots,$$

und da ein Untervektorraum von voller Dimension bereits der ganze Raum ist, folgt

$$\ker(\Phi^t) = \ker(\Phi^{t+1}) = \ker(\Phi^{t+2}) = \ldots \quad \text{und} \quad \mathrm{Bild}(\Phi^t) = \mathrm{Bild}(\Phi^{t+1}) = \mathrm{Bild}(\Phi^{t+2}) = \ldots, \tag{6.6.1}$$

d.h. die Fahne der Kerne bzw. Bilder der Potenzen von Φ stabilisiert sich zu irgendeinem Zeitpunkt t. Wir nennen dann

$$\ker_\infty(\Phi) := \ker(\Phi^t) \quad \text{bzw.} \quad \mathrm{Bild}_\infty(\Phi) := \mathrm{Bild}(\Phi^t).$$

den *stabilen Kern* bzw. das *stabile Bild* von Φ.

Beispiel 6.6.2. Ist Φ nilpotent, so ist $\ker_\infty(\Phi) = V$ (aber im Allgemeinen $\ker(\Phi) \neq V$) und daher $\mathrm{Bild}_\infty(\Phi) = \{0\}$ (aber im Allgemeinen $\mathrm{Bild}(\Phi) \neq \{0\}$). Der stabile Kern kann also echt größer als der Kern sein, und das stabile Bild kann echt kleiner als das Bild sein.

Bemerkung 6.6.3. Wegen der Rang-Defekt-Formel gilt: Ist $\ker(\Phi^t) = \ker(\Phi^{t+1}) = \ker(\Phi^{t+2}) = \ldots$ für ein $t > 0$, so gilt auch schon $\mathrm{Bild}(\Phi^t) = \mathrm{Bild}(\Phi^{t+1}) = \mathrm{Bild}(\Phi^{t+2}) = \ldots$ (und umgekehrt).

Satz 6.6.4 (Fitting-Zerlegung)**.** *Der stabile Kern und das stabile Bild haben die folgenden Eigenschaften:*

(i) $\ker_\infty(\Phi)$ *und* $\mathrm{Bild}_\infty(\Phi)$ *sind* Φ*-invariante Unterräume von* V*.*

(ii) $\ker_\infty(\Phi)$ *ist* Φ*-invariant und der induzierte Endomorphismus* $\Phi_{\ker_\infty(\Phi)}$ *ist nilpotent.*

(iii) $\mathrm{Bild}_\infty(\Phi)$ *ist* Φ*-invariant und* $\Phi_{\mathrm{Bild}_\infty(\Phi)}$ *ist bijektiv.*

(iv) $V = \ker_\infty(\Phi) \oplus \mathrm{Bild}_\infty(\Phi)$*.*

Beweis. Es sei stets $t \in \mathbb{N}$ wie in (6.6.1) gewählt. Der Beweis ist ein einziger „Schwindel mit Unendlichkeiten“, und beruht grob gesagt auf den formalen Identitäten „$\infty \pm 1 = \infty$“ (vgl. Hilberts Hotel) und „$2 \cdot \infty = \infty$“.

(i) Für alle $k \in \mathbb{N}$ und $x, y \in V$ gelten die beiden Implikationen

$$\Phi^k(x) = 0 \implies \Phi^{k-1}(\Phi(x)) = 0 \quad \text{und} \quad x = \Phi^k(y) \implies \Phi(x) = \Phi(\Phi^k(y)) = \Phi^{k+1}(y),$$

und folglich gilt $\Phi[\ker(\Phi^k)] \subseteq \ker(\Phi^{k-1})$ und $\Phi[\mathrm{Bild}(\Phi^k)] \subseteq \mathrm{Bild}(\Phi^{k+1})$. Die Idee ist nun, zu verwenden, dass „$\infty \pm 1 = \infty$“. Etwas formaler rechnet man nach, dass

$$\begin{aligned} \Phi[\ker_\infty(\Phi)] &= \Phi[\ker(\Phi^{t+1})] \subseteq \ker(\Phi^t) = \ker_\infty(\Phi), \\ \Phi[\mathrm{Bild}_\infty(\Phi)] &= \Phi[\mathrm{Bild}(\Phi^t)] \subseteq \mathrm{Bild}(\Phi^{t+1}) = \mathrm{Bild}_\infty(\Phi). \end{aligned}$$

(ii) Es gilt $(\Phi_{\ker_\infty(\Phi)})^t = \Phi^t_{\ker_\infty(\Phi)} = \Phi^t_{\ker(\Phi^t)} = 0$.

(iii) Es gilt $\Phi[\mathrm{Bild}(\Phi^t)] = \mathrm{Bild}(\Phi^{t+1})$ (warum?), also ist $\Phi_{\mathrm{Bild}_\infty(\Phi)}$ nach dem obigen „$\infty + 1 = \infty$-Trick“ surjektiv, und daher bijektiv.

(iv) Sei $x \in \ker_\infty(\Phi) \cap \mathrm{Bild}_\infty(\Phi) = \ker(\Phi^t) \cap \mathrm{Bild}_\infty(\Phi^t)$. Dann existiert ein $y \in V$ mit $\Phi^t(y) = x$ und es gilt $\Phi^t(x) = 0$. Daraus folgt nun aber

$$\Phi^{2t}(y) = \Phi^t(\Phi^t(y)) = \Phi^t(x) = 0, \quad \text{also} \quad y \in \ker(\Phi^{2t}).$$

Nun ist aber $\ker(\Phi^{2t}) = \ker(\Phi^t)$ (oder informell, „$2 \cdot \infty = \infty$“), also $y \in \ker(\Phi^t)$, und daher $x = \Phi^t(y) = 0$.

Dieser Schwindel zeigt, dass die Summe $\ker_\infty(\Phi) \oplus \mathrm{Bild}_\infty(\Phi)$ direkt ist. Ihre Dimension ist daher gegeben durch $\mathrm{def}(\Phi^t) + \mathrm{rk}(\Phi^t)$, was nach der Rang-Defekt-Formel gerade $\dim V$ ist. Dies zeigt, dass $V = \ker_\infty(\Phi) \oplus \mathrm{Bild}_\infty(\Phi)$. □

Übung 6.6.5 (Fitting-Zerlegung für diagonalisierbare Endomorphismen)**.** Zeigen Sie: Ist Φ diagonalisierbar, so ist $\ker_\infty(\Phi) = \ker(\Phi)$ und $\mathrm{Bild}_\infty(\Phi) = \mathrm{Bild}(\Phi)$, insbesondere gilt dann die „Erstsemesterzerlegung“ $V = \ker(\Phi) \oplus \mathrm{Bild}(\Phi)$.

Bemerkung 6.6.6 (Fitting-Zerlegung für Matrizen)**.** In Matrizensprache besagt der Satz, dass es für jede Matrix $A \in \mathbb{K}^{n \times n}$ eine Matrix $S \in \mathrm{GL}_n$ sowie eine nilpotente Matrix $B \in \mathbb{K}^{k \times k}$ und eine invertierbare Matrix $C \in \mathrm{GL}_{n-k}(\mathbb{K})$ gibt mit

$$A = S \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} S^{-1}.$$

Hierbei ist $k := \dim \ker_\infty(A)$, und die Spalten von S setzen sich aus einer Basis von $\ker_\infty(\Phi)$ und einer Basis von $\mathrm{Bild}_\infty(\Phi)$ zusammen.

Beispiel 6.6.7 (Eine Fitting-Zerlegung)**.** Wir betrachten die Matrix

$$A := \begin{pmatrix} 3 & 5 & -4 \\ -3 & 1 & 1 \\ 0 & 6 & -3 \end{pmatrix}.$$

Es gilt dann

$$A^2 = \begin{pmatrix} -6 & -4 & 5 \\ -12 & -8 & 10 \\ -18 & -12 & 15 \end{pmatrix},$$

also hat die Matrix A^2 den Rang 1 und ihr Bild wird von $v := (1,2,3)^\top$ aufgespannt. Nun gilt aber $Av = v$, und daher ist

$$\mathrm{Bild}_\infty(A) = \mathrm{Bild}(A^2) = \mathrm{Bild}(A^3) = \cdots = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \right\rangle.$$

Daraus folgt nun, dass

$$\ker_\infty(A) = \ker(A^2) = \ker \begin{pmatrix} -6 & -4 & 5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 5 \\ 0 \\ 6 \end{pmatrix}, \begin{pmatrix} -4 \\ 6 \\ 0 \end{pmatrix} \right\rangle$$

Es gilt $A(5,0,6)^\top = (-9,-9,-18)^\top$ und $A(-9,-9,-18)^\top = 0$, also ist $\{(5,0,6)^\top, (-9,-9,18)^\top\}$ eine Kettenbasis für $A_{\ker_\infty(A)}$. Wir erhalten daher

$$A = \begin{pmatrix} -9 & 5 & 1 \\ -9 & 0 & 2 \\ -18 & 6 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -9 & 5 & 1 \\ -9 & 0 & 2 \\ -18 & 6 & 3 \end{pmatrix}^{-1}.$$

In diese speziellen Fall (wo der invertierbare Teil nur eine Einheitsmatrix ist), erhalten wir

$$A^2 = A^3 = \cdots = \begin{pmatrix} -9 & 5 & 1 \\ -9 & 0 & 2 \\ -18 & 6 & 3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -9 & 5 & 1 \\ -9 & 0 & 2 \\ -18 & 6 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} -6 & -4 & 5 \\ -12 & -8 & 10 \\ -18 & -12 & 15 \end{pmatrix}.$$

[24.04.24]

Lemma 6.6.8 (Eigenschaften der Fitting-Zerlegung)**.** *Die Fitting-Zerlegung hat die folgenden Eigenschaften:*

(i) (Eindeutigkeit) *Ist $V = U \oplus W$ eine beliebige Zerlegung in Φ-invariante Unterräume mit Φ_U nilpotent und Φ_W bijektiv, so ist $U = \ker_\infty(\Phi)$ und $W = \mathrm{Bild}_\infty(\Phi)$.*

(ii) (Natürlichkeit) *Sei W ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\Psi \in \mathrm{End}_\mathbb{K}(W)$. Ist $\alpha \in \mathrm{Hom}_\mathbb{K}(V,W)$ mit $\alpha \circ \Phi = \Psi \circ \alpha$, so gilt*

$$\alpha[\ker_\infty(\Phi)] \subseteq \ker_\infty(\Psi) \quad \text{und} \quad \alpha[\mathrm{Bild}_\infty(\Phi)] \subseteq \mathrm{Bild}_\infty(\Psi).$$

(iii) Falls $\alpha \in \mathrm{End}_\mathbb{K}(V)$ mit Φ vertauscht, so sind $\ker_\infty(\Phi)$ und $\mathrm{Bild}_\infty(\Phi)$ auch α-invariant.

(iv) Ist $T < V$ ein Untervektorraum mit $\Phi[T] = T$, so ist $T \subseteq \mathrm{Bild}_\infty(\Phi)$.

(v) Ist $V = \bigoplus_{i=1}^m V_i$ eine Zerlegung in Φ-invariante Unterräume, so gilt

$$\ker_\infty(\Phi) = \bigoplus_{i=1}^m \ker_\infty(\Phi_{V_i}) = \bigoplus_{i=1}^m (\ker_\infty(\Phi) \cap V_i) \text{ und } \mathrm{Bild}_\infty(\Phi) = \bigoplus_{i=1}^m \mathrm{Bild}_\infty(\Phi_{V_i}) = \bigoplus_{i=1}^m (\mathrm{Bild}_\infty(\Phi) \cap V_i).$$

Beweis. Es sei stets $t \in \mathbb{N}$ wie in (6.6.1) gewählt.

(i) Zwei Inklusionen sieht man leicht: Ist $u \in U$, so existiert ein $m \geq t$ mit $\Phi^m(u) = 0$, also ist $u \in \ker(\Phi^m) = \ker_\infty(\Phi)$ und ist $w \in W$, so ist $w = \Phi^t((\Phi_W^{-1})^t(w)) \in \mathrm{Bild}(\Phi^t) = \mathrm{Bild}_\infty(\Phi)$, also

$$U \subseteq \ker_\infty(\Phi) \quad \text{und} \quad W \subseteq \mathrm{Bild}_\infty(\Phi).$$

Wäre eine der beiden Inklusionen echt, so wäre $n = \dim(U \oplus W) < \dim(\ker_\infty(\Phi) \oplus \mathrm{Bild}_\infty(\Phi)) = n$, was ein Widerspruch ist.

(ii) Dies ist eine Routine-Rechnung (Übung!).

(iii) Dies ist ein Spezialfall von (ii), nämlich der Fall $\Phi = \Psi$.

(iv) Nach Annahme ist $\Psi := \Phi_T : T \to T$ surjektiv, also bijektiv, und $\Psi|_{\{0\}}$ nilpotent, also ist die Zerlegung $T = \{0\} \oplus T$ nach (i) die Fitting-Zerlegung von Ψ, und insbesondere gilt $T = \mathrm{Bild}_\infty(\Psi)$. Ist $\alpha : T \to V$ die Inklusion, so gilt $\alpha \circ \Phi = \Psi \circ \alpha$, und wegen (ii) gilt dann $T = \alpha(T) = \alpha(\mathrm{Bild}_\infty(\Psi)) \subseteq \mathrm{Bild}_\infty(\Phi)$.

(v) Nach Definition ist Φ nilpotent auf $\ker_\infty(\Phi_{V_i})$ und injektiv (und daher bijektiv) auf $\mathrm{Bild}_\infty(\Phi_{V_i})$, und daher auf der direkten Summe dieser Räume. Mit (i) folgt, dass

$$\ker_\infty(\Phi) = \bigoplus_{i=1}^m \ker_\infty(\Phi_{V_i}) \quad \text{und} \quad \mathrm{Bild}_\infty(\Phi) = \bigoplus_{i=1}^m \mathrm{Bild}_\infty(\Phi_{V_i}).$$

Nach Definition gilt für $x \in V$, dass

$$x \in \ker_\infty(\Phi_{V_i}) \Leftrightarrow \exists\, t \in \mathbb{N} : \Phi_{V_i}^t(x) = 0 \Leftrightarrow x \in V_i \text{ und } \exists\, t \in \mathbb{N} : \Phi^t(x) = 0 \Leftrightarrow x \in V_i \cap \ker_\infty(\Phi).$$

Dies zeigt die Aussage für die stabilen Kerne. Die Inklusion $\mathrm{Bild}_\infty(\Phi_{V_i}) \subseteq \mathrm{Bild}_\infty(\Phi) \cap V_i$ ist klar. Sei umgekehrt $x \in \mathrm{Bild}_\infty(\Phi) \cap V_i$. Schreibe $x = \Phi^t(y_1 + \cdots + y_m)$ mit $t \in \mathbb{N}$ und $y_j \in V_j$. Dann gilt

$$x - \Phi^t(y_i) = \sum_{j \neq i} \Phi^t(y_j) \in V_i \cap (\bigoplus_{j \neq i} V_j) = \{0\},$$

also $x = \Phi^t(y_i) \in \mathrm{Bild}_\infty(\Phi_{V_i})$. Dies zeigt die Aussage über die stabilen Bilder. □

Bemerkung 6.6.9 (Fitting-Zerlegung und charakteristisches Polynom)**.** Sei $V = U \oplus W$ die Fitting-Zerlegung von Φ. Da Φ_U nilpotent ist, gilt $\chi_{\Phi_U} = X^{\dim U}$. Da Φ_W bijektiv ist, ist $\ker(\Phi_W) = \{0\}$ und daher 0 kein Eigenwert von Φ_W. Es gilt also

$$\chi_\Phi = \chi_{\Phi_U}\chi_{\Phi_W} = X^{\dim U}\chi_{\Phi_W} \quad \text{mit } X \nmid \chi_{\Phi_W}.$$

Φ_U hat also nur den Eigenwert 0 und Φ_W hat alle Eigenwerte von Φ außer 0.

Beispiel 6.6.10. Ist $\Phi = \Phi_A$ mit A wie in Beispiel 6.6.7, so ist $\chi_\Phi = X^2(X-1)$. Ist $\mathbb{R}^3 = U \oplus W$ die zugehörige Fitting-Zerlegung, so gilt also $\chi_{\Phi_U} = X^2$ und $\chi_{\Phi_W} = X - 1$.

Ist hingegen $\Psi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^5)$ mit $\chi_\Psi = X^2(X-1)^2(X-2)$ und Fitting-Zerlegung $\mathbb{R}^5 = U \oplus W$, so ist $\chi_{\Psi_U} = X^2$ und $\chi_{\Psi_W} = (X-1)^2(X-2)$.

Konstruktion 6.6.11 (Haupträume)**.** Für $\lambda \in \mathbb{K}$ schreiben wir $\Phi_\lambda := \Phi - \lambda \cdot \mathrm{Id}$. Nach Definition ist dann

$$V_\lambda(\Phi) := \ker(\Phi_\lambda)$$

der Eigenraum zum Eigenwert λ. Falls Φ nicht diagonalisierbar ist, so sind diese Eigenräume zu klein, um ganz V aufzuspannen. In diese Fall können wir die Eigenräume vergrößern, indem wir den Kern durch den stabilen Kern ersetzen. Wir nennen

$$V^\lambda(\Phi) := \ker_\infty(\Phi_\lambda) = \{v \in V \mid \exists k \in \mathbb{N} \colon (\Phi - \lambda \cdot \mathrm{Id})^k v = 0\}.$$

den *Hauptraum* zu λ. Nach Definition ist Φ_λ nilpotent auf $V^\lambda(\Phi)$ (und wirkt durch 0 auf dem Unterraum $V_\lambda(\Phi)$).

Übung 6.6.12. Zeigen Sie:

(i) $\chi_{\Phi_\lambda}(X) = \chi_\Phi(X + \lambda)$ und $\chi_\Phi(X) = \chi_{\Phi_\lambda}(X - \lambda)$.

(ii) Ist $U \leq V$ ein Φ-invarianter Unterraum, so gilt $(\Phi_U)_\lambda = (\Phi_\lambda)_U$.

(iii) Es gilt $V^\lambda(\Phi) \neq \{0\}$ genau dann, wenn $\lambda \in \mathrm{spec}_{\mathbb{K}}(\Phi)$.

Wie hängen nun die stabilen Kerne und Bilder der verschiedenen Φ_λ zusammen?

Lemma 6.6.13. *Seien $\lambda, \mu \in \mathbb{K}$.*

(i) $\ker_\infty(\Phi_\lambda)$ *und* $\mathrm{Bild}_\infty(\Phi_\lambda)$ *sind Φ_μ-invariant.*

(ii) Falls $\lambda \neq \mu$, so gilt $\ker_\infty(\Phi_\lambda) \subseteq \mathrm{Bild}_\infty(\Phi_\mu)$.

(iii) Falls $\lambda \neq \mu$, so gilt

$$V = V^\lambda(\Phi) \oplus V^\mu(\Phi) \oplus (\mathrm{Bild}_\infty(\Phi_\lambda) \cap \mathrm{Bild}_\infty(\Phi_\mu)).$$

Beweis. (i) Wegen Lemma 6.6.8.(iii) genügt es zu zeigen, dass

$$\Phi_\lambda \circ \Phi_\mu = (\Phi - \lambda \cdot \mathrm{Id}) \circ (\Phi - \mu \cdot \mathrm{Id}) = \Phi^2 - (\lambda + \mu)\Phi + \lambda\mu \cdot \mathrm{Id} = (\Phi - \mu \cdot \mathrm{Id}) \circ (\Phi - \lambda \cdot \mathrm{Id}) = \Phi_\mu \circ \Phi_\lambda.$$

(ii) Wir betrachten den induzierten Endomorphismus

$$\Psi := (\Phi_\mu)_{\ker_\infty(\Phi_\lambda)} : \ker_\infty(\Phi_\lambda) \to \ker_\infty(\Phi_\lambda), \quad v \mapsto \Phi_\mu(v).$$

Wäre Ψ nicht surjektiv (also nicht injektiv), dann gäbe es ein $v \in \ker_\infty(\Phi_\lambda) \setminus \{0\}$ mit $\Psi(v) = 0$, also $\Phi(v) = \mu v$ und daher $\Phi_\lambda(v) = (\mu - \lambda)v$, also hätte die Einschränkung von Φ_λ auf seinen stabilen Kern den Eigenwert $\mu - \lambda \neq 0$ im Widerspruch zu Bemerkung 6.6.9.

Es gilt also $\Phi_\mu[\ker_\infty(\Phi_\lambda)] = \ker_\infty(\Phi_\lambda)$ und Anwenden von Lemma 6.6.8.(iv) auf $T := \ker_\infty(\Phi_\lambda)$ liefert die Behauptung.

(iii) Aus (i) und Lemma 6.6.8.(v) folgt, dass

$$\begin{aligned} V = &(\ker_\infty(\Phi_\lambda) \cap \ker_\infty(\Phi_\mu)) \oplus (\mathrm{Bild}_\infty(\Phi_\lambda) \cap \ker_\infty(\Phi_\mu)) \\ &\oplus (\ker_\infty(\Phi_\lambda) \cap \mathrm{Bild}_\infty(\Phi_\mu)) \oplus ((\mathrm{Bild}_\infty(\Phi_\lambda) \cap (\mathrm{Bild}_\infty(\Phi_\mu)), \end{aligned}$$

und aus (ii) folgt, dass $\ker_\infty(\Phi_\lambda) \cap \ker_\infty(\Phi_\mu) = \{0\}$ sowie $\mathrm{Bild}_\infty(\Phi_\lambda) \cap \ker_\infty(\Phi_\mu) = \ker_\infty(\Phi_\mu)$ und $\mathrm{Bild}_\infty(\Phi_\lambda) \cap \ker_\infty(\Phi_\mu) = \ker_\infty(\Phi_\mu)$. Die Behauptung folgt dann aus der Definition der Haupträume. □

Bemerkung 6.6.14. Das Argument in (iii) können wir iterieren: Sind $\lambda_1, \dots, \lambda_k$ paarweise verschieden, so erhalten wir

$$V = V^{\lambda_1}(\Phi) \oplus \cdots \oplus V^{\lambda_k}(\Phi) \oplus \bigcap_{j=1}^{k} \mathrm{Bild}_\infty(\Phi_{\lambda_j}). \tag{6.6.2}$$

Satz 6.6.15 (Satz von der Hauptraumzerlegung)**.** *Es seien $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von Φ in $\mathbb{K}$ und $e_1, \dots, e_k$ ihre algebraischen Vielfachheiten. Wir definieren*

$$V^\emptyset(\Phi) = \bigcap_{j=1}^{k} \mathrm{Bild}_\infty(\Phi_{\lambda_j}).$$

*(i) V besitzt die folgende Zerlegung in Φ-invariante Unterräume (*Hauptraumzerlegung*):*

$$V = V^{\lambda_1}(\Phi) \oplus \cdots \oplus V^{\lambda_k}(\Phi) \oplus V^\emptyset(\Phi).$$

(ii) $\dim_{\mathbb{K}} V^{\lambda_j}(\Phi) = e_j$ *und* $\Phi_{V^{\lambda_j}(\Phi)}$ *hat charakteristisches Polynom* $(X - \lambda_j)^{e_j}$ *für alle* $j \in \{1, \dots, k\}$.

(iii) $\dim_{\mathbb{K}} V^\emptyset(\Phi) = \dim V - \sum_{j=1}^{k} e_j$ *und* $\mathrm{spec}(\Phi_{V^\emptyset(\Phi)}) = \emptyset$.

Beweis. Wir schreiben das charakteristische Polynom von Φ als

$$\chi_\Phi(X) = (X - \lambda_1)^{e_1} \cdots (X - \lambda_k)^{e_k} \cdot f(X),$$

wobei $f \in \mathbb{K}[X]$ ein Polynom ist, dass in $\mathbb{K}$ keine weitere Nullstelle besitzt. (i) folgt nun unmittelbar aus (6.6.2). Aus Bemerkung 6.6.9 und Übung 6.6.12.(i) folgt, dass

$$\chi_{\Phi_{V^{\lambda_j}(\Phi)}} = (X - \lambda_j)^{e_j} \quad \text{und} \quad \chi_{\Phi_{V^\emptyset(\Phi)}} = f.$$

Dies impliziert nun unmittelbar (ii) und (iii). □

Falls χ_Φ über $\mathbb{K}$ in Linearfaktoren zerfällt, so gilt $V^\emptyset(\Phi) = \{0\}$, also erhalten wir:

Korollar 6.6.16 (Hauptraumzerlegung, trigonalisierbarer Fall)**.** *Falls χ_Φ über $\mathbb{K}$ in Linearfaktoren zerfällt, so gilt*

$$V = \bigoplus_{\lambda \in \mathrm{spec}_{\mathbb{K}}(\Phi)} V^\lambda(\Phi),$$

d.h. V zerfällt als direkte Summe der Haupträume von Φ. □

Notation 6.6.17. Für $\lambda \in \mathbb{K}$ und $m \in \mathbb{N}$ definieren wir den *λ-Jordan-Block* der Größe m as

$$J_+[(m)_\lambda] = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix} \in \mathbb{K}^{m\times m}.$$

Definition 6.6.18. Eine Matrix ist in *Jordannormalform* wenn sie blockdiagonal ist und alle ihre Diagonalblöcke Jordan-Blöcke sind.

Notation 6.6.19. Gegeben $\lambda_1,\dots,\lambda_k \in \mathbb{K}$ und $n_{11},\dots,n_{1m_1},\dots,n_{k1},\dots,n_{km_k} \in \mathbb{N}$ schreiben wir $J_+[(n_{11},\dots,n_{1m_1})_{\lambda_1};\dots;(n_{k1},\dots,n_{km_k})_{\lambda_k}]$ für die Matrix in Jordannormalform, deren Diagonalblöcke durch $J_+[(n_{11})_{\lambda_1}]$, …, $J_+[(n_{1m_1})_{\lambda_1}]$, …, $J_+[(n_{k1})_{\lambda_k}]$, …, $J_+[(n_{km_k})_{\lambda_k}]$ gegeben sind.

Satz 6.6.20 (Satz von der Jordannormalform)**.** *Jeder trigonalisierbare Endomorphismus $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ wird durch eine darstellende Matrix in Jordannormalform repräsentiert, und folglich ist jede trigonalisierbare Matrix ähnlich zu einer Matrix in Jordannormalform.*

Beweis. Sei $\lambda \in \mathrm{spec}_{\mathbb{K}}(\Phi)$ und $V^\lambda(\Phi) = \ker_\infty(\Phi_\lambda)$. Dann ist $(\Phi_\lambda)_{V^\lambda(\Phi)}$ nilpotent, und wir können eine Kettenbasis von $V^\lambda(\Phi)$ für $(\Phi_\lambda)_{V^\lambda(\Phi)}$ finden. Ordnen wir die Ketten nach absteigender Länge und jede Kette rückwärts an, so erhalten wir eine geordnete Basis $\mathscr{B}_\lambda$ von $V^\lambda(\Phi)$, und bzgl. dieser Basis gilt

$$D_{\mathscr{B}_\lambda}((\Phi_\lambda)_{V^\lambda(\Phi)}) = J_+[n_1,\dots,n_k] \implies D_{\mathscr{B}_\lambda}(\Phi_{V^\lambda(\Phi)}) = J_+[(n_1,\dots,n_k)_\lambda],$$

wobei $(n_1,\dots,n_k)$ die normalisierte Partition zu $(\Phi_\lambda)_{V^\lambda(\Phi)}$ ist. Aufgrund von Korollar 6.6.16 können wir nun die Kettenbasen der Haupträume zu einer Basis von V zusammenfügen und erhalten so eine geordnete Basis von V bzgl. derer Φ in Jordannormalform ist. □

Beispiel 6.6.21. Es sei $\Phi : \mathbb{Q}^4 \to \mathbb{Q}^4$ gegeben durch die darstellende Matrix (bzgl. Standardbasis)

$$A := \begin{pmatrix} 1 & 1 & 6 & -2 \\ 0 & 1 & -3 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 2 \end{pmatrix}.$$

Das charakteristische Polynom von Φ ist dann gegeben durch

$$\chi_\Phi(X) = \det\begin{pmatrix} X-1 & -1 & -6 & 2 \\ 0 & X-1 & 3 & -2 \\ 0 & 0 & X-1 & 0 \\ 0 & 0 & 2 & X-2 \end{pmatrix} = \det\begin{pmatrix} X-1 & -1 \\ 0 & X-1 \end{pmatrix}\cdot\det\begin{pmatrix} X-1 & 0 \\ 2 & X-2 \end{pmatrix} = (X-1)^3(X-2),$$

und insbesondere gilt

$$\mathrm{spec}(\Phi) = \{1,2\}.$$

Wir bestimmen zunächst den Hauptraum $V^1(\Phi) = \ker_\infty(\Phi_1)$ zum Eigenwert 1. Nach Satz 6.6.15 ist dieser 3-dimensional. Wir berechnen dazu

$$\ker(\Phi_1) = \ker\begin{pmatrix} 0 & -1 & -6 & 2 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix} = \langle e_1 \rangle,$$

$$\ker(\Phi_1^2) = \ker \begin{pmatrix} 0 & -1 & -6 & 2 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix}^2 = \ker \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -4 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 \end{pmatrix} = \langle e_1, e_2 \rangle,$$

und schließlich

$$\ker(\Phi_1^3) = \ker \begin{pmatrix} 0 & -1 & -6 & 2 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix}^3 = \ker \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix} = \left\langle e_1, e_2, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} \right\rangle.$$

Dieser letzte Kern ist 3-dimensional und daher schon der gesamte Hauptraum $V^1(\Phi)$.

Sei nun $\Psi_1 := (\Phi_1)_{V^1(\Phi)}$. Dann ist Ψ_1 nilpotent vom Grad 3, und seine kanonische Fahne ist nach der obigen Rechnung gegeben durch

$$K_0(\Psi_1) = \{0\} \subsetneq K_1(\Psi_1) = \langle e_1 \rangle \subsetneq K_2(\Psi_1) = \langle e_1, e_2 \rangle \subsetneq K_3(\Psi_1) = \left\langle e_1, e_2, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} \right\rangle.$$

Insbesondere gilt $\operatorname{def}(\Psi_1^j) = \dim K_j(\Psi_1) = j$ und daher $r_j := \operatorname{rk}(\Psi_1^j) = 3 - j$ für $j \in \{0, \ldots, 3\}$. Nach Satz 6.5.14 gibt es daher einer Kette der Länge 2 und keine Ketten der Länge 1 und 0, denn

$$c_3 = r_2 - 2r_3 + r_4 = 1 - 2 \cdot 0 + 0 = 1, \quad c_2 = r_1 - 2r_2 + r_3 = 2 - 2 \cdot 1 + 0 = 0 \quad \text{und} \quad c_1 = r_0 - 2r_1 + r_2 = 3 - 2 \cdot 2 + 1 = 0.$$

Um die eine benötigte Ψ_1-Kette zu finden, können wir einen beliebigen Vektor in $K_3(\Psi_1) \setminus K_2(\Psi_1)$ wählen. Eine offensichtliche Wahl ist hier $v := (0,0,1,2)^\top$, und die zugehörige Kette ist

$$\left\{ v = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \Psi_1(v) = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \Psi_1^2(v) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

Bzgl. der Basis $\mathscr{B}_1 := (\Psi_1^2(v), \Psi_1(v), v)$ gilt dann

$$D_{\mathscr{B}_1}(\Psi_1) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad D_{\mathscr{B}_1}(\Phi_{V^1(\Phi)}) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Der Hauptraum $V^2(\Phi)$ zum Eigenwert 2 ist 1-dimensional, und daher durch den Eigenraum

$$\ker(\Phi_2) = \ker \begin{pmatrix} 1 & -1 & -6 & 2 \\ 0 & 1 & 3 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 \end{pmatrix} = \ker \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \left\langle \underbrace{\begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}}_{=:w} \right\rangle$$

gegeben. Wir setzen daher $\mathscr{B}_2 := \{w\}$ und $\mathscr{B} := (\Psi_1^2(v), \Psi(v), v, w)$. Es gilt dann

$$D_{\mathscr{B}}(\Phi) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

und diese Matrix ist in Jordannormalform. Damit haben wir gezeigt, dass

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

Konstruktion 6.6.22 (Jordan-Datum)**.** Es sei $A \in \mathbb{K}^{n\times n}$; wir wählen eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$, so dass das charakteristische Polynom χ_A über $\mathbb{L}$ in Linearfaktoren zerfällt, also

$$\chi_A = (X-\lambda_1)^{e_1}\cdots(X-\lambda_k)^{e_k},$$

wobei $\lambda_1,\dots,\lambda_k$ die verschiedenen Eigenwerte von A in $\mathbb{L}$ und $e_1,\dots,e_k$ ihre algebraischen Vielfachheiten sind. Es sei dann $\Phi : \mathbb{L}^n \to \mathbb{L}^n$, $v \mapsto Av$ der zugehörige Endomorphismus. Für $j \in \{1,\dots,k\}$ ist $(\Phi_{\lambda_j})_{V^{\lambda_j}(\Phi)}$ nilpotent, und seine Ähnlichkeitsklasse wird daher durch eine normalisierte Partition p_j von e_j parametrisiert. Bezeichnet $\mathscr{P}^0$ die Menge der normalisierten Partitionen, so erhalten wir also eine Abbildung

$$D : \operatorname{spec}_{\mathbb{L}}(A) \to \mathscr{P}^0, \quad D(\lambda_j) := p_j,$$

die jedem Eigenwert eine normalisierte Partition seiner algebraischen Vielfachheit zuordnet. Diese Abbildung heißt das *Jordan-Datum* von A über $\mathbb{L}$. Wir können dieses visualisieren, indem wir zu jedem Eigenwert das entsprechende Tableau zeichnen.

Beispiel 6.6.23. Das Jordan-Datum zur Matrix A aus Beispiel 6.6.21 ist gegeben durch

$$1 \mapsto (3),\ 2 \mapsto (1) \quad \text{bzw.} \quad 1 \mapsto \ydiagram{3},\ 2 \mapsto \ydiagram{1}$$

Satz 6.6.24 (Normalformenproblem für trigonalisierbare Matrizen)**.** *Zwei Matrizen $A,B \in \mathbb{K}^{n\times n}$ sind genau dann ähnlich, wenn sie (über einer hinreichend großen Körpererweiterung von $\mathbb{K}$) dasselbe Jordan-Datum besitzen. Ähnlichkeitsklassen von Matrizen werden also durch Jordan-Daten parametrisiert.*

Beweis. Wir dürfen annehmen, dass $\mathbb{K}$ so groß gewählt ist, dass die charakteristischen Polynome von A und B über $\mathbb{K}$ zerfallen.

Besitzen A und B dasselbe Jordan-Datum $\lambda_1 \mapsto p_1,\dots,\lambda_k \mapsto p_k$, so sind sie beide ähnlich zur Matrix $J_+((p_1)_{\lambda_1},\dots,(p_k)_{\lambda_k})$, also zueinander.

Umgekehrt seien A und B ähnlich und $S \in \mathrm{GL}_n(\mathbb{K})$ mit $B = SAS^{-1}$. Da das charakteristische Polynom eine Ähnlichkeitsinvariante ist, haben dann A und B dieselben Eigenwerte mit denselben geometrischen Vielfachheiten. Insbesondere haben dann die Haupträume von Φ_A und Φ_B dieselben Dimensionen.

Für alle $\lambda \in \operatorname{spec}_{\mathbb{K}}(A) = \operatorname{spec}_{\mathbb{K}}(B)$ gilt nun

$$\Phi_S[V^\lambda(\Phi_A)] = V^\lambda(\Phi_B) \quad \text{und} \quad (\Phi_B)_\lambda)_{V^\lambda(\Phi_B)} = \Phi_S \circ ((\Phi_A)_\lambda)_{V^\lambda(\Phi_A)} \circ \Phi_S^{-1}.$$

Unter der Verwendung der Natürlichkeit der Fitting-Zerlegung ist dies eine Routinerechnung (Übung!). Insbesondere sind die nilpotenten Endomorphismen $((\Phi_B)_\lambda)_{V^\lambda(\Phi_B)}$ und $((\Phi_A)_\lambda)_{V^\lambda(\Phi_A)}$ konjugiert und definieren daher dieselbe Partition, d.h. A und B haben dasselbe Jordan-Datum. □

Bemerkung 6.6.25. In reiner Matrizensprache können wir Satz 6.6.24 auch so formulieren: Jede Matrix ist – über einem möglicherweise etwas größeren Körper – ähnlich zu einer Matrix in Jordannormalform, welche eindeutig bis auf Vertauschung der Reihenfolge der Blöcke ist.

Bemerkung 6.6.26 (Der Kreis schließt sich)**.** Wir verstehen nun, *warum* die geometrische Vielfachheit eines Eigenwerts durch die algebraische Vielfachheit beschränkt ist: Da der Eigenraum im Hauptraum enthalten ist, ist die Dimension des Eigenraums (= geometrische Vielfachheit) durch die Dimension des Hauptraums (= algebraische Vielfachheit) beschränkt. Wenn die geometrische Vielfachheit gleich der algebraischen ist, dann ist der Hauptraum gleich dem Eigenraum. Das bedeutet aber gerade, dass alle Ketten die Länge 1 (bzw. alle Blöcke die Größe 1) haben, und das ist offensichtlich äquivalent zur Diagonalisierbarkeit.

Zusammenfassung von Abschnitt 6.6

(1) Jeder Endomorphismus zerlegt sich kanonisch in einen nilpotenten und einen invertierbaren Endomorphismus (Fitting-Zerlegung). Diese sind durch die Einschränkung auf den stabilen Kern bzw. das stabile Bild gegeben.

(2) Der Hauptraum eines Endomorphismus Φ zu einem Eigenwert λ ist der stabile Kern von $\Phi - \lambda \cdot \mathrm{Id}$ und enthält insbesondere den Eigenraum (d.h. den Kern von $\Phi - \lambda \cdot \mathrm{Id}$). Seine Dimension ist die algebraische Vielfachheit von λ.

(3) Ist ein Endomorphismus trigonalisierbar, so zerfällt der Vektorraum in die direkte Summe der Haupträume. Daraus folgt, dass Φ eine darstellende Matrix in Jordannormalform besitzt.

(4) Ähnlichkeitsklassen trigonalisierbarer Endomorphismen/Matrizen werden durch Jordan-Daten parametrisiert: Zu jedem Eigenwert benötigt man eine normalisierte Partition der entsprechenden algebraischen Vielfachheit.

[26.04.24]

6.7 Ergänzungen zur Jordan-Theorie

In diesem Abschnitt sei stets $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum mit $n := \dim_{\mathbb{K}}(V) < \infty$ und $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$.

Bemerkung 6.7.1 (Der reelle Fall)**.** Nach Satz 6.6.24 und dem Fundamentalsatz der Algebra sind zwei reelle Matrizen daher genau dann ähnlich, wenn sie dasselbe *komplexe* Jordan-Datum besitzen. Anders gesagt: Für jede reelle Matrix $A \in \mathbb{R}^{n\times n}$ existieren *komplexe* Matrizen $S, J \in \mathbb{C}^{n\times n}$ mit S invertierbar und J in Jordannormalform, so dass $A = SJS^{-1}$, und S ist eindeutig bis auf Vertauschen der Blöcke. Die Ähnlichkeitsklasse jeder reellen Matrix wird also durch eine *komplexe* Matrix in Jordannormalform repräsentiert. Wir wollen uns nun noch überlegen, wie wir einen (möglichst kanonischen) *reellen* Repräsentanten für die Ähnlichkeitsklasse von A finden können. Außerdem wollen wir noch klären, welche Ähnlichkeitsklassen komplexer Matrizen durch reelle Matrizen repräsentiert werden können.

Bemerkung 6.7.2 (Galois-Involution von $\mathbb{C}$ über $\mathbb{R}$)**.** Wir erinnern daran, dass jede komplexe Zahl $z \in \mathbb{C}$ eindeutig geschrieben werden kann als $z = a + bi$ mit $a, b \in \mathbb{R}$, wobei i eine imaginäre Einheit (das Bild von X unter der kanonischen Projektion $\mathbb{R}[X] \to \mathbb{R}[X]/(X^2+1) = \mathbb{C}$) mit $i^2 = -1$ ist. Insbesondere erhalten wir einen Isomorphismus von $\mathbb{R}$-Vektorräumen

$$\mathbb{R}^2 \to \mathbb{C}, \quad \begin{pmatrix} a \\ b \end{pmatrix} \mapsto a + bi.$$

Die reellen Zahlen a und b heißen auch der *Real-* bzw. *Imaginärteil* von z, geschrieben $\mathrm{Re}(z) := a$ und $\mathrm{Im}(z) := b$. Wir definieren die zu $z = a + bi$ *konjugiert-komplexe Zahl* als $\overline{z} := a - bi$. Es gilt dann insbesondere

$$a = \mathrm{Re}(z) = \frac{z+\overline{z}}{2} \quad \text{und} \quad b = \mathrm{Im}(z) = \frac{z-\overline{z}}{2i} = -\frac{z-\overline{z}}{2}i.$$

Unter der Identifikation von $\mathbb{C}$ mit $\mathbb{R}^2$ entspricht die Abbildung

$$\sigma : \mathbb{C} \to \mathbb{C}, \quad z = a + bi \mapsto \overline{z} = a - bi$$

gerade der Spiegelung an der reellen Achse, insbesondere ist σ eine Spiegelung und daher Involution (d.h. $\sigma^2 = \mathrm{Id}$). Die Fixgerade dieser Spiegelung ist gerade $\mathbb{R} \subseteq \mathbb{C}$, d.h. es gilt

$$\mathbb{R} = \mathbb{C}^{\sigma} := \{z \in \mathbb{C} \mid \sigma(z) = z\}. \tag{6.7.1}$$

Das Wichtige an der Involution σ ist nun, dass σ sogar ein Körperautomorphismus ist, d.h. das für alle $w, z \in \mathbb{C}$ gilt (Nachrechnen!):

$$\overline{w+z} = \overline{w} + \overline{z} \quad \text{und} \quad \overline{wz} = \overline{w} \cdot \overline{z}$$

Der Körper $\mathbb{R}$ ist also der Fixkörper des involutorischen Körperautomorphismus σ von $\mathbb{C}$. Dieser heißt auch[13] die *Galois-Involution* der Körpererweiterung $\mathbb{C}$ über $\mathbb{R}$.

[13] Viele Autoren nennen σ auch einfach die *komplexe Konjugation*. Das hat historische Gründe, ist aber etwas unglücklich, weil σ weder komplex-linear noch eine Konjugation in Sinne der Gruppentheorie ist.

Bemerkung 6.7.2 erlaubt weitreichende Verallgemeinerungen, über die Sie mehr in der Vorlesung ALGEBRA lernen können. Ist $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$ und lässt sich $\mathbb{K}$ häufig als Fixpunktmenge einer Gruppe von Körperautomorphismen von $\mathbb{L}$ (der sogenannten *Galois-Gruppe*) schreiben - z.B. wenn $\mathbb{K}$ Charakteristik 0 hat oder wenn $\mathbb{K}$ und $\mathbb{L}$ endlich sind. Im Fall der Körpererweiterung $\mathbb{C}$ von $\mathbb{R}$ ist die Situation besonders einfach, weil die Galoisgruppe von einer einzigen Involution erzeugt wird. Deshalb beschränken wir hier uns auf diesen Spezialfall, aber die Methoden, die wir hier vorführen, funktionieren ganz allgemein, indem man die Galois-Involution durch die Galoisgruppe ersetzt.

Konstruktion 6.7.3 (Galois-Involution auf Vektoren/Matrizen)**.** Die in Bemerkung 6.7.2 definierte Galois-Involution $\sigma : \mathbb{C} \to \mathbb{C}$ induziert eine $\mathbb{R}$-lineare Involution des Vektorraums $\mathbb{C}^n$, die wir ebenfalls mit σ bezeichnen, und die durch

$$\sigma : \mathbb{C}^n \to \mathbb{C}^n, \quad \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \mapsto \begin{pmatrix} \overline{z}_1 \\ \vdots \\ \overline{z}_n \end{pmatrix}$$

gegeben ist. Analog definiert man die Galois-Involution der Matrizenalgebra $\mathbb{C}^{n\times n}$ durch

$$\sigma : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}, \quad (z_{ij}) \mapsto (\overline{z}_{ij}).$$

Man beachte: Alle diese Involutionen sind $\mathbb{R}$-linear, aber nicht $\mathbb{C}$-linear, d.h. man kann reelle, nicht aber komplexe Skalare aus σ herausziehen. Die Galois-Involution von $\mathbb{C}^{n\times n}$ ist sogar ein Automorphismus von $\mathbb{R}$-Algebren. Wiederum gilt die *Fixpunkteigenschaft*

$$\mathbb{R}^n = (\mathbb{C}^n)^\sigma := \{z \in \mathbb{C}^n \mid \sigma(z) = z\} \quad \text{und} \quad \mathbb{R}^{n\times n} = (\mathbb{C}^{n\times n})^\sigma := \{Z \in \mathbb{C}^{n\times n} \mid \sigma(Z) = Z\}.$$

Notation 6.7.4. Ab jetzt sei $A \in \mathbb{R}^{n\times n}$ eine reelle $(n \times n)$-Matrix. Wir definieren $V_{\mathbb{C}} := \mathbb{C}^n$ und $V_{\mathbb{R}} := \mathbb{R}^n = V_{\mathbb{C}}^\sigma$. Dann definiert A zwei lineare Abbildungen

$$\Phi_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}} \quad \text{und} \quad \Phi_{\mathbb{R}} : V_{\mathbb{R}} \to V_{\mathbb{R}},$$

die beide durch die Matrixmultiplikation $v \mapsto Av$ gegeben sind. Man nennt $\Phi_{\mathbb{C}}$ auch die *Komplexifizierung* von $\Phi_{\mathbb{R}}$.

Der $\mathbb{C}$-lineare Endomorphismus $\Phi_{\mathbb{C}}$ ist triagonalisierbar und besitzt daher eine darstellende Matrix in Jordannormalform, aber bei dem $\mathbb{R}$-linearen Endomorphismus $\Phi_{\mathbb{R}}$ ist das möglicherweise nicht der Fall. Wir bezeichnen im Folgenden die Haupt- bzw. Eigenräume von $\Phi_{\mathbb{C}}$ kurz mit $V^\lambda(\Phi_{\mathbb{C}})$ bzw. $V_\lambda(\Phi_{\mathbb{C}})$ (statt $(V_{\mathbb{C}})^\lambda(\Phi_{\mathbb{C}})$ bzw. $(V_{\mathbb{C}})_\lambda(\Phi_{\mathbb{C}})$.

Übung 6.7.5. Zeigen Sie: Ein $\mathbb{C}$-linearer Endomorphismus $\Phi_{\mathbb{C}} : \mathbb{C}^n \to \mathbb{C}^n$ ist genau dann die Komplexifizierung eines $\mathbb{R}$-linearen Endomorphismus $\Phi_{\mathbb{R}} : \mathbb{R}^n \to \mathbb{R}^n$ wenn $\Phi_{\mathbb{C}} \circ \sigma = \sigma \circ \Phi_{\mathbb{C}}$.

Proposition 6.7.6 (Galois-Wirkung auf Spektrum und Eigen-/Haupträumen)**.** *Die Eigenwerte, Eigenräume und Haupträume von $\Phi_{\mathbb{C}}$ haben die folgenden Eigenschaften.*

(i) Ist $\lambda \in \operatorname{spec}(\Phi_{\mathbb{C}})$, so gilt auch $\sigma(\lambda) \in \operatorname{spec}_{\mathbb{C}}(\Phi_{\mathbb{C}})$.

(ii) Ist $\lambda \in \operatorname{spec}_{\mathbb{C}}(\Phi_{\mathbb{C}})$, so ist $\sigma[V_\lambda(\Phi_{\mathbb{C}})] \subseteq V_{\sigma(\lambda)}(\Phi_{\mathbb{C}})$, und σ induziert einen $\mathbb{R}$-linearen (aber nicht $\mathbb{C}$-linearen!) Isomorphismus $\sigma : V_\lambda(\Phi_{\mathbb{C}}) \to V_{\sigma(\lambda)}(\Phi_{\mathbb{C}})$.

(iii) Ist $\lambda \in \operatorname{spec}_{\mathbb{C}}(\Phi_{\mathbb{C}})$, so ist $\sigma[V^\lambda(\Phi_{\mathbb{C}})] \subseteq V^{\sigma(\lambda)}(\Phi_{\mathbb{C}})$, und σ induziert einen $\mathbb{R}$-linearen (aber nicht $\mathbb{C}$-linearen!) Isomorphismus $\sigma : V^\lambda(\Phi_{\mathbb{C}}) \to V^{\sigma(\lambda)}(\Phi_{\mathbb{C}})$.

(iv) Ist $\lambda \in \operatorname{spec}_{\mathbb{R}}(\Phi_{\mathbb{R}}) \subseteq \operatorname{spec}_{\mathbb{C}}(\Phi_{\mathbb{C}})$*, so gilt*

$$V^{\lambda}(\Phi_C)^{\sigma} = V^{\lambda}(\Phi_{\mathbb{R}}).$$

Beweis. Für $\lambda \in \mathbb{C}$ und $v \in V_{\mathbb{C}}$ gilt

$$(\sigma \circ \lambda \cdot \mathrm{Id})(v) = \sigma(\lambda \cdot v) = \overline{\lambda} \cdot \sigma(v),$$

und daher

$$\sigma \circ (\Phi_{\mathbb{C}} - \lambda \cdot \mathrm{Id}) = \sigma \circ \Phi_{\mathbb{C}} - \sigma \circ \lambda \cdot \mathrm{Id} = \Phi_{\mathbb{C}} \circ \sigma - \overline{\lambda} \cdot \mathrm{Id} \circ \sigma = (\Phi_{\mathbb{C}} - \overline{\lambda} \cdot \mathrm{Id}) \circ \sigma.$$

Für $k \in \mathbb{N}$, $\lambda \in \mathbb{C}$ und $v \in V_{\mathbb{C}}$ gelten daher die folgenden Äquivalenzen:

$$\begin{aligned} (\Phi_{\mathbb{C}} - \lambda \cdot \mathrm{Id})^k(v) = 0 \quad &\Longleftrightarrow \quad \sigma((\Phi_{\mathbb{C}} - \lambda \cdot \mathrm{Id})^k(v)) = 0 \\ &\Longleftrightarrow \quad (\Phi_{\mathbb{C}} - \overline{\lambda} \cdot \mathrm{Id})^k(\sigma(v)) = 0. \end{aligned}$$

Dies zeigt insbesondere, dass $v \in V^{\lambda}(\Phi_{\mathbb{C}})$ (bzw. für $k = 1$ auch $v \in V_{\lambda}(\Phi_{\mathbb{C}})$) genau dann gilt, wenn $\sigma(v) \in V^{\sigma(\lambda)}(\Phi_{\mathbb{C}})$ (bzw. $\sigma(v) \in V_{\sigma(\lambda)}(\Phi_{\mathbb{C}})$) ist. Die Aussagen (i)-(iii) folgen nun unmittelbar.

Für (iv) rechnen wir nach, dass für $\lambda \in \mathbb{R}$ die Gleichheit

$$\begin{aligned} V^{\lambda}(\Phi_{\mathbb{C}})^{\sigma} &= \{v \in V_{\mathbb{C}} \mid \sigma(v) = v \text{ und } \exists k \in \mathbb{N} \colon (\Phi_{\mathbb{C}} - \lambda_j \cdot \mathrm{Id})^k(v) = 0\} \\ &= \{v \in V_{\mathbb{R}} \mid \exists k \in \mathbb{N} \colon (\Phi_{\mathbb{R}} - \lambda_j \cdot \mathrm{Id})^k(v) = 0\} \quad = \quad V_{\mathbb{R}}^{\lambda_j}(\Phi_{\mathbb{R}}). \end{aligned}$$

gilt. □

Bemerkung 6.7.7. Ist $\lambda \in \operatorname{spec}(\Phi_{\mathbb{C}})$, so gibt es nach Proposition 6.7.6 zwei Möglichkeiten: Entweder, λ ist reell, und daher $\overline{\lambda} = \lambda$, oder λ ist nicht-reell, und daher sind λ und $\overline{\lambda}$ zwei verschiedene, zueinander konjugierte nicht-reelle Eigenwerte von $\Phi_{\mathbb{C}}$.

Ab jetzt seien $\lambda_1, \ldots, \lambda_r$ die verschiedenen reellen Eigenwerte von $\Phi_{\mathbb{C}}$ und es seien $\mu_1, \overline{\mu_1}, \ldots, \mu_s, \overline{\mu}_s$ die verschiedenen nicht-reellen Eigenwerte von $\Phi_{\mathbb{C}}$ (nach Paaren geordnet).

Aufgrund der komplexen Hauptraumzerlegung (Korollar 6.6.16) gilt

$$V_{\mathbb{C}} = V^{\lambda_1}(\Phi_{\mathbb{C}}) \oplus \cdots \oplus V^{\lambda_r}(\Phi_{\mathbb{C}}) \oplus \left(V^{\mu_1}(\Phi_{\mathbb{C}}) \oplus V^{\overline{\mu_1}}(\Phi_{\mathbb{C}})\right) \oplus \cdots \oplus \left(V^{\mu_s}(\Phi_{\mathbb{C}}) \oplus V^{\overline{\mu_s}}(\Phi_{\mathbb{C}})\right), \tag{6.7.2}$$

und nach Proposition 6.7.6 ist dies ist eine Zerlegung von $V_{\mathbb{C}}$ in *σ-invariante komplexe Unterräume*.

Lemma 6.7.8 (Reelle Formen)**.** *Sei $W_{\mathbb{C}} \subseteq \mathbb{C}^n$ ein σ-invarianter komplexer Untervektorraum. Dann ist*

$$W_{\mathbb{C}}^{\sigma} := \{w \in W_{\mathbb{C}} \mid \sigma(w) = w\} = W_{\mathbb{C}} \cap \mathbb{R}^n$$

ein reeller Untervektorraum von $\mathbb{R}^n$ mit $\dim_{\mathbb{C}} W_{\mathbb{C}} = \dim_{\mathbb{R}} W_{\mathbb{R}}$.

Beweis. Die Gleichheit $W_{\mathbb{C}}^{\sigma} = W_{\mathbb{C}} \cap \mathbb{R}^n$ folgt aus (6.7.1). Da $\sigma : W_{\mathbb{C}} \to W_{\mathbb{C}}$ eine $\mathbb{R}$-lineare Involution ist, ist nach Beispiel 6.2.15 $W_{\mathbb{C}}$ die direkte Summe der Eigenräume von σ zu den Eigenwerten 1 und -1. Der Eigenraum zum Eigenwert 1 ist gerade $W_{\mathbb{C}}^{\sigma}$, und der Eigenraum zum Eigenwert -1 ist $W' := \{w \in W_{\mathbb{C}} \mid \sigma(w) = -w\}$, folglich gilt

$$\dim_{\mathbb{R}} W_{\mathbb{C}}^{\sigma} + \dim_{\mathbb{R}} W' = \dim_{\mathbb{R}} W_{\mathbb{C}} = 2 \cdot \dim_{\mathbb{C}} W_{\mathbb{C}}.$$

Für $w \in W_{\mathbb{C}}$ gilt aber $\sigma(iw) = \sigma(i)\sigma(w) = -i\sigma(w)$. Daraus folgt, dass

$$w \in W_{\mathbb{C}}^{\sigma} \iff \sigma(w) = w \iff \sigma(iw) = -iw \iff iw \in W',$$

also definiert $\Psi : W_{\mathbb{C}}^{\sigma} \to W'$, $w \to iw$ einen $\mathbb{R}$-linearen Isomorphismus (mit Inversem $w \mapsto -iw$). Insbesondere gilt

$$2\dim_{\mathbb{C}} W_{\mathbb{C}} = \dim_{\mathbb{R}} W_{\mathbb{C}}^{\sigma} + \dim_{\mathbb{R}} W' = 2\dim_{\mathbb{R}} W_{\mathbb{C}}^{\sigma}. \qquad \square$$

Korollar 6.7.9. *Ist $\mathbb{C}^n = \bigoplus_{j=1}^{k} W_{\mathbb{C},k}$ eine Zerlegung in σ-invariante komplexe Unterräume, so gilt*

$$\mathbb{R}^n = \bigoplus_{j=1}^{k} W_{\mathbb{R},k}, \quad \textit{wobei} \quad W_{\mathbb{R},k} := W_{\mathbb{C},k}^{\sigma}.$$

Beweis. Nach Proposition 6.7.8 ist die direkte Summe auf der rechten Seite ein Untervektorraum von $\mathbb{R}^n$ der reellen Dimension n, also bereits der ganze $\mathbb{R}^n$. $\square$

Konstruktion 6.7.10 (Reelle Jordanbasis)**.** Aus Proposition 6.7.6.(iv), Korollar 6.7.9 und (6.7.2) erhalten wir die folgende Zerlegung von $V_{\mathbb{R}}$ in $\Phi_{\mathbb{R}}$-invariante reelle Vektorräume:

$$V_{\mathbb{R}} = V_{\mathbb{R}}^{\lambda_1}(\Phi_{\mathbb{R}}) \oplus \cdots \oplus V_{\mathbb{R}}^{\lambda_r}(\Phi_{\mathbb{R}}) \oplus \left(V_{\mathbb{C}}^{\mu_1}(\Phi_{\mathbb{C}}) \oplus V_{\mathbb{C}}^{\overline{\mu_1}}(\Phi_{\mathbb{C}})\right)^{\sigma} \oplus \cdots \oplus \left(V_{\mathbb{C}}^{\mu_s}(\Phi_{\mathbb{C}}) \oplus V_{\mathbb{C}}^{\overline{\mu_s}}(\Phi_{\mathbb{C}})\right)^{\sigma}. \tag{6.7.3}$$

Mit Proposition 6.7.6.(iii) und Lemma 6.7.8 folgt, dass

$$\dim_{\mathbb{R}} \left(V^{\mu_1}(\Phi_{\mathbb{C}}) \oplus V^{\overline{\mu_1}}(\Phi_{\mathbb{C}})\right)^{\sigma} = 2\dim_{\mathbb{C}} V^{\mu_j}(\Phi_{\mathbb{C}}). \tag{6.7.4}$$

Wir finden nun wie folgt Basen für diese invarianten Vektorräume:

(i) Sei $j \in \{1,\dots,r\}$. Für $V_{\mathbb{R}}^{\lambda_j}(\Phi_{\mathbb{R}})$ wählen wir eine Kettenbasis für den nilpotenten Endomorphismus $(\Phi_{\mathbb{R}})_{\lambda_j}$. Wir ordnen diese Basis wieder so an, das jede Kette rückwärts durchlaufen wird; dann istdie zugehörige darstellende Matrix von $(\Phi_{\mathbb{R}})_{V_{\mathbb{R}}^{\lambda_j}}$ in oberer Jordannormalform ist.

(ii) Nun sei $k \in \{1,\dots,s\}$. Wir betrachten den nilpotenten Endomorphismus $\Psi_k := \Phi_{\mathbb{C}} - \mu_k \cdot \mathrm{Id}$ von $V_{\mathbb{C}}^{\mu_k}(\Phi_{\mathbb{C}})$, und wählen dazu eine (komplexe) Kettenbasis $(v_1,\dots,v_d)$ (wobei wir Ketten wieder rückwärts durchlaufen). Für $m \in \{1,\dots,d\}$ definieren wir

$$u_m := \mathrm{Re}(v_m) = \frac{v_m + \overline{v_m}}{2} \quad \text{und} \quad w_m := \mathrm{Im}(v_m) = \frac{v_m - \overline{v_m}}{2i}.$$

Wegen wegen $\overline{v_m} \in V^{\overline{\mu}_k}(\Phi_{\mathbb{C}})$ gilt $u_1, w_1, \dots, u_d, w_d \in V^{\mu_k}(\Phi_{\mathbb{C}}) \oplus V^{\overline{\mu}_k}$. Nun rechnet man nach, dass $\sigma(u_m) = u_m$ und $\sigma(w_m) = w_m$, also folgt

$$u_1, w_1, \dots, u_d, w_d \in \left(V^{\mu_k}(\Phi_{\mathbb{C}}) \oplus V^{\overline{\mu}_k}(\Phi_{\mathbb{C}})\right)^{\sigma} \subseteq V_{\mathbb{R}}.$$

Wir behaupten, dass $(u_1, w_1, \dots, u_d, w_d)$ eine Basis dieses $\mathbb{R}$-Vektorraums ist. Aus Dimensionsgründen genügt es zu zeigen, dass die Vektoren linear unabhängig sind. Seien also $a_m, b_m \in \mathbb{R}$ mit

$$0 = \sum_{m=1}^{d} a_m u_m + b_m w_m = \sum_{m=1}^{d} a_m \frac{v_m + \overline{v_m}}{2} + b_m \frac{v_m - \overline{v_m}}{2i} = \sum_{m=1}^{d} \left(\frac{a_m}{2} + \frac{b_m}{2i}\right) v_m + \sum_{m=1}^{d} \left(\frac{a_m}{2} - \frac{b_m}{2i}\right) \overline{v_m}.$$

Es gilt dann

$$\sum_{m=1}^{d}\left(\frac{a_m}{2}+\frac{b_m}{2i}\right)v_m = -\sum_{m=1}^{d}\left(\frac{a_m}{2}-\frac{b_m}{2i}\right)\overline{v_m} \in V^{\mu_k}(\Phi_{\mathbb{C}})\cap V^{\overline{\mu}_k}(\Phi_{\mathbb{C}}) = \{0\},$$

und da $v_1,\dots,v_d$ linear unabhängig über $\mathbb{C}$ sind, erhält man

$$a_m - ib_m = 2\cdot\left(\frac{a_m}{2}+\frac{b_m}{2i}\right) = 0 \quad \text{für alle } m\in\{1,\dots,d\},$$

und daher $a_1=\dots=a_d=b_1=\dots=b_d=0$. Wir haben also ausgehend von einer Kettenbasis $(v_1,\dots,v_d)$ von $V^{\mu_k}(\Phi_{\mathbb{C}})$ durch Übergang zu Real- und Imaginärteil eine Basis $(u_1,w_1,\dots,u_d,w_d)$ für $\left(V^{\mu_k}(\Phi_{\mathbb{C}})\oplus V^{\overline{\mu}_k}(\Phi_{\mathbb{C}})\right)^{\sigma}$ gefunden.

Wir nennen eine Basis von $V_{\mathbb{R}}$, die sich aus den obigen Basen für die einzelnen Summanden zusammensetzt eine *reelle Jordanbasis* von $V_{\mathbb{R}}$ bzgl. Φ.

Bemerkung 6.7.11 (Reelle Jordannormalform)**.** Wie sieht nun die darstellende Matrix von Φ bzgl. einer reellen Jordanbasis aus? Die Blöcke, die zu reellen Eigenwerten gehören, zerfallen in gewöhnliche Jordan-Blöcke, die wiederum Ketten entsprechen.

Interessanter ist der Fall eines nicht-reellen Eigenwerts μ. Nehmen wir zuerst an, dass $\Psi := \Phi_{\mathbb{C}}-\mu\cdot\mathrm{Id}$ auf dem Hauptraum $V^{\mu}(\Phi_{\mathbb{C}})$ eine Basis $(v_1,\dots,v_l)$ besitzt, die nur aus einer einzigen Ψ-Kette (in umgekehrter Reihenfolge) besteht. Diese bedeutet gerade, dass

$$\Phi_{\mathbb{C}}(v_1)=\mu v_1 \quad\text{und}\quad \Phi_{\mathbb{C}}(v_j)=\mu v_j+v_{j-1} \quad (j\in\{2,\dots,l\}).$$

Die zugehörige reelle Basis von $(V^{\mu}(\Phi_{\mathbb{C}})\oplus V^{\overline{\mu}}(\Phi_{\mathbb{C}}))^{\sigma}$ ist dann gegeben durch

$$(u_1,w_1,\dots,u_l,w_l)=\left(\frac{v_1+\overline{v_1}}{2},\frac{v_1-\overline{v_1}}{2i},\dots,\frac{v_l+\overline{v_l}}{2},\frac{v_l-\overline{v_l}}{2i},\right).$$

Ist nun $\mu=a+bi$ mit $a,b\in\mathbb{R}$, so gelten für $j\in\{1,\dots,l\}$ die Identitäten

$$\begin{aligned}\Phi_{\mathbb{R}}(u_j) &= \Phi_{\mathbb{C}}(u_j) = \Phi_{\mathbb{C}}\left(\frac{v_j+\overline{v_j}}{2}\right) = \frac{\Phi_{\mathbb{C}}(v_j)+\overline{\Phi_{\mathbb{C}}(v_j)}}{2}\\ &= \frac{\mu v_j+v_{j-1}+\overline{\mu}\,\overline{v_j}+\overline{v_{j-1}}}{2} = \frac{v_{j-1}+\overline{v_{j-1}}}{2}+a\frac{v_j+\overline{v_j}}{2}+ib\frac{v_j-\overline{v_j}}{2}\\ &= u_{j-1}+au_j-bw_j,\end{aligned}$$

und analog (Übung!)

$$\Phi_{\mathbb{R}}(w_j)=w_{j-1}+bu_j+aw_j.$$

Das bedeutet aber gerade, dass die darstellende Matrix der Einschränkung von Φ auf den Unterraum $\left(V^{\mu_k}(\Phi_{\mathbb{C}})\oplus V^{\overline{\mu}_k}(\Phi_{\mathbb{C}})\right)^{\sigma}$ bzgl. der Basis $(u_1,w_1,\dots,u_l,w_l)$ gegeben ist durch

$$\begin{pmatrix} a & b & 1 & 0 & & & & 0\\ -b & a & 0 & 1 & & & & \\ & & a & b & 1 & 0 & & \\ & & -b & a & 0 & 1 & & \\ & & & & \ddots & & \ddots & \\ & & & & & a & b & 1 & 0\\ & & & & & -b & a & 0 & 1\\ & & & & & & & a & b\\ 0 & & & & & & & -b & a \end{pmatrix}.$$

Einen solchen Block bezeichnet man als *verallgemeinerten reellen Jordanblock*, und eine reelle Matrix in Blockdiagonalform, deren Blöcke entweder Jordanblöcke oder verallgemeinerte reelle Jordanblöcke sind, bezeichnet man als Matrix in *reeller Jordannormalform*. Falls Ψ wie hier angenommen eine Ketten-Basis mit nur einer Kette der Länge l besitzt, ist die entsprechende darstellende Matrix ein verallgemeinerter reeller Jordan-Block der Größe $2l$. Im Falle mehrerer Ketten besteht die darstellende Matrix entsprechend aus mehreren solcher Blöcke.

Insgesamt haben wir gezeigt:

Satz 6.7.12 (Reelle Jordannormalform)**.** *Jede reelle Matrix ist ähnlich zu einer Matrix in reeller Jordannormalform.* □

Die Blockgrößen in der Jordannormalform entsprechen wieder Kettenlängen. Im Fall von reellen Eigenwerten entspricht ein Jordan-Block der Größe l einer Kette der Länge l, und im Fall nicht-reeller Eigenwerte entspricht ein verallgemeinerter reeller Jordanblock der Größe $2l$ einer Kette der Länge l. Wir halten noch einen wichtigen Spezialfall fest, nämlich den Fall, in dem alle Ketten die Länge 1 haben:

Korollar 6.7.13. *Ist eine Matrix $A \in \mathbb{R}^{n\times n}$ diagonalisierbar über $\mathbb{C}$, so ist sie (über $\mathbb{R}$) ähnlich zu einer Blockdiagonalmatrix bestehend aus (2×2)-Blöcken der Form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ mit $a,b \in \mathbb{R}$ und (1×1)-Blöcken.* □

Bemerkung 6.7.14 (Ähnlichkeitsklassen reeller Matrizen)**.** In Analogie zum komplexen Fall, könnte man vermuten dass es in jeder Ähnlichkeitsklasse reeller Matrizen bis auf Reihenfolge der Blöcke genau eine Matrix in reeller Jordannormalform gibt. Dies ist aber **falsch**. Das Problem besteht darin, dass wir aus jedem Paar nicht-reeller Eigenwerte einen ausgewählt und μ genannt haben - wir hätten aber genauso gut mit $\overline{\mu}$ arbeiten können. Diese unterschiedlichen Wahlen führen zu unterschielden Vorzeichen auf der Nebendiagonalen:

$$\mu \rightsquigarrow \begin{pmatrix} \mathrm{Re}(\mu) & \mathrm{Im}(\mu) \\ -\mathrm{Im}(\mu) & \mathrm{Re}(\mu) \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{und} \quad \overline{\mu} \rightsquigarrow \begin{pmatrix} \mathrm{Re}(\overline{\mu}) & \mathrm{Im}(\overline{\mu}) \\ -\mathrm{Im}(\overline{\mu}) & \mathrm{Re}(\overline{\mu}) \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Die Ähnlichkeitsklasse einer Matrix in reeller Jordannormalform ändert sich also nicht, wenn man in den Diagonalblöcken zu den nicht-reellen Eigenwerten die Vorzeichen der beiden Nebendiagonaleinträge vertauscht. Das ist aber dann auch die einzige zusätzliche Uneindeutigkeit der reellen Jordannormalform, wie man durch Vergleich der entsprechenden komplexen Jordan-Daten leicht sieht.

An dieser Stelle haben wir reelle Matrizen bis auf Ähnlichkeit vollständig klassifiziert. Formuliert man das ganze nun noch in der Sprache der Endomorphismen um, so erhält man den folgenden Satz:

Satz 6.7.15 (Normalformenproblem für reelle Endomorphismen)**.** *Seien Φ und Ψ Endomorphismen eines endlichdimensionalen $\mathbb{R}$-Vektorraums. Dann sind die folgenden Aussagen äquivalent:*

(i) *Φ und Ψ sind ähnlich zueinader.*

(ii) *Φ und Ψ haben darstellende Matrizen in reeller Jordannormalform, die durch Vertauschen der Blöcke und ggf. Vertauschen der Vorzeichen der beiden Nebendiagonaleinträge in den Diagonalblöcken zu den nicht-reellen Eigenwerten auseinander hervorgehen.*

Prinzipiell ist das praktische Berechnen reeller Jordannormalformen nicht schwieriger als das Berechnen komplexer Jordannormalformen. Um allerdings überhaupt mindestens eine Kette der Länge ≥ 1 zu sehen, die zu einem nicht-reellen Eigenwert gehört, muss die Matrix mindestens Größe 4×4 besitzen, und daher werden die Rechnungen häufig unhandlich. Wir begnügen uns daher mit einem Minimalbeispiel.

Beispiel 6.7.16. Wir bestimmen die komplexe und reelle Jordannormalform der Matrix

$$A := \begin{pmatrix} 1 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ -2 & -1 & -1 & -1 \end{pmatrix} \in \mathbb{R}^{4\times 4} \subseteq \mathbb{C}^{4\times 4}.$$

Es seien $\Phi_{\mathbb{C}} : \mathbb{C}^4 \to \mathbb{C}^4$ und $\Phi_{\mathbb{R}} : \mathbb{R}^4 \to \mathbb{R}^4$ die zugehörigen Endomorphismen. Das charakteristische Polynom von A ist dann gegeben durch

$$\begin{aligned}
\chi_A(X) &= \det\begin{pmatrix} X-1 & -1 & 0 & 0 \\ 2 & X & -1 & 0 \\ -2 & 0 & X & -1 \\ 2 & 1 & 1 & X+1 \end{pmatrix} = (X-1)\cdot\det\begin{pmatrix} X & -1 & 0 \\ 0 & X & -1 \\ 1 & 1 & X+1 \end{pmatrix} + 1\cdot\det\begin{pmatrix} 2 & -1 & 0 \\ -2 & X & -1 \\ 2 & 1 & X+1 \end{pmatrix} \\
&= (X-1)\cdot X\cdot\det\begin{pmatrix} X & -1 \\ 1 & X+1 \end{pmatrix} + (X-1)\cdot\det\begin{pmatrix} -1 & 0 \\ X & -1 \end{pmatrix} + 2\cdot\det\begin{pmatrix} X & -1 \\ 1 & X+1 \end{pmatrix} - (-1)\cdot\det\begin{pmatrix} -2 & -1 \\ 2 & X+1 \end{pmatrix} \\
&= (X^2-X)(X^2+X+1) + (X-1) + 2(X^2+X+1) + (-2X) \\
&= X^4+X^3+X^2-X^3-X^2-X+X-1+2X^2+2X+2-2X \\
&= X^4+2X^2+1 = (X^2+1)^2 = (X-i)^2(X+i)^2.
\end{aligned}$$

Die Matrix A hat also zwei nicht-reelle Eigenwerte i und $-i$, und diese sind zueinander konjugiert. Betrachten wir nun zuerst den komplexen Hauptraum von $\Phi_{\mathbb{C}}$ zum Eigenwert i. Seine Dimension ist gegeben durch die algebraische Vielfachheit von i, also 2. Nun ist[14]

$$\begin{aligned}
\ker(i\cdot\mathrm{Id}-\Phi) &= \ker\begin{pmatrix} i-1 & -1 & 0 & 0 \\ 2 & i & -1 & 0 \\ -2 & 0 & i & -1 \\ 2 & 1 & 1 & i+1 \end{pmatrix} = \ker\begin{pmatrix} -2 & -i-1 & 0 & 0 \\ 2 & i & -1 & 0 \\ -2 & 0 & i & -1 \\ 2 & 1 & 1 & i+1 \end{pmatrix} \\
&= \ker\begin{pmatrix} -2 & -i-1 & 0 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & i+1 & i & -1 \\ 0 & -i & 1 & i+1 \end{pmatrix} = \ker\begin{pmatrix} -2 & -i-1 & 0 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & i+1 & i+1 \end{pmatrix} \\
&= \ker\begin{pmatrix} 2 & i+1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \ker\begin{pmatrix} 2 & 0 & 0 & i+1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\
&= \left\langle \begin{pmatrix} -i-1 \\ 2 \\ -2 \\ 2 \end{pmatrix} \right\rangle
\end{aligned}$$

[14] **Hinweis zu Zeilenumformungen für komplexe Matrizen:** Wenn man einen Eintrag der Form $(a+bi)$ vereinfachen möchte, kann man die entsprechende Zeile mit $(a-bi)$ multiplizieren. Der neue Eintrag ist dann a^2+b^2, also reell. Der Preis, den man bezahlt, ist, dass ggf. andere Einträge in der Zeile komplizierter werden.

eindimensional, also noch nicht der gesamte Hauptraum. Wir rechnen also weiter:

$$\begin{aligned}
\ker(i\cdot\mathrm{Id}-\Phi)^2 &= \ker\begin{pmatrix} i-1 & -1 & 0 & 0\\ 2 & i & -1 & 0\\ -2 & 0 & i & -1\\ 2 & 1 & 1 & i+1\end{pmatrix}^2 = \ker\begin{pmatrix} -2-2i & 1-2i & 1 & 0\\ 4i & -3 & -2i & 1\\ -4i & 1 & -2 & -1-2i\\ 4i & -1+2i & 2i & -1+2i\end{pmatrix}\\
&= \ker\begin{pmatrix} 4 & 1+3i & -1+i & 0\\ 4i & -3 & -2i & 1\\ -4i & 1 & -2 & -1-2i\\ 4i & -1+2i & 2i & -1+2i\end{pmatrix} = \ker\begin{pmatrix} 4 & 1+3i & -1+i & 0\\ 0 & -i & 1-i & 1\\ 0 & -2+i & -3-i & -1-2i\\ 0 & 2+i & 1+3i & -1+2i\end{pmatrix}\\
&= \ker\begin{pmatrix} 4 & 1+3i & -1+i & 0\\ 0 & 1 & 1+i & i\\ 0 & 5 & 5+5i & 5i\\ 0 & 5 & 5+5i & 5i\end{pmatrix} = \ker\begin{pmatrix} 4 & 0 & 1-3i & 3-i\\ 0 & 1 & 1+i & i\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}\\
&= \left\langle \begin{pmatrix} -3+i\\ -4i\\ 0\\ 4\end{pmatrix}, \begin{pmatrix} -1+3i\\ -4-4i\\ 4\\ 0\end{pmatrix}\right\rangle.
\end{aligned}$$

Damit haben wir den Hauptraum $V^i(\Phi_{\mathbb{C}})$ gefunden. Wir betrachten nun den nilpotenten Endomorphismus

$$\Psi := (\Phi_{\mathbb{C}} - i\cdot\mathrm{Id})|_{V^i(\Phi_{\mathbb{C}})}.$$

Seine kanonische Fahne ist gegeben durch

$$\{0\} \subseteq \left\langle \begin{pmatrix} -i-1\\ 2\\ -2\\ 2\end{pmatrix}\right\rangle \subseteq \left\langle \begin{pmatrix} -3+i\\ -4i\\ 0\\ 4\end{pmatrix}, \begin{pmatrix} -1+3i\\ -4-4i\\ 4\\ 0\end{pmatrix}\right\rangle = V^i(\Phi_{\mathbb{C}}),$$

und folglich hat Ψ eine Kettenbasis bestehend aus einer Kette der Länge 1. Wir können z.B. die folgende Kettenbasis (v_1, v_2) wählen:

$$v_2 := \begin{pmatrix} -3+i\\ -4i\\ 0\\ 4\end{pmatrix} \Longrightarrow v_1 := \Psi(v_2) = \begin{pmatrix} -i+1 & 1 & 0 & 0\\ -2 & -i & 1 & 0\\ 2 & 0 & -i & 1\\ -2 & -1 & -1 & -i-1\end{pmatrix}\begin{pmatrix} -3+i\\ -4i\\ 0\\ 4\end{pmatrix} = \begin{pmatrix} -2\\ 2-2i\\ -2+2i\\ 2-2i\end{pmatrix}.$$

Bzgl. der geordneten Basis (v_1, v_2) von $V^i(\Phi_{\mathbb{C}})$ hat nun $\Phi_{\mathbb{C}}|_{V^i(\Phi_{\mathbb{C}})}$ die darstellende Matrix $\begin{pmatrix} i & 1\\ 0 & i\end{pmatrix}$.

Ein wichtiger Trick ist nun der Folgende: Da die Matrix A reell ist, besteht der Hauptraum $V^{-i}(\Phi_{\mathbb{C}})$ nun gerade aus den Vektoren, die zu denen aus $V^i(\Phi_{\mathbb{C}})$ konjugiert sind. Wir müssen also nicht nochmal rechnen, sondern erhalten gratis, dass $(\overline{v_1}, \overline{v_2})$ eine Kettenbasis ist. Mit anderen Worten, $\Phi_{\mathbb{C}}$ ist in komplexer Jordannormalform bzgl. der Basis $(v_1, v_2, \overline{v_1}, \overline{v_2})$ und es gilt

$$\begin{pmatrix} 1 & 1 & 0 & 0\\ -2 & 0 & 1 & 0\\ 2 & 0 & 0 & 1\\ -2 & -1 & -1 & -1\end{pmatrix} = \begin{pmatrix} -2 & -3+i & -2 & -3-i\\ 2-2i & -4i & 2+2i & 4i\\ -2+2i & 0 & -2-2i & 0\\ 2-2i & 4 & 2+2i & 4\end{pmatrix}\begin{pmatrix} i & 1 & 0 & 0\\ 0 & i & 0 & 0\\ 0 & 0 & -i & 1\\ 0 & 0 & 0 & -i\end{pmatrix}\begin{pmatrix} -2 & -3+i & -2 & -3-i\\ 2-2i & -4i & 2+2i & 4i\\ -2+2i & 0 & -2-2i & 0\\ 2-2i & 4 & 2+2i & 4\end{pmatrix}^{-1}.$$

Damit haben wir die komplexe Jordannormalform sowie den zugehörigen Basiswechsel gefunden. Die reelle Jordannormalform können wir nun ebenfalls direkt ablesen: Eine reelle Jordanbasis ist gegeben durch $(\mathrm{Re}(v_1), \mathrm{Im}(v_1), \mathrm{Re}(v_2), \mathrm{Im}(v_2))$, und wegen $i = 0 + 1 \cdot i$ erhalten wir

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

Wir haben also die reelle Jordannormalform und den zugehörigen Basiswechsel bestimmt.

Mit der gezeigten Methode lässt sich das Normalformenproblem über vielen Körpern lösen. Zu einer gegebenen Matrix A über einem Körper $\mathbb{K}$ findet man zunächst eine endliche Körpererweiterung $\mathbb{L}$, über der das charakteristische Polynom zerfällt. Die Eigenwerte von A in $\mathbb{L}$ kommen dann immer paketweise - im Fall von $\mathbb{R}$ und $\mathbb{C}$ gab es immer Zweierpakete, gegeben durch die Bahnen der komplexen Konjugation. Im Allgemeinen sind die Pakete größer und entsprechen Bahnen der Galois-Gruppe. Nimmt man nun alle Haupträume in $\mathbb{L}^n$ zu einem Paket von Eigenwerten zusammen, und schneidet deren direkte Summe mit $\mathbb{K}^n$, so erhält man einen A-invarianten Unterraum in $\mathbb{K}^n$, den man dann - ähnlich wie oben im reellen Fall vorgeführt - durch sogenannten Galois-Abstieg behandeln kann.

Bemerkung 6.7.17 (Historische Bemerkung)**.** Die klassische Theorie der Jordannormalform erfuhr in der zweiten Hälfte des 20. Jahrhunderts eine wesentliche Umformulierung zu einer Theorie der Zerlegbarkeit von Matrizen in einfachere Bausteine. Die moderne Theorie der Matrix-Gruppen („lineare algebraische Gruppen“) beruht ganz wesentlich auf dieser Interpretation. Wir werden nun die Grundlagen dieser modernen Sichtweise auf die klassische Jordansche Theorie kurz erkären. Die Sonderrolle, die einerseits diagonalisierbare und andererseits nilpotente Matrizen spielen, wird in der modernen Formulierung besonders klar.

Definition 6.7.18. Ein Paar (Φ_d, Φ_n) von Endomorphismen von V heißt eine *(additive) Jordan–Chevalley*[15]*–Zerlegung* von Φ, falls gilt:

(JC1) $\Phi = \Phi_d + \Phi_n$.

(JC2) Φ_d ist diagonalisierbar und Φ_n ist nilpotent.

(JC3) $\Phi_d \circ \Phi_n = \Phi_n \circ \Phi_d$.

Analog definiert man eine (additive) Jordan–Chevalley-Zerlegung (A_d, A_n) einer Matrix A.

Beispiel 6.7.19. Wir schauen uns einige Beispiele für Jordan–Chevalley-Zerlegungen an:

(i) Es gilt $J_+[(n)_\lambda] = \mathrm{diag}(\lambda, \ldots, \lambda) + J_+[n]$, wobei der erste Summand offensichtlich diagonalisierbar und der zweite Summand nilpotent ist. Da $\mathrm{diag}(\lambda, \ldots \lambda)$ mit beliebigen Matrizen vertauscht, ist dies bereits eine Jordan–Chevalley-Zerlegung des Blocks $J_+[(n)_\lambda]$.

(ii) Ist J eine Matrix in Jordannormalform, so können wir jeden seiner Jordanblöcke wie in (i) zerlegen. Auf diese Weise erhalten wir dann wieder eine Diagonalmatrix D (im Allgemeinen kein Vielfaches der Identität mehr) und eine nilpotente Matrix N mit $J = D + N$ und

[15] Claude Chevalley (1909-1984), frz. Mathematiker, einer der Väter der modernen Theorie der Matrix-Gruppen („lineare algebraische Gruppen“)

$D \cdot N = N \cdot D$, wobei die Vertauschbarkeit von D und N aus der blockweisen Vertauschbarkeit folgt. Zum Beispiel gilt

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

(iii) Es sei nun $A \in \mathbb{K}^{n\times n}$ eine trigonalisierbare Matrix. Dann existiert eine Matrix $S \in \mathrm{GL}_n(\mathbb{K})$ und eine Matrix $J \in \mathbb{K}^{n\times n}$ in Jordannormalform, so dass $A = SJS^{-1}$. Die Matrix J können wir dann wieder schreiben als $J = D + N$ mit D diagonal, N nilpotent und $DN = ND$. Wir definieren dann $A_d := SDS^{-1}$ und $A_n := SNS^{-1}$. Es gilt dann: A_d ist diagonalisierbar, A_n ist nilpotent (denn $A_n^k = SN^kS^{-1} = 0$ für hinreichende große k), $A = A_d + A_n$ und

$$A_dA_n = SDS^{-1}SNS^{-1} = SDNS^{-1} = SNDS^{-1} = SNS^{-1}SDS^{-1} = A_nA_d.$$

Damit haben wir den folgenden Satz bewiesen:

Proposition 6.7.20. *Jeder trigonalisierbare Endomorphismus und jede trigonalisierbare Matrix besitzen eine (additive) Jordan–Chevalley-Zerlegung.*

Bemerkung 6.7.21 (Potenzrechnung mittels Jordan–Chevalley-Zerlegung)**.** In *kommutativen* $\mathbb{K}$-Algebren gilt (mit dem aus den reellen Zahlen bekannten Beweis) die binomische Formel

$$(A+B)^m = \sum_{k=0}^{m} \binom{m}{k} A^k B^{m-k}.$$

Für allgemeine Matrizen A und B gilt diese Formel ausdrücklich nicht, z.B. gilt für Matrizen mit $AB \neq BA$ stets

$$(A+B)^2 = A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2.$$

Sie gilt aber sehr wohl für miteinander vertauschende Matrizen. Ist daher A eine Matrix mit additiver Jordan–Chevalley Zerlegung $A = A_d + A_n$, so gilt

$$A^m = (A_d + A_n)^m = (A_n + A_d)^m = \sum_{k=0}^{m} \binom{m}{k} A_n^k A_d^{m-k}$$

Die Potenzen einer Diagonalmatrix lassen sich sehr leicht berechnen, und mittels Diagonalisierung berechnet man auch die Potenzen von A_d relativ leicht. Die Potenzen von A_n wiederum sind für hinreichend große Exponenten schlicht 0. Dies erlaubt eine effiziente Berechnung von Matrixpotenzen.

[03.05.24]

Für die moderne Theorie der Jordan–Chevalley-Zerlegung ist das folgende Lemma entscheidend:

Lemma 6.7.22 (Lemma von Chevalley)**.** *Ist $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ trigonalisierbar, so existieren Polynome $p, q \in \mathbb{K}[X]$ ohne konstanten Term, so dass $\Phi_d := p(\Phi)$ und $\Phi_n := q(\Phi)$ eine additive Jordan–Chevalley-Zerlegung von Φ bilden.*

Der Beweis des Lemmas geht über die Methoden dieser Vorlesung hinaus. Mit den Methoden, die Sie im 4. Semester in der EINFÜHRUNG IN ALGEBRA UND ZAHLENTHEORIE lernen werden, ist der Beweis nicht schwierig. Auch wenn Sie den Beweis von Lemma 6.7.22 erst zu einem späteren Zeitpunkt verstehen können, so ist es doch wichtig, die moderne Formulierung der Jordanschen Theorie zu kennen.

Für die Neugierigen unter Ihnen skizzieren wir den Beweis im Kleingedruckten. Aus der EINFÜHRUNG IN ALGEBRA UND ZAHLENTHEORIE benötigen wir das folgende Hilfsmittel:

Lemma 6.7.23 (Chinesischer Restsatz für Polynome)**.** *Seien $\chi_1, \dots, \chi_k \in \mathbb{K}[X]$ paarweise teilerfremde Polynome. Dann existiert für alle $q_1, \dots, q_k \in \mathbb{K}[X]$ ein Polynom $p \in \mathbb{K}[X]$, das für alle $j \in \{1, \dots, k\}$ bei Division durch χ_j denselben Rest lässt wie q_j.* □

Damit folgt nun leicht das gewünschte Lemma.

Beweis von Lemma 6.7.22. Es seien $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von Φ. Weiter sei $\chi_\Phi(X) = (X-\lambda_1)^{e_1} \cdots (X-\lambda_k)^{e_k}$ und es sei $V = V^{\lambda_1} \oplus \cdots \oplus V^{\lambda_k}$ die zugehörige Hauptraumzerlegung. Definieren wir $\chi_j := (X-\lambda_j)^{e_j}$, so sind die Polynome $\chi_1, \dots, \chi_k$ paarweise teilerfremd. Nach dem Chinesischen Restsatz existiert daher ein Polynom $p \in \mathbb{K}[X]$ mit

$$p(X) \in \lambda_j + (\chi_j) \text{ für } j \in \{1, \dots, k\}. \tag{6.7.5}$$

Falls 0 nicht ohnehin ein Eigenwert ist, können wir zusätzlich verlangen, dass $p(X)$ bei Division durch X den Rest 0 lässt; dies stellt sicher, dass p keinen konstanten Term hat. Es sei nun $\Phi_j : V^{\lambda_j} \to V^{\lambda_j}$ die Einschränkung von Φ. Sein charakteristisches Polynom ist dann gerade χ_j, und mit Cayley–Hamilton folgt $\chi_j(\Phi_j) = 0$. Mittels (6.7.5) erhalten wir $p(\Phi_j) = \lambda_j \cdot \mathrm{Id}_{V^{\lambda_j}}$. Wegen der Invarianz der Haupträume gilt daher

$$p(\Phi)|_{V^{\lambda_j}} = p(\Phi_j) = \lambda_j \cdot \mathrm{Id}_{V^{\lambda_j}},$$

d.h. $p(\Phi)$ wirkt auf dem Hauptraum V^{λ_j} gerade durch Multiplikation mit λ_j. Das ist aber genau dasselbe, was der diagonalisierbare Teil Φ_d in der Jordan–Chevalley-Zerlegung tut! Dies zeigt, dass $p(\Phi) = \Phi_d$ und setzen wir $q(X) := X - p(X)$, so erhalten wir

$$q(\Phi) = \Phi - p(\Phi) = \Phi - \Phi_d = \Phi_n. \qquad \square$$

Mittels Lemma 6.7.22 erhält man nun das folgende Resultat:

Satz 6.7.24 (Eigenschaften der additiven Jordan–Chevalley-Zerlegung)**.** *Sei $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ trigonalisierbar und $\Psi \in \mathrm{End}_{\mathbb{K}}(V)$.*

(i) Φ besitzt eine eindeutige Jordan–Chevalley-Zerlegung (Φ_d, Φ_n).

(ii) $\Phi \circ \Psi = \Psi \circ \Phi$ gilt genau dann, wenn $\Phi_d \circ \Psi = \Psi \circ \Phi_d$ und $\Phi_n \circ \Psi = \Psi \circ \Phi_n$.

(iii) $W < V$ ist Φ-invariant genau dann, wenn er Φ_d-invariant und Φ_n-invariant ist.

(iv) Ist Ψ ebenfalls trigonalisierbar mit additiver Jordan–Chevalley-Zerlegung (Ψ_d, Ψ_n) und gilt $\Phi \circ \Psi = \Psi \circ \Phi$, so gilt $(\Phi + \Psi)_d = \Phi_d + \Psi_d$ und $(\Phi + \Psi)_n = \Phi_n + \Psi_n$.

Beweis. Es sei $\Phi = \Phi_d + \Phi_n$ eine additive Jordan–Chevalley-Zerlegung wie in Lemma 6.7.22 und $\Phi = \Phi'_d + \Phi'_n$ eine weitere additive Jordan–Chevalley Zerlegung (die a priori nicht notwendig von dieser Form ist). Für die Zerlegung $\Phi = \Phi_d + \Phi_n$ folgen (ii) und (iii) sofort aus Lemma 6.7.22. (Übung!). Wir zeigen nun die Eindeutigkeit der Zerlegung, woraus dann (ii) und (iii) allgemein folgen. Aus $\Phi = \Phi_d + \Phi_n = \Phi'_d + \Phi'_n$ folgt sofort, dass

$$\Phi_d - \Phi'_d = \Phi'_n - \Phi_n. \tag{6.7.6}$$

Weil Φ'_d und Φ'_n miteinander vertauschen, vertauschen sie auch mit $\Phi'_d + \Phi'_n = \Phi$ und daher wegen (ii) auch mit Φ_d und Φ_n. Da Φ_d und Φ'_d vertauschen und diagonalisierbar sind, sind sie simultan diagonalisierbar. Da Φ_n und Φ'_n nilpotent sind und vertauschen, ist ihre Differenz nilpotent: In der binomischen Formel für $(\Phi_n - \Phi'_n)^{2k}$ tauchen nämlich nur Terme auf, in denen entweder Φ_n^k oder $(\Phi'_n)^k$ als Faktoren vorkommen. Der Endomorphismus in (6.7.6) ist also sowohl diagonalisierbar als auch nilpotent und daher 0. Dies zeigt $\Phi_d = \Phi'_d$ und $\Phi_n = \Phi'_n$, wodurch (i), (ii) und (iii) bewiesen sind.

Sind schließlich Φ und Ψ wie in (iv), so folgt durch zweimaliges Anwenden von (ii), dass Φ_d, Φ_n, Ψ_d und Ψ_n allesamt miteinander vertauschen. Dann ist aber wieder $\Phi_d + \Psi_d$ diagonalisierbar und $\Phi_n + \Psi_n$ nilpotent und da beide Summen miteinander vertauschen, folgt (iv) dann aus (i). □

Später werden wir noch die folgende Variante der Jordan–Chevalley-Zerlegung benötigen:

Definition 6.7.25. Es sei Φ invertierbar. Ein Paar (Φ_d, Φ_u) von Endomorphismen von V heißt eine *multiplikative Jordan–Chevalley-Zerlegung* von Φ, falls gilt:

(JC1) $\Phi = \Phi_d \circ \Phi_u$.

(JC2) Φ_d ist diagonalisierbar und Φ_u ist unipotent (d.h. $\Phi_u - \mathrm{Id}$ ist nilpotent).

(JC3) $\Phi_d \circ \Phi_u = \Phi_u \circ \Phi_d$.

Analog definiert man eine multiplikative Jordan–Chevalley-Zerlegung einer invertierbaren Matrix.

Bemerkung 6.7.26. Ist (Φ_d, Φ_u) eine multiplikative Jordan–Chevalley-Zerlegung von Φ, so folgt aus der Bijektivität von Φ und (JC1), dass Φ_u surjektiv und Φ_d injektiv ist, also sind Φ_u und Φ_d ebenfalls bijektiv. (Jeder unipotenten Endomorphismus ist automatisch invertierbar, wie man leicht mittels der geometrischen Reihe zeigt, vgl. die Übungen.)

Beispiel 6.7.27. Wir schauen uns wieder die Standardbeispiele an:

(i) Für einen Jordanblock gilt $J_+[(n)_\lambda] = (\lambda \cdot \mathbf{1})(\mathbf{1} + \frac{1}{\lambda} J_+[n])$, oder in Matrizen ausgeschrieben

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{\lambda} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & \frac{1}{\lambda} \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}.$$

Ist $\lambda \neq 0$, so ist $\lambda \cdot \mathbf{1}$ diagonal(isierbar) und invertierbar und vertauscht mit jeder Matrix. Die Matrix $\mathbf{1} + \frac{1}{\lambda} J_+[n]$ ist unipotent, weil $\frac{1}{\lambda} J_+[n]$ nilpotent ist. Für $\lambda \neq 0$ ist $(\lambda \cdot \mathbf{1}, \mathbf{1} + \frac{1}{\lambda} J_+[n])$ daher eine multiplikative Jordan–Chevalley-Zerlegung von $J_+[(n)_\lambda]$.

(ii) Ist allgemein $J \in \mathbb{K}^{n\times n}$ eine invertierbare Matrix in Jordannormalform, so gilt $0 \notin \operatorname{spec}_{\mathbb{K}}(J)$. In dem man blockweise wie in (i) zerlegt erhält man daher eine Zerlegung $J = D\cdot U$, wo D eine invertierbare Diagonalmatrix und U eine unipotente obere Dreiecksmatrix ist mit 1en auf der Diagonale ist. Aus (i) folgt dann, dass (D,U) eine multiplikative Jordan–Chevalley-Zerlegung von J ist.

(iii) Ist A invertierbar und trigonalisiebar über $\mathbb{K}$, so gilt $A = SJS^{-1}$ für ein $S \in \mathrm{GL}_n(\mathbb{K})$. Es sei (D,U) eine multiplikative Jordan–Chevalley-Zerlegung vo J. Dann ist SDS^{-1} diagonalisierbar und invertierbar, SUS^{-1} ist unipotent und es gilt

$$SDS^{-1}\cdot SUS^{-1} = SJS^{-1} = A \quad \text{und} \quad SUS^{-1}\cdot SDS^{-1} = SUDS^{-1} = SDUS^{-1} = A.$$

Folglich ist (SDS^{-1}, SUS^{-1}) eine multiplikative Jordan–Chevalley-Zerlegung von A.

Damit haben wir gezeigt:

Proposition 6.7.28. *Jeder trigonalisierbare Automorphismus und jede trigonalisierbare invertierbare Matrix besitzt eine multiplikative Jordan–Chevalley-Zerlegung.* □

Lemma 6.7.29 (Additive vs. multiplikative Zerlegung)**.** *Es sei $A \in \mathrm{GL}_n(\mathbb{K})$ trigonalisierbar. Ist (A_d, A_u) eine multiplikative Jordan–Chevalley-Zerlegung von A und ist $A_n := A_d(A_u - \mathbf{1})$, so ist (A_d, A_n) die eindeutige additive Jordan–Chevalley-Zerlegung von A, und es gilt $A_u = \mathbf{1} + A_d^{-1}A_n$.*

Beweis. Da A_d und A_u miteinander und mit der Einheitsmatrix vertauschen, vertauscht auch A_n mit A_d und A_u (und daher mit A). Nach Definition ist A_d diagonalisierbar, und $A_u - \mathbf{1}$ ist nilpotent, also gilt $(A_u - \mathbf{1})^n = 0$. Da A_d und $A_u - \mathbf{1}$ miteinander vertauschen, gilt

$$A_n^n = A_d^n(A_u - \mathbf{1})^n = 0,$$

also ist A_n nilpotent. Mit

$$A_d + A_n = A_d + A_d(A_u - \mathbf{1}) = A_d + A_dA_u - A_d = A$$

folgt, dass (A_d, A_n) die additive Jordan–Chevalley-Zerlegung von A ist. Da A invertierbar ist, ist auch A_d invertierbar, und es gilt $A_u = \mathbf{1} + A_d^{-1}A_d(A_u - \mathbf{1}) = \mathbf{1} + A_d^{-1}A_n$. □

Da A_d und A_n (und daher $A_u = \mathbf{1} + A_d^{-1}A_n$) durch A eindeutig bestimmt sind, erhalten wir:

Korollar 6.7.30 (Eindeutigkeit)**.** *Die multiplikative Jordan–Chevalley-Zerlegung einer trigonalisierbaren Matrix $A \in \mathrm{GL}_n(\mathbb{K})$ ist eindeutig und ihr diagonalisierbarer Teil stimmt mit dem diagonalisierbaren Teil der additiven Jordan–Chevalley-Zerlegung überein. Insbesondere ist letzterer invertierbar.* □

Aufgrund von Lemma 6.7.29 übertragen sich nun die Eigenschaften der additiven Jordan–Chevalley-Zerlegung aus Satz 6.7.24 aus die multiplikative Zerlegung:

Übung 6.7.31. Es sei $\Phi \in \mathrm{GL}(V)$ trigonalisierbar mit multiplikativer Jordan–Chevalley-Zerlegung (Φ_d, Φ_u). Zeigen Sie:

(i) $\Psi \in \mathrm{GL}(V)$ vertauscht mit Φ genau dann, wenn es mit Φ_d und Φ_u vertauscht.

(ii) $W \leq V$ ist Φ-invariant genau dann, wenn er Φ_d-invariant und Φ_u-invariant ist.

(iii) Ist $\Psi \in \mathrm{GL}(V)$ trigonalisierbar und vertauscht mit Φ, so gilt $(\Phi\circ\Psi)_d = \Phi_d\circ\Psi_d$ und $(\Phi\circ\Psi)_u = \Phi_u\circ\Psi_u$.

Zusammenfassung von Abschnitt 6.7

(1) Jede Ähnlichkeitsklasse reeller Matrizen besitzt einen Repräsentanten in reeller Jordannormalform, der eindeutig bis aus Vertauschen der Blöcke und Vorzeichen der Nebendiagonaleinträge ist. Man erhält diesen aus der entsprechenden komplexen Jordannormalform durch Galois-Abstieg.

(2) Jeder Endomorphismus lässt sich eindeutig als Summe eines diagonalisierbaren Endomorphismus und eines damit vertauschenden nilpotenten Endomorphismus schreiben. Jeder Automorphismus lässt sich eindeutig als Produkt eines diagonalisierbaren Automorphismus und eines damit vertauschenden unipotenten Automorphismus schreiben.

7 Sesquilinearformen

7.1 Motivation: Skalarprodukte

Bemerkung 7.1.1 (Was fehlt bisher?)**.** Bisher haben wir den $\mathbb{R}^n$ nur in seiner Eigenschaft als Vektorraum behandelt. In einem abstrakten Vektorraum kann man lediglich Vektoren addieren und mit Skalaren multiplizieren. Mithilfe dieser Struktur kann man Geraden, Ebenen und allgemeiner affine Unterräume definieren, man kann darüber reden, ob Vektoren linear unabhängig oder affine Unterräume gleicher Dimension parallel sind. Die geometrischen Fragen, die man hier untersuchen kann, sind im Wesentlichen auf die *Geometrie der Lage* beschränkt. Man kann also z.B. mit Hilfe der Vektorraumstruktur entscheiden, ob Geraden im $\mathbb{R}^3$ sich schneiden, parallel oder windschief sind.

Man kann dagegen in einem abstrakten Vektorraum nicht von der *Länge* eines Vektors reden, genauso wenig wie man sinnvoll einen *Winkel* zwischen zwei Vektoren definieren kann. Sie wissen aber aus der Schule, dass es im $\mathbb{R}^n$ sehr wohl eine Möglichkeit gibt, Längen- und Winkelbegriffe einzuführen, und diese Begriffe spielen eine zentrale Rolle in den meisten geometrischen Fragestellungen. Um Längen und Winkel im $\mathbb{R}^n$ zu bestimmen, benötigt man neben der Vektorraumstruktur aber eine Zusatzstruktur, nämlich ein Skalarprodukt. Es wird sich herausstellen, dass man in jedem endlichdimensionalen abstrakten Vektorraum über $\mathbb{R}$ oder $\mathbb{C}$ solche Strukturen definieren und damit Geometrie treiben kann.

Wenn man einmal ein Skalarprodukt gewählt hat, dann kann man viele unserer bisherigen Resultate verfeinern. Statt beliebiger linearer Abbildungen kann man solche betrachten, die Längen und Winkel erhalten, und statt allgemeiner linearer Koordinatensysteme zu betrachten, kann man sich auf die aus der Schule bekannten *kartesischen* Koordinatensysteme beschränken, bei denen man verlangt, dass die Koordinatenachsen senkrecht aufeinander stehen. Das führt dann auf ganz neue Probleme, die wesentlich geometrischer (und damit näher an der Ihnen bekannten Schulmathematik) sind als die bisher betrachteten.

Definition 7.1.2. Es sei $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Ein kontravarianter 2-Tensor $B : V \times V \to \mathbb{K}$ heißt eine *Bilinearform*. Eine Bilinearform B heißt *symmetrisch*, falls $B(v,w) = B(w,v)$ für alle $v,w \in V$ gilt. In diesem Fall heißt die Abbildung $q_B : V \to \mathbb{K}$, $v \mapsto B(v,v)$ die zu B gehörige *quadratische Form*. Ist $\mathbb{K} = \mathbb{R}$, so heißt eine symmetrische Bilinearform *positiv-definit* bzw. ein *(reelles) Skalarprodukt*, falls $q_B(v) > 0$ für alle $v \in V \setminus \{0\}$ gilt. In diesem Fall heißt (V,B) ein *euklidischer Vektorraum*.

Übung 7.1.3 (Polarisierung)**.** Es sei $B : V \times V \to \mathbb{K}$ eine symmetrische Bilinearform mit zugehöriger quadratischer Form $q = q_B$ und es gelte $\mathrm{char}(\mathbb{K}) \neq 2$. Zeigen Sie, dass die *Polarisierungsidentität*

$$B(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) \quad (x,y \in V)$$

gilt, und folgern Sie daraus, dass B durch q eindeutig bestimmt ist.

Beispiel 7.1.4 (Euklidische Ebene)**.** Das *Standardskalarprodukt* auf $\mathbb{R}^2$ ist definiert als

$$B_0 : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}, \quad (v,w) \mapsto v^\top w.$$

Die zugehörige quadratische Form ist dann gegeben durch

$$q_0 : \mathbb{R}^2 \to \mathbb{R}, \quad v \mapsto v^\top v = v_1^2 + v_2^2.$$

Mittels dieses Skalarprodukts kann man Längen und Winkel in der euklidischen Ebene beschreiben:

Ist $v \in \mathbb{R}^2$, so bilden die Punkte $0 = (0,0)^\top$, $(v_1,0)^\top$ und $v = (v_1,v_2)^\top$ ein rechtwinkliges Dreieck. Der Abstand von v zum Ursprung ist die Länge der Hypothenuse dieses Dreiecks, die nach dem Satz des Pythagoras durch

$$\|v\| = \sqrt{v_1^2 + v_2^2} = \sqrt{q_0(v)} = \sqrt{B_0(v,v)}$$

gegeben ist. Wir nennen $\|v\|$ die *euklidische Norm* des Vektors v. Sind v und w zwei beliebige Punkte der Anschauungsebene $\mathbb{R}^2$, so ist ihr *euklidischer Abstand* gegeben durch

$$d(v,w) := \|v-w\| = \sqrt{q_0(v-w)} = \sqrt{B_0(v-w,v-w)}.$$

Mittels des Skalarprodukts kann man aber nicht nur Längen, sondern auch Winkel bestimmen: Es seien v und w zwei linear unabhängige Vektoren, wobei wir die Reihenfolge so wählen, dass der Strahl durch w aus dem Strahl durch v mittels einer Drehung von weniger als 180 Grad hervorgeht. Es sei $\alpha = \angle(v,w) \in (0,\pi)$ der Winkel zwischen diesen beiden Strahlen, gemessen in Bogenmaß. Dies ist gerade der Winkel an 0 im Dreieck mit Eckpunkten 0, v und w, dessen Seitenlängen durch $\|v\|$, $\|w\|$ und $\|v-w\|$ (gegenüber von 0) gegeben sind. Der Kosinussatz liefert dann die Formel

$$\|v-w\|^2 = \|v\|^2 + \|w\|^2 - 2\|v\|\|w\|\cos(\alpha). \tag{7.1.1}$$

Um diese Gleichung nach α aufzulösen, verwenden wir die Bilinearität und Symmetrie von B_0: Es ist nämlich

$$\|v-w\|^2 = B_0(v-w,v-w) = B_0(v,v) - B_0(v,w) - B_0(w,v) + B_0(w,w) = \|v\|^2 + \|w\|^2 - 2B_0(v,w).$$

Einsetzen in 7.1.1 liefert

$$\|v\|^2 + \|w\|^2 - 2B_0(v,w) = \|v\|^2 + \|w\|^2 - 2\|v\|\|w\|\cos(\alpha), \quad \text{also} \quad \cos(\alpha) = \frac{B_0(v,w)}{\|v\|\|w\|}.$$

Da der Cosinus sich zu einer Bijektion $[0,\pi] \to [-1,1]$ einschränkt, ist dadurch α eindeutig festgelegt. Bezeichnen wir mit $\arccos : [-1,1] \to [0,\pi]$ die entsprechende Umkehrfunktion („Hauptzweig des Arkuscosinus“), so gilt also

$$\angle(v,w) = \arccos\left(\frac{B_0(v,w)}{\|v\|\|w\|}\right). \tag{7.1.2}$$

Diese Formel gilt auch nocht, wenn v und w linear abhängig, aber nicht 0 sind - in diesem Fall ist dann $\angle(v,w) \in \{0,\pi\}$.

Ein besonders wichtiger Fall tritt ein, wenn v und w einen rechten Winkel bilden. Wir schreiben dann $v \perp w$ und sagen v und w sind *orthogonal*. Aus (7.1.2) folgt sofort, dass

$$v \perp w \iff \cos(\angle(v,w)) = 0 \iff B_0(v,w) = 0.$$

Beispiel 7.1.5 (Höhere Dimensionen)**.** Analog zum Standardskalarprodukt im $\mathbb{R}^2$ definiert man das *Standardskalarprodukt* im $\mathbb{R}^n$ durch die Formel

$$B_0 : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, \quad (v,w) \mapsto B_0(v,w) := v^\top w.$$

Das ist wieder ein Skalarprodukt mit zugehöriger quadratischer Form $q_0(v) = \sum_{i=1}^n v_i^2$. Für $n = 3$ können wir euklidische Längen und Winkel mit denselben Formeln wie in der Ebene beschreiben. In höheren Dimensionen *definieren* wir Abstände und Winkel ganz einfach durch diese Formeln. Damit können wir jetzt 7-dimensionale euklidische Geometrie betreiben! Einen Haken gibt es aber noch: Wir müssen uns überlegen, warum die Definition des Winkels in höheren Dimensionen noch wohldefiniert ist. Dies folgt aus der folgenden Abschätzung, die für weite Teile der Analysis zentral ist.

Lemma 7.1.6 (Cauchy–Schwarz-Ungleichung[1])**.** *Es sei (V,B) ein euklidischer Vektorraum.*

(i) Für alle $x,y \in V$ gilt

$$B(x,y)^2 \le B(x,x)B(y,y), \quad \textit{und daher} \quad |B(x,y)| \le \|x\|\|y\|. \tag{7.1.3}$$

(ii) Es gilt Gleichheit in (i) genau dann, wenn x und y linear abhängig sind.

Beweis. Für $y = 0$ gelten (i) und (ii) offensichtlich. Sei also $y \neq 0$; für alle $\lambda \in \mathbb{R}$ gilt dann

$$0 \le B(x-\lambda y, x-\lambda y) = B(x,x) - \lambda B(y,x) - \lambda B(x,y) + \lambda^2 B(y,y),$$

wobei wegen der positiven Definitheit Gleichheit genau dann gilt, wenn $x = \lambda y$. Der Trick besteht nun darin, den speziellen Wert $\lambda := B(x,y)/B(y,y)$ zu wählen; wir erhalten dann

$$0 \le B(x,x) - \frac{B(x,y)^2}{B(y,y)} - \frac{B(x,y)^2}{B(y,y)} + \frac{B(x,y)^2}{B(y,y)} = B(x,x) - \frac{B(x,y)^2}{B(y,y)},$$

was gleichbedeutend mit (7.1.3) ist. Wenn Gleichheit gilt, so ist $x = \lambda y$, also sind x und y linear abhängig. Sind umgekehrt x und y linear abhängig (und $y \neq 0$), so können wir $x = \lambda y$ für ein $\lambda \in \mathbb{R}$ schreiben, und erhalten dann

$$B(x,y)^2 = B(\lambda y, y)^2 = \lambda^2 B(y,y)B(y,y) = B(\lambda y, \lambda y)B(y,y) = B(x,x)B(y,y).$$

Damit ist alles gezeigt. □

Definition 7.1.7. Sei (V,B) ein euklidischer Vektorraum mit zugehöriger quadratischer Form $q = q_B : V \to \mathbb{R}$.

(i) Für $v \in V$ heißt $\|v\| := \sqrt{q(v)}$ die *Norm* von v.

(ii) Für $v,w \in V$ heißt $d(v,w) := \|v-w\|$ der *Abstand* von v und w.

(iii) Sind $v,w \in V \setminus \{0\}$, so definieren wir $\angle(v,w)$ durch (7.1.2) – dies ist wegen der Cauchy–Schwarz-Ungleichung wohldefiniert.

[1] auch Cauchy–Schwarz–Bunjakowski-Ungleichung genannt, nach AUGUSTIN-LOUIS CAUCHY (frz. Mathematiker, 1789-1857), HERMANN AMANDUS SCHWARZ (dt. Mathematiker, 1843-1921) und VIKTOR BUNJAKOWSKI (russ. Mathematiker 1804-1889). Wie die Namen schon andeuten, wurde diese Ungleichung in verschiedenen Kulturkreisen mehrfach entdeckt.

(iv) Wir schreiben $v \perp w$ und nennen v und w *orthogonal*, falls $B(v,w) = 0$ gilt (falls also entweder $v = 0$ oder $w = 0$ gilt oder der Winkel $\pi/2$ ist).

Für die Standardskalarprodukte im $\mathbb{R}^2$ und $\mathbb{R}^3$ liefert das die aus der Schule vertrauten Begriffe - in höheren Dimensionen erhalten wir die „natürlichen“ Verallgemeinerungen.

Bemerkung 7.1.8 (Eigenschaften von Norm und Abstand)**.** Ist (V,B) ein euklidischer Vektorraum, so ist die zugehörige Norm $\|\cdot\|$ eine *Norm* im Sinne der Analysis, d.h. für $x,y \in V$ und $\lambda \in \mathbb{R}$ gilt

(N1) $\|x\| = 0 \iff x = 0$. (Definitheit)

(N2) $\|\lambda x\| = |\lambda|\|x\|$. (positive Homogenität)

(N3) $\|x+y\| \le \|x\| + \|y\|$. (Subadditivität)

(N1) folgt hierbei sofort aus der positiven Definitheit, und für (N2) rechnet man nach, dass

$$\|\lambda x\|^2 = B(\lambda x, \lambda x) = \lambda^2 B(x,x) = (|\lambda|\|x\|)^2.$$

(N3) folgt aus der Cauchy–Schwarz-Ungleichung wegen

$$\begin{aligned} \|x+y\|^2 &= B(x+y,x+y) = B(x,x)+B(x,y)+B(y,x)+B(y,y) = B(x,x)+2B(x,y)+B(y,y) \\ &\le B(x,x)+2|B(x,y)|+B(y,y) \\ &\le \|x\|^2 + \|x\|\|y\| + \|y\|^2 = (\|x\|+\|y\|)^2. \end{aligned}$$

Daraus folgt nun sofort, dass $d(x,y) := \|x-y\|$ eine *Metrik* im Sinne der Analysis auf V definiert, dass also für alle $x,y,z \in V$ die folgenden Axiome gelten:

(M1) $d(x,y) = 0 \iff x = y$. (Definitheit)

(M2) $d(x,y) = d(y,x)$. (Symmetrie)

(M3) $d(x,z) \le d(x,y) + d(y,z)$. (Dreiecksungleichung)

Wie sie aus der Analysis wissen, liefern solche Metriken einen sehr vernünftigen Abstandsbegriff. Metriken die von Normen herkommen haben noch die wichtige Zusatzeigenschaft der *Translationsinvarianz*: Für alle $x,y,z \in V$ gilt nämlich

$$d(x+z,y+z) = \|(x+z)-(y+z)\| = \|x-y\| = d(x,y).$$

Abstrakte Skalarprodukte liefern also translationsinvariante Metriken auf Vektorräumen. Diese Metriken haben noch weitere zusätzliche Eigenschaften, die in der folgenden Übung beschrieben werden.

Übung 7.1.9. Es sei (V,B) ein euklidischer Vektorraum und $\|\cdot\|$ die zugehörige Norm. Zeigen Sie:

(i) Es gilt der *Satz des Pythagoras* und seine Umkehrung: Für $x,y \in V$ ist $B(x,y) = 0$ genau dann, wenn $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.

(ii) Es gilt die *Parallelogrammgleichung*: Für $x,y \in V$ ist $\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$. Was folgt daraus für die Längen der Seiten und Diagonalen eines Parallelogramms in der euklidischen Ebene?

Gewisse unendlich-dimensionale Varianten der Standardskalarprodukte spielen in der Analysis eine zentrale Rolle:

Beispiel 7.1.10 (Integral als Skalarprodukt)**.** Es bezeichne $\mathscr{R}([0,1],\mathbb{R})$ die Menge der Riemann-integrierbaren reell-wertigen Funktionen auf dem Intervall $[0,1]$ und $C([0,1],\mathbb{R})$ die Teilmenge der stetigen Funktionen. Aus der Analysis ist bekannt, dass $C([0,1],\mathbb{R})$ ein Vektorraum bzgl. punktweiser Addition und Skalarmultiplikation ein Vektorraum ist und sogar bzgl. punktweiser Multiplikation eine $\mathbb{R}$-Algebra bildet. Aus der Linearität des Integrals folgt dann leicht, dass

$$B : C([0,1],\mathbb{R}) \times C([0,1],\mathbb{R}) \to \mathbb{R}, \quad B(f,g) := \int_0^1 f(x)g(x)\,dx$$

ein Skalarprodukt mit zugehöriger quadratischer Form $\int_0^1 f(x)^2\,dx$ ist. (Man benötigt aus der Analysis die nicht-triviale Tatsache, dass für eine nicht-negative stetige Funktion $g : [0,1] \to \mathbb{R}$ mit $g \neq 0$ das Integral $\int_0^1 g(x)\,dx$ stets strikt positiv ist - für allgemeine Riemann-integrierbare Funktionen gilt das nicht unbedingt!) Man beachte die formale Ähnlichkeit zwischen den Ausdrücken

$$\sum_{i=1}^{n} f_i g_i \quad \text{und} \quad \int f(x)g(x)\,dx.$$

Im Folgenden wollen wir aber lediglich Skalarprodukte auf *endlichdimensionalen* Vektorräumen betrachten.

Definition 7.1.11. Ist (V,B) ein euklidischer Vektorraum, so heißt $\Phi \in \mathrm{GL}_{\mathbb{R}}(V)$ *orthogonal* bzgl. B, falls

$$B(\Phi(v),\Phi(w)) = B(v,w)$$

für alle $v,w \in V$ gilt. Wir bezeichnen mit $O_{\mathbb{R}}(V,B) \subseteq \mathrm{GL}_{\mathbb{R}}(V)$ die Teilmenge der orthogonalen Abbildungen.

Nach Definition erhalten orthogonale Abbildungen das Skalarprodukt und daher Längen und Winkel. Insbesondere erhalten sie Orthogonalität.

Übung 7.1.12. Zeigen Sie, dass die orthogonalen Abbildungen von $\mathbb{R}^2$ bzgl. des Standardskalarprodukts genau die Spiegelungen an Ursprungsgeraden und die Drehungen um den Ursprung sind.

Es ist ein naheliegendes Ziel, alle Skalarprodukte auf reellen Vektorräumen und die zugehörigen orthogonalen Abbildungen zu beschreiben. Als ersten Schritt in diese Richtung überlegen wir uns, wie wir allgemein Bilinearformen (ohne Positivitätsbedingungen) beschreiben können. Wir schauen uns das gleich über einem beliebigen Körper an - das bereitet keine zusätzlichen Schwierigkeiten. Im Folgenden sei stets $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und

$$\mathrm{Bil}_{\mathbb{K}}(V) := \{B : V \times V \to \mathbb{K} \mid B \text{ ist bilinear}\}.$$

Bemerkung 7.1.13. Sei $B \in \mathrm{Bil}_{\mathbb{K}}(V)$ und $\mathscr{B} = (v_1,\ldots,v_n)$ eine geordnete Basis von V. Für beliebige $x,y \in V$ erhalten wir dann

$$B(x,y) \;=\; B\left(\sum_{i=1}^{n} v_i^*(x)v_i, \sum_{j=1}^{n} v_j^*(y)v_j\right) \;=\; \sum_{i=1}^{n}\sum_{j=1}^{n} v_i^*(x)v_j^*(y)B(v_i,v_j). \tag{7.1.4}$$

Es seien nun $[x]_{\mathscr{B}} = (v_1^*(x), \dots, v_n^*(x))^\top$ und $[y]_{\mathscr{B}} = (v_1^*(y), \dots, v_n^*(y))^\top$ die Koordinatenvektoren von x und y. Definieren wir eine Matrix

$$A := (a_{ij}) \in \mathbb{K}^{n\times n} \quad \text{durch} \quad a_{ij} := B(v_i, v_j),$$

so können wir dies schreiben als

$$B(x,y) = [x]_{\mathscr{B}}^\top A [y]_{\mathscr{B}}. \tag{7.1.5}$$

Definition 7.1.14. Sei $B \in \mathrm{Bil}_{\mathbb{K}}(V)$ und $\mathscr{B} = (v_1, \dots, v_n)$ eine geordnete Basis von V. Dann heißt die Matrix $D_{\mathscr{B}}(B) := (a_{ij})$ mit

$$a_{ij} := B(v_i, v_j)$$

die *darstellende Matrix* von B bzgl. $\mathscr{B}$.

Proposition 7.1.15. *Für jede geordnete Basis $\mathscr{B}$ von V ist die Abbildung $D_{\mathscr{B}} : \mathrm{Bil}_{\mathbb{K}}(V) \to \mathbb{K}^{n\times n}$ ein Vektorraumisomorphismus.*

Beweis. Linearität von $D_{\mathscr{B}}$ rechnet man leicht nach, und Injektivität folgt aus (7.1.5). Ist umgekehrt $A \in \mathbb{K}^{n\times n}$, so überlegt man sich, dass die Abbildung $B : V \times V \to \mathbb{K}$ gegeben durch $B(x,y) := [x]_{\mathscr{B}}^\top A [y]_{\mathscr{B}}$ eine Bilinearform ist, und dass $D_{\mathscr{B}}(B) = A$ gilt (Übung!). □

Beispiel 7.1.16. Wählen wir für $\mathscr{B}$ die Standardbasis des $\mathbb{K}^n$, so besagt Proposition 7.1.15 gerade, dass jede Bilinearform B auf $\mathbb{K}^n$ als $B(x,y) = x^\top A y$ für eine eindeutige Matrix $A \in \mathbb{K}^{n\times n}$ geschrieben werden kann. Das Standardskalarprodukt auf $\mathbb{R}^n$ entspricht dabei gerade der Einheitsmatrix!

Bilinearformen werde also durch Matrizen beschrieben. Aber Moment, beschreiben Matrizen nicht auch lineare Abbildungen? Was geht hier vor?

Übung 7.1.17 (Bilinearformen als lineare Abbildungen)**.** Zeigen Sie:

(i) Für eine Bilinearform $B \in \mathrm{Bil}_{\mathbb{K}}(V)$ und $v, w \in V$ sei $\Phi_B(v)(w) := B(v,w)$. Dann ist $\Phi_B(v) \in V^*$, und die Abbildung

$$\Phi_B : V \to V^*, \quad v \mapsto \Phi_B(v)$$

ist linear.

(ii) Die Abbildung

$$\Phi : \mathrm{Bil}_{\mathbb{K}}(V) \to \mathrm{Hom}_{\mathbb{K}}(V, V^*), \quad B \mapsto \Phi_B.$$

ist ein Vektorraumiomorphismus.

[Hinweis: Zum Beweis der Bijektivität geben Sie am besten eine explizite Umkehrabbildung an!]

(iii) Ist $\mathscr{B}$ eine Basis von V und $B \in \mathrm{Bil}_{\mathbb{K}}(V)$, so ist

$$D_{\mathscr{B}}(B) = D_{\mathscr{B}^*,\mathscr{B}}(\Phi_B)^\top,$$

wobei $\mathscr{B}^*$ die zu $\mathscr{B}$ duale Basis von V^* ist.

Bis auf eine Transposition (die der Konvention geschuldet ist) ist die darstellende Matrix einer Bilinearform also nichts anderes als die darstellende Matrix der entsprechenden linearen Abbildung $V \to V^*$.

Übung 7.1.18. Es sei $V := \mathrm{Pol}_{\leq 3}(\mathbb{R})$ der Vektorraum der Polynomfunktionen vom Grad ≤ 3 auf $\mathbb{R}$. Zeigen Sie, dass auf V eine symmetrische Bilinearform definiert wird durch

$$B : V \times V \to \mathbb{R}, \quad (p,q) \mapsto \int_0^1 p(x)q(x)\mathrm{d}x.$$

Bestimmen Sie außerdem die darstellende Matrix $D_{\mathscr{B}}(B)$ bzgl. der geordneten Basis $\mathscr{B} := \{1, x, x^2, x^3\}$ von V.

Wie im Fall von linearen Abbildungen stellt sich die Frage nach der Abhängigkeit der darstellenden Matrix von der Wahl der geordneten Basis. In unserem neuen Setting haben wir das folgende Gegenstück zur Basiswechselformel.

Satz 7.1.19 (Basiswechsel für Bilinearformen)**.** *Seien $\mathscr{B}_1 = (v_1, \ldots, v_n)$ und $\mathscr{B}_2 = (w_1, \ldots, w_n)$ geordnete Basen von V und $B : V \times V \to \mathbb{K}$ eine Sesquilinearform. Dann gilt:*

$$D_{\mathscr{B}_2}(B) = D_{\mathscr{B}_1,\mathscr{B}_2}(\mathrm{Id})^\top \cdot D_{\mathscr{B}_1}(B) \cdot D_{\mathscr{B}_1,\mathscr{B}_2}(\mathrm{Id}).$$

Beweis. Es sei $D_{\mathscr{B}_1,\mathscr{B}_2}(\mathrm{Id}) = (a_{ij})$, $D_{\mathscr{B}_1}(B) = (b_{ij})$, $D_{\mathscr{B}_2}(B) = (c_{ij})$. Dann gilt

$$w_j = \sum_{i=1}^n a_{ij} v_i,$$

und daher

$$\begin{aligned} c_{ij} &= B(w_i, w_j) = B\left(\sum_{r=1}^n a_{ri} v_r, \sum_{s=1}^n a_{sj} v_s\right) \\ &= \sum_{r=1}^n \sum_{s=1}^n a_{ri} a_{sj} B(v_r, v_s) = \sum_{r=1}^n a_{ri} \left(\sum_{s=1}^n b_{rs} a_{sj}\right). \end{aligned}$$

Dies besagt aber gerade, dass

$$(c_{ij}) = (a_{ir})^\top (b_{rs})(a_{sj}),$$

woraus die Behauptung folgt. □

Man beachte, dass hier anders als beim Basiswechsel für lineare Abbildungen keine Matrix invertiert werden muss. Nach Satz 7.1.19 sind darstellende Matrizen derselben Bilinearform zu verschiedenen Basen zueinander kongruent im Sinne der folgenden Definition:

Definition 7.1.20. Zwei Matrizen $A, B \in \mathbb{K}^{n\times n}$ heißen *kongruent*, falls eine Matrix $P \in \mathrm{GL}_n(\mathbb{K})$ existiert mit $B = P^\top AP$.

Beispiel 7.1.21. Wir betrachten neben der Standardbasis $\mathscr{B}_1 = (e_1, e_2)$ noch eine zweite Basis von $V = \mathbb{R}^2$ gegeben durch

$$\mathscr{B}_2 := \left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}\right)$$

Es sei B das Standardskalarprodukt auf $\mathbb{R}^2$. Wir berechnen $D_{\mathscr{B}_2}(B)$ auf zwei Arten:

(i) Durch direktes Rechnen: Wir haben

$$B\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = 2, \quad B\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}\right) = -1, \quad B\left(\begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = -1, \quad B\left(\begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}\right) = 1,$$

und daher $D_{\mathscr{B}_2}(B) = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$.

(ii) Durch Basiswechsel: Es gilt

$$D_{\mathscr{B}_1}(B) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad D_{\mathscr{B}_1,\mathscr{B}_2}(\mathrm{Id}) = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix},$$

und folglich

$$D_{\mathscr{B}_2}(B) = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}^{\top} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}.$$

Das Ergebnis ist natürlich dasselbe.

[08.05.24]

Bemerkung 7.1.22 (Skalarprodukte und Matrizen)**.** Jede Matrix $A \in \mathbb{R}^{n\times n}$ definiert eine Bilinearform B_A auf $\mathbb{R}^n$ durch $B_A(v,w) := v^\top Aw$ (und jede Bilinearform auf $\mathbb{R}^n$ ist von dieser Form). Ist B_A symmetrisch, so gilt insbesondere

$$\forall\, i,j \in \{1,\dots,n\}:\ a_{ij} = e_i^\top A e_j = B_A(e_i,e_j) = B_A(e_j,e_i) = e_j^\top A e_i = a_{ji} \implies A = A^\top.$$

Diese Bedingung ist auch schon hinreichend, denn ist $A = A^\top$, so gilt

$$B_A(w,v) = w^\top Av = (w^\top Av)^\top = v^\top A^\top w = B_A(v,w),$$

wobei wir verwendet haben, dass für Matrizen M und N stets $(MN)^\top = N^\top M^\top$ gilt und dass jede (1×1)-Matrix mit ihrer Transponierten übereinstimmt. Die Bilinearform ist also genau dann symmetrisch, wenn $A^\top = A$ gilt; wir nennen dann A eine *symmetrische* Matrix.

Ist A eine symmetrische Matrix, so ist A genau dann ein Skalarprodukt, wenn für alle $x \in \mathbb{R}^n \setminus \{0\}$ die Ungleichung

$$x^\top Ax > 0$$

gilt. In diesem Fall nennen wir A eine *positiv-definite* Matrix. Skalarprodukte im $\mathbb{R}^n$ werden also durch positiv-definite symmetrische Matrizen beschrieben. Allgemeiner gilt: Eine Bilinearform ist genau dann ein Skalarprodukt wenn ihre darstellende Matrix bzgl. einer (und daher jeder) Basis positiv-definit und symmetrisch ist.

Wir werden später noch Kriterien sehen, die es uns erlauben, symmetrische Matrizen systematisch auf positive Definitheit zu untersuchen (Hauptminorenkriterium, Eigenwertkriterium). An dieser Stelle sei nur eine sehr schwache notwendige Bedingung erwähnt:

Lemma 7.1.23. *Ist $A \in \mathbb{R}^{n\times n}$ symmetrisch und positiv-definit, so ist jeder reelle Eigenwert von A positiv.*

Beweis. Ist $Av = \lambda v$ für ein $\lambda \in \mathbb{R}$ und $v \in \mathbb{R}^n \setminus \{0\}$, so gilt $v^\top Av = \lambda v^\top v$ und daher

$$\lambda = \frac{v^\top Av}{v^\top v} > 0. \qquad \square$$

Wir werden später noch sehen, dass sogar alle komplexen Eigenwerte (und daher die Determinante) reell und positiv sein müssen.

Bemerkung 7.1.24 (Orthogonale Abbildungen und Matrizen)**.** Ist $B = B_A$ wie in Bemerkung 7.1.22, und ist $C \in \mathbb{R}^{n\times n}$, so gilt für alle $x,y \in \mathbb{R}^n$, dass

$$B_A(Cx,Cy) = x^\top C^\top ACy \quad \text{und} \quad B_A(Cx,Cx) = x^\top C^\top ACx.$$

Insbesondere gilt für die Abbildung $\Phi_C : \mathbb{R}^n \to \mathbb{R}^n$, $x \mapsto Cx$, dass

$$\Phi_C \in \mathrm{O}(\mathbb{R}^n, B_A) \iff \forall x,y \in V : x^\top C^\top ACy \iff C^\top AC = A.$$

Die erste Äquivalenz ist die Definition, und die Rückrichtung der zweiten Implikation ist klar. Für die Hinrichtung wählt man für x und y Standardbasisvektoren und verwendet, dass $e_i A e_k = a_{ij}$. Ist speziell B_0 das Standardskalarprodukt, so gilt

$$\Phi_C \in \mathrm{O}(\mathbb{R}^n, B_0) \iff C^\top C = \mathbf{1} \iff C^\top = C^{-1}.$$

In diesem Fall nennen wir C eine *orthogonale Matrix*; die Gruppe der orthogonalen Matrizen bezeichnen wir mit $\mathrm{O}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R})$.

Im Folgenden sei stets (V,B) ein endlichdimensionaler euklidischer Vektorraum. Der folgende Satz ist fundamental für die Geometrie solcher Vektorräume.

Definition 7.1.25. Eine Teilmenge $C \subseteq V$ heißt *konvex*, falls $(x+y)/2 \in C$ für alle $x, y \in C$ gilt.

Lemma 7.1.26 (Hilbertscher Projektionssatz)**.** *Sei $C \subseteq V$ eine konvexe abgeschlossene Teilmenge und $x \in V$. Dann existiert ein eindeutiges $c_0 \in C$ mit*

$$d(x, c_0) = \inf_{c \in C} d(x, c).$$

Beweis. Es sei $D := \inf_{c \in C} d(x,c)$. Nach Definition existiert dann eine Folge (c_n) in C mit

$$d(x, c_n)^2 \leq D^2 + 1/n,$$

und wir definieren $c_{m,n} := (c_n + c_m)/2$. Da C konvex ist, gilt $c_{m,n} \in C$ und daher $d(c_{m,n}, x) \geq D$. Wir wenden nun die Parallelogrammidentität auf $x - c_n$ und $x - c_m$ an und erhalten so

$$\|(x-c_n)+(x-c_m)\|^2 + \|(x-c_n)-(x-c_m)\|^2 = 2(\|x-c_n\|^2 + \|x-c_m\|^2).$$

Wegen $(x-c_n)+(x-c_m) = 2(x-c_{m,n})$ und $(x-c_n)-(x-c_m) = c_m - c_n$ können wir dies umschreiben als

$$4d(x, c_{m,n})^2 + d(c_n, c_m)^2 = 2d(x, c_n)^2 + 2d(x, c_m)^2.$$

Daraus folgt nun, dass

$$d(c_n, c_m)^2 \quad \leq \quad 2\left(D^2 + \frac{1}{n}\right) + 2\left(D^2 + \frac{1}{m}\right) - 4D^2 \quad = \quad \frac{2}{n} + \frac{2}{m}.$$

Dies zeigt, dass (c_n) eine Cauchy-Folge im normierten Vektorraum $(V, \|\cdot\|)$ ist. In der Vorlesung ANALYSIS II lernt man, dass eine solche Folge gegen ein $c \in V$ konvergiert (im Sinne von $d(c_n, c) \to 0$). Da C abgeschlossen ist, gilt dann $c \in C$ und es gilt

$$D \leq d(x,c) \leq d(x, c_n) + d(c_n, c) \xrightarrow{n \to \infty} D + 0 = D,$$

also $d(x,c) = D$. Es sei nun $c' \in C$ ein weiterer Vektor mit $d(x,c') = D$. Wir wenden die Parallelogrammidentität auf $x - c$ und $x - c'$ an und erhalten

$$\|(x-c)+(x-c')\|^2 + \|(x-c)-(x-c')\|^2 = 2\|x-c\|^2 + 2\|x-c'\|^2 = 4D^2.$$

Wegen $(c+c')/2 \in C$ gilt dann $d(x, (c+c')/2) \geq D$ und daher

$$\|c'-c\|^2 = 4D^2 - \|2x-c-c'\|^2 = 4D^2 - 4\|x-(c+c')/2\|^2 \leq 4D^2 - 4D^2 = 0,$$

und dies impliziert $d(c', c) = 0$, also $c = c'$. □

Der Beweis des Hilbertschen Projektionssatzes verwendet die Parallelogrammidentität, die in euklidischen Vektorräumen, nicht aber in allgemeinen normierten Vektorräumen, wie sie in der Analysis verwendet werden, gilt. Die analoge Aussage in normierten Vektorräumen ist falsch, vgl. die Übungen.

Notation 7.1.27. Ist $C \subseteq V$ abgeschlossen und konvex, so schreiben wir $\pi_C(x)$ für den eindeutigen Punkt in C mit

$$d(x, \pi_C(x)) = \min_{c \in C} d(x, c).$$

Proposition 7.1.28 (Orthogonalprojektion)**.** *Es sei $U \leq V$ ein Unterraum. Dann gilt:*

(i) *U ist abgeschlossen und konvex.*

(ii) *Es gilt $\pi_U(x) = p$ genau dann, wenn*

$$\forall\, u \in U : (x-p) \perp u. \tag{7.1.6}$$

(iii) *$\pi_U : V \to V$ ist linear mit $\mathrm{Bild}(\pi_U) = U$.*

(iv) *Es gilt $\ker(\pi_U) = U^\perp := \{v \in V \mid \forall\, u \in U : v \perp u\}$.*

(v) *Es gilt $V = U \oplus U^\perp$, und $\pi_U = \pi_U^{U^\perp}$ ist die Projektion auf U in Richtung $U^\perp$.*

Beweis. (i) Konvexität folgt unmittelbar aus der Definition eines Unterraums. Für Abgeschlossenheit s. die Vorlesung ANALYSIS II.

(ii) Sei zunächst $p = \pi_U(x)$ und $u \in U \setminus \{0\}$. Wir setzen $u_0 := u/\|u\|$, so dass $\|u_0\| = 1$, sowie

$$\lambda := B(p-x, u_0) \quad \text{und} \quad q := p - \lambda u_0.$$

Wegen $p \in U$ und $u_0 \in U$ gilt dann $q \in U$ und daher

$$\|p-x\|^2 \leq \|q-x\|^2 = \|(p-x) - \lambda u_0\|^2 = \|p-x\|^2 - 2B(p-x, \lambda u_0) + \lambda^2 \|u_0\|^2.$$

Dies impliziert, dass

$$0 \leq \lambda^2 \|u_0\|^2 - 2B(p-x, \lambda u_0) = \lambda^2 - 2\lambda B(p-x, u_0) = \lambda^2 - 2\lambda^2 = -\lambda^2,$$

und daher $\lambda = 0$. Dann ist aber auch $B(p-x, u) = \|u\|\lambda = 0$, und für $u = 0$ gilt dies ohnehin.

Umgekehrt sei $p \in U$, so dass (7.1.6) gilt. Ist $q \in U$, so gilt $p - q \in U$ und daher $B(x-p, p-q) = 0$. Mit Pythagoras folgt, dass

$$\|x-q\|^2 = \|(x-p) + (p-q)\|^2 = \|x-p\|^2 + \|p-q\|^2 \geq \|x-p\|^2,$$

und daher $p = \pi_U(x)$.

(iii) und (iv) folgen unmittelbar aus (ii) (Übung!).

(v) Für alle $u \in U$ gilt $\pi_U(u) = u$. Mit (iii) folgt daraus, dass $\mathrm{Bild}(\pi_U^2) \subseteq \mathrm{Bild}(\pi_U) = U \subseteq \mathrm{Bild}(\pi_U^2)$ und daher $\mathrm{Bild}(\Phi_U) = \mathrm{Bild}(\Phi_U^2) = \mathrm{Bild}_\infty(\Phi_U)$ und daher $\ker_\infty(\Phi_U) = \ker(\Phi_U)$. Deshalb ist die Fitting-Zerlegung von π_U durch $V = \mathrm{Bild}(\Phi_U) \oplus \ker(\Phi_U) = U \oplus U^\perp$ gegeben. Die letzte Aussage folgt dann aus der Tatsache, dass $\pi_U(u) = u$ für alle $u \in U$ und $\pi_U(v) = 0$ für alle $v \in U^\perp$. □

Bemerkung 7.1.29 (Komplemente)**.** In der Linearen Algebra I haben wir großen Wert darauf gelegt, dass ein Unterraum U eines Vektorraums V zwar stets ein Komplement besitzt, dass dieses aber im Allgemeinen hochgradig uneindeutig ist. In *euklidischen* Vektorräumen[2] ist die Situation eine andere: Hier besitzt jeder Unterraum U ein *kanonisches* Komplement, nämlich $U^\perp$. Man nennt dieses auch das *orthogonale Komplement* zu U. Insbesondere gilt stets

$$U \cap U^\perp = \{0\} \quad \text{und} \quad \dim U^\perp = \dim V - \dim U. \tag{7.1.7}$$

Das orthogonale Komplement einer Ebene bzw. Gerade im $\mathbb{R}^3$ ist also eine Gerade bzw. Ebene. Die Dimensionsformel impliziert auch, dass $\dim(U^\perp)^\perp = \dim U$ gilt. Da offensichtlich stets die Inklusion $U \subseteq (U^\perp)^\perp$ gilt, folgt damit

$$(U^\perp)^\perp = U. \tag{7.1.8}$$

[2] In der Schule haben Sie vermutlich immer stillschweigend in euklidischen Vektorräumen gearbeitet, und daher waren Sie gewohnt, dass Unterräume kanonische Komplemente haben.

Bemerkung 7.1.30. Nach Proposition 3.5.13 ist die Orthogonalprojektion $\pi = \pi_U$ der eindeutige Endomorphismus π von V mit $\pi^2 = \pi$, $\ker(\pi) = U^\perp$ und $\mathrm{Bild}(\pi) = U$. Weiterhin gilt

$$\pi_U + \pi_{U^\perp} = \mathrm{Id}. \tag{7.1.9}$$

Beispiel 7.1.31 (Projektion auf eine Gerade)**.** Sei $U < V$ eine Gerade mit Richtungsektor $v \in V \setminus \{0\}$, also $U = \mathbb{R}v$. Sei $x \in V$ mit i $y := \pi_{U^\perp}(x)$ und $\lambda \in \mathbb{R}$ mit $\pi_U(x) = \lambda v$. Nach (7.1.9) gilt dann $x = \lambda v + y$, und daher

$$B(x,v) = B(\lambda v + y, v) = \lambda B(v,v) + B(y,v) = \lambda B(v,v).$$

Dies zeigt, dass

$$\pi_U(x) = \lambda x = \frac{B(x,v)}{B(v,v)} v \quad \text{und daher} \quad \pi_U^\perp(x) = x - \frac{B(x,v)}{B(v,v)} v. \tag{7.1.10}$$

Insbesondere gilt stets

$$v \perp \left(x - \frac{B(x,v)}{B(v,v)} v \right).$$

Man kann also erreichen, dass ein gegebener Vektor senkrecht auf v steht, indem man ein passendes Vielfaches von v abzieht.

Mittels Orthogonalprojektionen können wir nun Skalarprodukte „diagonalisieren“:

Definition 7.1.32. Eine geordnete Basis $\mathscr{B} = (v_1, \ldots, v_n)$ von V heißt eine *Orthogonalbasis* (OGB), falls $v_i \perp v_j$ für alle $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt. Sie heißt eine *Orthonormalbasis* (ONB), falls zusätzlich $\|v_i\| = 1$ für alle $i \in \{1, \ldots, n\}$ gilt.

Orthonormalbasen bzgl. des Standardskalarprodukts im $\mathbb{R}^n$ korrespondieren zu den aus der Schule bekannten *kartesischen Koordinatensystemen*, d.h. die zugehörigen Koordinatenachsen $\mathbb{K}v_1$ stehen paarweise senkrecht aufeinander und die Koordinatenmarkierungen auf den Achsen sind auf Länge 1 skaliert.

Beispiel 7.1.33. Die Standardbasis ist eine ONB für das Standardskalarprodukt auf $\mathbb{R}^n$. Diese ist aber nicht die einzige solche ONB. Eine andere ONB für $(\mathbb{R}^2, B_0)$ ist z.B. gegeben durch

$$\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right).$$

Bemerkung 7.1.34. Nach Definition ist $\mathscr{B}$ genau dann eine OGB für B, wenn $D_{\mathscr{B}}(B)$ diagonal ist und genau dann eine ONB, wenn $D_{\mathscr{B}}(B) = \mathbf{1}$ gilt. Die Existenz einer ONB ist daher äquivalent zur Existenz eines Basiswechsels, der die darstellende Matrix von B in die Einheitsmatrix überführt.

Satz 7.1.35 (Orthonormalbasen für Skalarprodukte)**.** *Jeder endlichdimensionale euklidische Vektorraum besitzt eine Orthonormalbasis.*

In Matrizensprache können wir den Satz so formulieren:

Korollar 7.1.36. *Eine Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann positiv-definit und symmetrisch, wenn sie kongruent zur Einheitsmatrix ist, also $A = P^\top P$ für ein $P \in \mathrm{GL}_n(\mathbb{R})$.*

Wir wenden uns nun dem Beweis von Satz 7.1.35 zu. Ist $(v_1, \ldots, v_n)$ eine OGB, so ist offensichtlich $(v_1/\|v_1\|, \ldots, v_n/\|v_n\|)$ eine ONB. Es genügt also, eine OGB zu konstruieren. Wir verwenden dabei die folgende Übung:

Übung 7.1.37. Zeigen Sie: Sind Vektoren $v_1,\dots,v_k$ paarweise orthogonal (d.h. gilt $v_i \perp v_j$ für alle $i,j \in \{1,\dots,k\}$ mit $i \neq j$), so sind sie linear unabhängig.

Konstruktion 7.1.38 (Gram-Schmidt-Orthogonalisierung[3])**.** Wir starten dazu mit einer beliebigen geordneten Basis $\mathscr{B} = (v_1,\dots,v_n)$ von V und konstruieren nach und nach paarweise orthogonale Vektoren $(w_1,\dots,w_n)$, so dass $\langle v_1,\dots,v_k\rangle = \langle w_1,\dots,w_k\rangle$ für alle $k \in \{1,\dots,n\}$.

- Wir setzen $w_1 := v_1$. Offensichtlich ist dann $U_1 := \mathbb{R}w_1 = \mathbb{R}v_1$.
- Wir setzen $w_2 := \pi_{U_1^\perp}(v_2) = v_2 - \frac{B(v_2,w_1)}{B(w_1,w_1)}w_1$. Nach Konstruktion ist dann $w_2 \perp w_1$ (insbesondere sind w_1 und w_2 dann linear unabhängig!) und es gilt $\langle w_1,w_2\rangle \subseteq \langle v_1,v_2\rangle$. Aus Dimensionsgründen gilt dann sogar Gleichheit.
- Es sei nun $V_2 := U_1^\perp$. Durch Einschränkung von B erhalten wir ein Skalarprodukt B_1 auf V_2, und wir setzen $U_2 := \mathbb{R}w_2 < V_2$. Wir können nun w_3 zuerst auf V_2 projizieren, also

  $$v_3' := \pi_{V_2}(v_3) = v_3 - \frac{B(v_3,w_1)}{B(w_1,w_1)}w_1,$$

  und dann innerhalb von V_2 auf $U_2^\perp$, also

  $$w_3 := \pi_{U_2^\perp}(v_3') = v_3' - \frac{B(v_3',w_2)}{B(w_2,w_2)}w_2 = v_3 - \frac{B(v_3,w_1)}{B(w_1,w_1)}w_1 - \frac{B(v_3,w_2)}{B(w_2,w_2)}w_2.$$

  Es gilt dann $w_3 \perp w_1$ und $w_3 \perp w_2$ nach Konstruktion, sowie $w_3 \in \langle w_1,w_2,v_3\rangle = \langle v_1,v_2,v_3\rangle$. Aus Dimensionsgründen folgt wieder $\langle v_1,v_2,v_3\rangle = \langle w_1,w_2,w_3\rangle$.
- Induktiv definiert man nun $w_4,\dots,w_n$ durch

  $$w_k := v_k - \sum_{j=1}^{k-1} \frac{B(v_k,w_j)}{B(w_j,w_j)}w_j.$$

  Es gilt dann $w_i \perp w_j$ für alle $i,j \in \{1,\dots,n\}$ mit $i \neq j$ und $\langle v_1,\dots,v_k\rangle = \langle w_1,\dots,w_k\rangle$ für alle $k \in \{1,\dots,n\}$.

Damit ist Satz 7.1.35 bewiesen. Die Konstruktion liefert sogar noch etwas mehr:

Korollar 7.1.39. *Jede ONB eines Unterraums $U < V$ lässt sich zu einer ONB von V fortsetzen.*

Beweis. Man ergänzt eine ONB von U zu einer Basis von V und wendet dann auf die resultierende Basis das Gram–Schmidt-Verfahren an. Die bereits orthonormalen Vektoren aus U ändern sich dabei nicht! □

Beispiel 7.1.40. Wir betrachten den drei-dimensionalen Unterraum V des $\mathbb{R}^4$, der von den Vektoren

$$v_1 := \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \quad v_2 := \begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \quad \text{und} \quad v_3 := \begin{pmatrix}0\\1\\0\\1\end{pmatrix},$$

[3] nach Jørgen Pedersen Gram (1850- 1916), dän. Mathematiker und Erhard Schmidt (1877-1959), dt. Mathematiker

aufgespannt wird. Wir wollen eine OGB von V bzgl. der Einschränkung des Standardskalarprodukts auf V bestimmen. Dazu berechnen wir in der Notation von Konstruktion 7.1.38 die Vektoren w_1, w_2 und w_3. Es ist $w_1 := v_1$ und

$$w_2 = v_2 - \frac{B(v_2,w_1)}{B(w_1,w_1)}w_1 = \begin{pmatrix}1\\0\\1\\0\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1/2\\-1/2\\1\\0\end{pmatrix}.$$

Aus rechenpraktischer Sicht ist es vermutlich einfacher, wenn man den Vektor w_2 durch den Vektor $w_2' := 2w_2$ ersetzt. (Multiplizieren mit Elementen aus $\mathbb{K}^\times$ ändert ja nichts an der linearen Hülle, und auch nichts an Orthogonalität.) Wir erhalten dann

$$w_3 = v_3 - \frac{B(v_3,w_1)}{B(w_1,w_1)}w_1 - \frac{B(v_3,w_2')}{B(w_2',w_2')}w_2' = \begin{pmatrix}0\\1\\0\\1\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\1\\0\\0\end{pmatrix} - \frac{(-1)}{6}\begin{pmatrix}1\\-1\\2\\0\end{pmatrix} = \begin{pmatrix}-1/3\\1/3\\1/3\\1\end{pmatrix},$$

und wiederum ist $w_3' := 3w_3$ etwas schöner anzusehen. Wir erhalten also als zwei mögliche OGB z.B. (w_1,w_2,w_3) und (w_1,w_2',w_3'). In dem wir die Vektoren passend normieren, erhalten wir daraus (falls gewünscht) eine ONB, nämlich

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \quad \frac{1}{\sqrt{6}}\begin{pmatrix}1\\-1\\2\\0\end{pmatrix}, \quad \frac{1}{2\sqrt{3}}\begin{pmatrix}-1\\1\\1\\3\end{pmatrix}.$$

Bemerkung 7.1.41 (Beschleunigtes Gram–Schmidt-Verfahren)**.** Wollen wir zu einem gegebenen Skalarprodukt eine ONB bestimmen, so können wir erst wie oben eine OGB $(u_1,\dots,u_n)$ bestimmen, und dann abschließend jeden der Vektoren u_j durch

$$u_j' := \frac{u_j}{\sqrt{B(u_j,u_j)}}$$

ersetzen. Man erspart sich Rechenaufwand, wenn man den Vektor u_j' immer sofort ausrechnet, sobald man den Vektor u_j bestimmt hat, und dann mit u_j' statt u_j weiterrechnet. in diesem Fall ist nämlich stets $B(u_j',u_j') = 1$, und man spart sich Nenner. Der Nachteil an diesem beschleunigten Gram–Schmidt-Verfahren ist, dass die Zahlen u.U. hässlicher werden, weil man sich Wurzeln einhandelt. Das beschleunigte Verfahren hat insbesondere Vorteile, wenn man es am Computer implementiert. Beim Rechnen von Hand empfiehlt es sich eher die Vektoren u_j durch Vielfache mit einfachen Zahlenwerten zu ersetzen, und erst am Ende zu normieren.

[10.05.24]

Bemerkung 7.1.42 (ONB vs. Standardbasis)**.** Es sei $(v_1,\dots,v_n)$ eine ONB von (V,B). Dann existiert ein eindeutiger Vektorraumisomorphismus $\Phi : V \to \mathbb{R}^n$, der v_j auf den $j$ten Standardbasisvektor abbildet. Es gilt dann

$$B(v_i,v_j) = \delta_{ij} = B_0(e_i,e_j) = B_0(\Phi(e_i),\Phi(e_j)),$$

In diesem Sinne liefert Φ also einen längen- und winkeltreuen Isomorphismus $(V,B) \to (\mathbb{R}^n,B_0)$. Es gibt also bis auf Isomorphie (in diesem Sinne) nur einen euklidischen Vektorraum der Dimension n und bis auf Kongruenz nur eine positiv-definite symmetrische reelle $(n \times n)$-Matrix. Alle aus $(\mathbb{R}^n,B_0)$ bekannten Rechenregeln übertragen sich daher auf beliebige euklidische Vektorräume. Wir führen das an ein paar Beispielen vor.

Lemma 7.1.43 (Abstrakte Fourierentwicklung)**.** *Es sei $(v_1,\dots,v_n)$ eine ONB von (V,B). Für alle $x \in V$ gilt dann die Formel*

$$x = \sum_{j=1}^{n} B(x,v_j)v_j.$$

Beweis. Ist $(v_1^*,\dots,v_n^*)$ die duale Basis von $(v_1,\dots,v_n)$, so gilt

$$B(x,v_k) = B\left(\sum_{j=1}^{n} v_j^*(x)v_j, v_k\right) = \sum_{j=1}^{n} v_j^*(x)B\left(v_j,v_k\right) = v_k^*(x). \qquad \square$$

Korollar 7.1.44 (Abstrakte Plancherel-Formel)**.** *Es sei $(v_1,\dots,v_n)$ eine ONB von (V,B). Für alle $x,y \in V$ gilt dann die Formel*

$$B(x,y) = \sum_{j=1}^{n} B(x,v_j)B(v_j,y).$$

Speziell gilt

$$\|x\|^2 = \sum_{j=1}^{n} B(x,v_j)^2$$

Beweis. Man setze für x die abstrakte Fourier-Entwicklung aus Lemma 7.1.43 ein. $\square$

Korollar 7.1.45 (Formel für Orthogonalprojektion)**.** *Es sei $U \leq V$ ein Unterraum und $(u_1,\dots,u_k)$ eine ONB von U. Dann gilt $\pi_U = \pi$, wobei*

$$\pi(x) = \sum_{j=1}^{k} B(x,u_j)u_j.$$

Beweis. Die Abbildung π ist offensichtlich linear, und ist $v \in U^\perp$, so gilt $\pi(v) = 0$. Ist hingegen $v \in U$ so gilt $\pi(v) = v$ nach Lemma 7.1.43. Dies impliziert, dass $\pi = \pi_U^{U^\perp} = \pi_U$. $\square$

Zum Abschluss dieses Abschnitts über euklidische Vektorräume betrachten wir noch die Frage nach den "natürlichen Symmetrien" solcher Vektorräume.

Bemerkung 7.1.46. Es sei (X,d) ein metrischer Raum, d.h. X ist eine Menge und $d : X \times X \to \mathbb{R}_{\geq 0}$ ist eine Metrik. Eine Abbildung $f : X \to X$ heißt *längentreu*, falls $d(f(x),f(y)) = d(x,y)$ für alle $x,y \in X$ gilt. Eine solche Abbildung ist automatisch injektiv, denn ist $f(x) = f(y)$, so folgt $d(x,y) = d(f(x),f(y)) = 0$ und daher $x = y$. Eine surjektive (und daher bijektive) längentreue Abbildung bezeichnet man als *Isometrie*. Die Isometrien eines metrischen Raumes bilden eine Gruppe (Übung!), die man mit $\mathrm{Is}(X,d)$ bezeichnet.

Beispiel 7.1.47. Es sei (V,B) ein euklidischer Vektorraum und (V,d) der zugehörige metrische Raum.

(i) Da die Metrix d translationsinvariant ist, ist für jedes $v \in V$ die *Translation* $T_v : V \to V$, $w \mapsto v+w$ eine Isometrie.

(ii) Ist $\Phi \in \mathrm{O}(V,B)$ orthogonal, so ist Φ eine Isometrie, denn für $v,w \in V$ gilt

$$d(\Phi(v),\Phi(w)) = B(\Phi(v)-\Phi(w),\Phi(v)-\Phi(w))^{\frac{1}{2}} = B(\Phi(v-w),\Phi(v-w))^{\frac{1}{2}} = B(v-w,v-w)^{\frac{1}{2}} = d(v,w).$$

Diese hat die Zusatzeigenschaft, dass sie linear ist und daher insbesondere die 0 auf die 0 abbildet.

(iii) Da die Verkettung von Isometrien wieder eine Isometrie ist, können wir beide Beispiele kombinieren. Die Menge

$$\mathrm{Mot}(V,B) := \{f : \mathbb{R}^n \to \mathbb{R}^n \mid f(x) = \Phi(x) + v \text{ mit } \Phi \in \mathrm{O}(V,B) \text{ und } v \in \mathbb{R}^n\}.$$

ist daher eine Teilmenge von $\mathrm{Is}(V,d)$ und sogar eine Untergruppe (Übung!). Sie heißt die *Gruppe der euklidischen Bewegungen* (engl. „Euclidean motions“) von (V,B).

Etwas überraschend stellt sich heraus, das die euklidischen Bewegungen die einzigen Isometrien euklidischer Vektorräume sind. Wir beweisen dies in zwei Schritten:

Satz 7.1.48. *Für eine Abbildung $f : V \to V$ sind die folgenden Aussagen äquivalent:*

(i) $f \in \mathrm{O}(V,B)$*, d.h.* f *ist eine* lineare *Isometrie.*

(ii) f *ist eine Isometrie und* $f(0) = 0$*.*

(iii) f *ist längenerhaltend und* $f(0) = 0$*.*

(iv) Für alle $x,y \in V$ *gilt* $B(f(x),f(y)) = B(x,y)$*.*

Insbesondere ist jede längenerhaltende Abbildung mit $f(0) = 0$ *linear und surjektiv.*

Beweis. Die Implikationen (i)⇒(ii)⇒(iii) folgen aus Beispiel 7.1.47 und der Definition.

(iii)⇒(iv): Sei f längenerhaltend mit $f(0) = 0$. Dann gilt für alle $x,y \in V$:

$$\begin{aligned} d(f(x),f(y))^2 &= B(f(x)-f(y),f(x)-f(y)) = \|f(x)\|^2 - 2B(f(x),f(y)) + \|f(y)\|^2 \\ &= d(f(x),0)^2 - 2B(f(x),f(y)) + d(f(y),0)^2 \\ &= d(f(x),f(0))^2 - 2B(f(x),f(y)) + d(f(y),f(0))^2 \\ &= d(x,0)^2 - 2B(f(x),f(y)) + d(y,0)^2 = \|x\|^2 - 2B(f(x),f(y)) + \|y\|^2. \end{aligned}$$

Da f längenerhaltend ist, folgt

$$\begin{aligned} 0 &= d(f(x),f(y))^2 - d(x,y)^2 = (\|x\|^2 - 2B(f(x),f(y)) + \|y\|^2) - B(x-y,x-y) \\ &= -2(B(f(x),f(y)) - B(x,y)), \end{aligned}$$

und daher $B(f(x),f(y)) = B(x,y)$.

(iv)⇒(i): Da f nach Annahme das Skalarprodukt erhält, bleibt nur noch zu zeigen, dass f linear und bijektiv ist. Seien also $v,w \in V$ und $\lambda \in V$.

Sei zunächst $z := f(v+w) - f(v) - f(w) \in \langle \text{Bild}(f) \rangle$; dann gilt für alle $u \in V$, dass

$$B(z, f(u)) = B(f(v+w), f(u)) - B(f(v), f(u)) - B(f(w), f(u)) = B(v+w, u) - B(v, u) - B(w, u) = 0,$$

also $z \in \text{Bild}(f)^\perp = \langle \text{Bild}(f) \rangle^\perp$. Es ist also $z \in \langle \text{Bild}(f) \rangle \cap \langle \text{Bild}(f) \rangle^\perp$. Dies impliziert $B(z,z) = 0$, und folglich $z = 0$, also $f(v+w) = f(v) + f(w)$.

Analog sei nun $z := f(\lambda v) - \lambda f(v) \in \langle \text{Bild}(f) \rangle$. Für $u \in V$ gilt dann

$$B(z, f(u)) = B(f(\lambda v), f(u)) - \lambda B(f(v), f(u)) = 0,$$

und daher wiederum $z = 0$, also $f(\lambda v) = \lambda f(v)$. Daher ist f linear. Da f längenerhaltend ist, ist f injektiv, und dann aus Dimensionsgründen auch surjektiv. □

Korollar 7.1.49 (Klassifikation der euklidischen Isometrien)**.** *Jede längentreue Selbstabbildung eines euklidischen Vektorraums ist eine euklidische Bewegung, insbesondere surjektiv, winkeltreu und volumenerhaltend.*

Beweis. Es sei $f : V \to V$ längentreu und $v := f(0)$. Definieren wir $f_0 : V \to V$ durch $f_0(x) := f(x) - v$, so ist f_0 ebenfalls längentreu (nach Beispiel 7.1.47), aber nun gilt auch $f_0(0) = v - v = 0$. Nach Satz 7.1.48 ist f_0 daher orthogonal, und es gilt $f(v) = f_0(v) + v$. □

Beispiel 7.1.50. In den Übungen haben Sie gezeigt, dass die Elemente von $\mathrm{O}(\mathbb{R}^2, B_0)$ genau die Drehungen um 0 und Spiegelungen an Ursprungsgeraden sind. Jede euklidischen Isometrien der Ebene lässt sich also schreiben als Drehung oder Spiegelung gefolgt von einer Translation.

Bemerkung 7.1.51 (Komplexe Skalarprodukte?)**.** Kann man auch auf komplexen Vektorräumen mittels eines Skalarprodukts einen Abstands- und Winkelbegriff einführen? Das hängt davon ab, was man in diesem Fall unter einem Skalarprodukt verstehen will! Naiv könnte man ein Skalarprodukt auf $\mathbb{C}^n$ als eine symmetrische Bilinearform B definieren, die der Bedingung $B(v,v) > 0$ für all $v \in \mathbb{C}^n \setminus \{0\}$ genügt. Leider funktioniert das nicht! Ist nämlich $v \in \mathbb{C}^n \setminus \{0\}$, so gilt

$$B(iv, iv) = iB(v, iv) = i^2 B(v,v) = -B(v,v),$$

also können $B(v,v)$ und $B(iv,iv)$ nicht beide positiv sein. Um trotzdem Geometrie über den komplexen Zahlen machen zu können, müssen wir die Bedingung der Bilinearität aufweichen. Betrachten wir als Beispiel $\mathbb{C}^1$. Die euklidische Länge eines Vektors $z = x + iy \in \mathbb{C}$ sollte gegeben sein durch

$$\|z\| = \sqrt{x^2 + y^2} = \sqrt{(x+iy)(x-iy)} = \sqrt{z\overline{z}}.$$

Dies motiviert die Definition des Standardskalarprodukts in $\mathbb{C}^n$ mittels

$$B_0 : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{R}, \quad (v,w) \mapsto B_0(v,w) := v^\top \overline{w} = \sum_{i=1}^{n} v_i \overline{w_i}.$$

Dieses hat nun die gewünschte Positivitätseigenschaft $B(v,v) \in (0,\infty)$ für alle $v \in \mathbb{C}^n$, ist aber weder bilinear noch symmetrisch. Es gilt stattdessen für $u, v, w \in \mathbb{C}^n$ und $\lambda \in \mathbb{K}$:

$$B_0(u+v, w) = B_0(u,w) + B_0(v,w), \quad B_0(\lambda v, w) = \lambda B_0(v,w), \tag{7.1.11}$$

$$B_0(v, u+w) = B_0(v,u) + B_0(v,w), \quad B_0(v, \lambda w) = \overline{\lambda} B_0(v,w), \tag{7.1.12}$$

$$B_0(v,w) = \overline{B_0(w,v)}. \tag{7.1.13}$$

Definition 7.1.52. Es sei $\mathbb{K}$ ein Körper, $\sigma : \mathbb{K} \to \mathbb{K}$ ein Körperautomorphismus der Ordnung ≤ 2 (also die Identität oder eine Involution) und V ein $\mathbb{K}$-Vektorraum.

(i) $\Phi : V \to \mathbb{K}$ heißt *σ-Semilinearform*[4], falls $\Phi(v+w) = \Phi(v) + \Phi(w)$ und $\Phi(\lambda v) = \sigma(\lambda)\Phi(v)$ für

[4] lat. semi = halb

alle $v,w \in V$ und $\lambda \in \mathbb{K}$.

(ii) $B : V \times V \to \mathbb{K}$ heißt *σ-Sesquilinearform*[5], falls für $v \in V$ die Abbildung $w \mapsto B(v,w)$ σ-semilinear und die Abbildung $w \mapsto B(w,v)$ linear ist, d.h. für $u,v,w \in V$ und $\lambda \in \mathbb{K}$ gilt

$$B(u+v,w) = B(u,w) + B(v,w), \quad B(\lambda v,w) = \lambda B(v,w),$$
$$B(v,u+w) = B(v,u) + B(v,w), \quad B(v,\lambda w) = \sigma(\lambda) B(v,w).$$

(iii) Eine σ-Sesquilinearform $B : V \times V \to \mathbb{K}$ heißt *hermitesch*[6] (bzw. *schief-hermitesch*), falls

$$B(v,w) = \sigma(B(w,v)) \quad (\text{bzw. } B(v,w) = -\sigma(B(w,v))) \quad \text{für alle } v,w \in V.$$

(iv) $\mathbb{K} = \mathbb{C}$ und σ die komplexen Konjugation, so heißt eine hermitsche Sesquilinearform $B : V \times V \to \mathbb{K}$ ein *komplexes Skalarprodukt*, wenn B *positiv-definit* ist, d.h.

$$B(v,v) \in (0,\infty) \quad \text{für alle } v \in V \setminus \{0\}.$$

In diesem Fall heißt das Paar (V,B) ein *unitärer Vektorraum*.

Nach Bemerkung 7.1.51 ist das Standardskalarprodukt auf $\mathbb{C}^n$ ein komplexes Skalarprodukt. Wie im reellen Fall definiert man auch auf einem unitären Vektorraum (V,B) die *Norm* bzw. *Metrik* durch

$$\|z\| := \sqrt{B(z,z)} \quad \text{und} \quad d(w,z) := \|w - z\|.$$

Wenn man das Rechnen mit reellen Skalarprodukten gewöhnt ist, dann muss man sich im Komplexen etwas umgewöhnen. Zur Übung beweise man die binomischen Formeln

$$\|w \pm z\|^2 = \|w\|^2 \pm 2\mathrm{Re}(B(w,z)) + \|z\|^2 \quad \text{und} \quad B(w+z,w-z) = \|w\|^2 - \|z\|^2 - 2i\,\mathrm{Im}(B(w,z)).$$

Bemerkung 7.1.53 (Einige Anpassungen)**.** Mit den angepassten binomischen Formeln kann man mit komplexen Skalarprodukten fast so rechnen wie mit reellen. Es gibt aber einige wichtige Unterschiede:

(i) Will man ein komplexes Skalarprodukt B aus der zugehörigen quadratischen Form $q(x) = B(x,x)$ durch *Polarisierung* zurückgewinnen, so braucht man 4 statt 2 Terme, nämlich

$$B(x,y) = \frac{1}{4}\left(q(x+y) - q(x-y) + iq(x+iy) - iq(x-iy)\right)$$

(ii) Die Cauchy–Schwarz-Ungleichung für komplexe Skalarprodukte lautet nun

$$|B(x,y)|^2 \le B(x,x)B(y,y)$$

(mit Gleichheit genau dann wenn x und y linear abhängig sind). Der zusätzliche Betrag ergibt sich aus dem Ansatz

$$0 \le B(x-\lambda y, x-\lambda y) = B(x,x) - \lambda B(y,x) - \overline{\lambda} B(x,y) + |\lambda|^2 B(y,y).$$

[5] lat. sesqui = anderthalb

[6] nach CHARLES HERMITE, frz. Mathematiker, 1822-1901

Man wählt dann wie im reellen Fall $\lambda := B(x,y)/B(y,y)$ und erhält

$$0 \le B(x,x) - \frac{|B(x,y)|^2}{B(y,y)} - \frac{|B(x,y)|^2}{B(y,y)} + \frac{|B(x,y)|^2}{B(y,y)} = B(x,x) - \frac{|B(x,y)|^2}{B(y,y)}.$$

Eine unerfreuliche Konsequenz ist, dass die Winkelformel der euklidischen Geometrie in unitären Vektorräumen nicht wohldefiniert ist, da man keinen Arcuscosinus aus einer komplexen Zahl vom Betrag ≤ 1 ziehen kann. Man kann auf andere Art einen Winkelbegriff einführen, aber wir werden diesen hier nicht brauchen. Unabhängig davon nennen wir komplexe Vektoren x, y nach wie vor *orthogonal*, wenn $B(x,y) = 0$.

(iii) Die Parallelogrammgleichung und der Satz von Pythagoras gelten auch in unitären Vektorräumen, allerdings schlägt die Umkehrung des Pythagoras fehl: Nach der ersten binomischen Formel gilt $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ genau dann, wenn $\mathrm{Re}(B(x,y)) = 0$ gilt. Diese Aussage ist echt schwächer als die Aussage $x \perp y$!

Bemerkung 7.1.54 (Darstellende Matrizen)**.** Es sei B eine Sesquilinearform auf einem komplexen Vektorraum V. Ist $\mathscr{B} = (v_1, \dots, v_n)$ eine geordnete $\mathbb{C}$-Basis von V so definieren wir im reellen Fall die *darstellende Matrix*

$$D_{\mathscr{B}}(B) := (B(v_i, v_j))_{1 \le i,j \le n} \in \mathbb{C}^{n \times n}.$$

Bezeichnen wir mit $\mathrm{Ses}(V)$ die Menge der Sesquilinearformen auf V, so erhalten wir analog zum reellen Fall einen Vektorraumisomorphismus

$$D_{\mathscr{B}} : \mathrm{Ses}(V) \to \mathbb{C}^{n \times n}.$$

Die Formel für die Umkehrabbildung ι^{-1} wird aber etwas komplizierter. Genauer gilt: Ist $D_{\mathscr{B}}(B) = A \in \mathbb{C}^{n \times n}$, so ist

$$B(x,y) \quad = \quad B\left(\sum_{i=1}^n v_i^*(x) v_i, \sum_{j=1}^n v_j^*(y) v_j\right) \quad = \quad \sum_{i=1}^n \sum_{j=1}^n v_i^*(x) \overline{v_j^*(y)} B(v_i, v_j),$$

und daher ist A die eindeutige Matrix, so dass

$$B(x,y) = [x]_{\mathscr{B}}^\top A \overline{[y]}_{\mathscr{B}} \quad (x, y \in V). \tag{7.1.14}$$

Insbesondere ist jede Sesquilinearform auf $\mathbb{C}^n$ von der Form

$$B(x,y) = x^\top A \overline{y}$$

für eine eindeutige Matrix $A \in \mathbb{C}^{n \times n}$ (nämlich die darstellende Matrix bzgl. der Standardbasis). Auch die Basiswechselformel muss entsprechend modifiziert werden: Sind $\mathscr{B}_1$ und $\mathscr{B}_2$ zwei geordnete Bases von V und ist $B : V \times V \to \mathbb{C}$ eine Sesquilinearform, so gilt

$$D_{\mathscr{B}_2}(B) = D_{\mathscr{B}_1, \mathscr{B}_2}(\mathrm{Id})^\top \cdot D_{\mathscr{B}_1}(B) \cdot \overline{D_{\mathscr{B}_1, \mathscr{B}_2}(\mathrm{Id})}. \tag{7.1.15}$$

Darstellende Matrizen A_1, A_2 zu verschiedenen Basen sind also *kongruent* im folgenden Sinne: Es existiert ein $C \in \mathrm{GL}_n(\mathbb{C})$, so dass

$$A_2 = C^\top A_1 \overline{C}.$$

Damit eine Sesquilinearform B mit darstellender Matrix A (bzgl. einer beliebigen Basis) hermitesch ist, muss für alle $x, y \in \mathbb{C}^n$ gelten, dass

$$x^\top A\overline{y} = \overline{y^\top A\overline{x}} = \overline{y}^\top \overline{A}x.$$

Analog zum reellen Fall rechnent man nach, dass

$$\overline{y}^\top \overline{A}x = (\overline{y}^\top \overline{A}x)^\top = x^\top \overline{A}^\top \overline{y}.$$

B ist also genau dann hermitesch, wenn $A = \overline{A}^\top$ gilt. Man nennt eine Matrix mit dieser Eigenschaft daher eine *hermitesche Matrix*. Zur Abkürzung schreibt man häufig[7] $A^* := \overline{A}^\top$. Hermitesche Matrizen sind also Matrizen von der Form $A = A^*$, und eine solche Matrix definiert genau dann ein komplexes Skalarprodukt wenn sie *positiv definit* ist im Sinne von

$$\forall\, x \in \mathbb{C}^n \setminus \{0\} :\ x^\top A\overline{x} > 0.$$

Dies muss dann natürlich auch für $\overline{x}$ gelten, und daher ist die positive Definitheit äquivalent zu

$$\forall\, x \in \mathbb{C}^n \setminus \{0\} :\ x^* Ax > 0. \tag{7.1.16}$$

Bemerkung 7.1.55 (Relle vs. komplexe positive Definitheit)**.** Es sei $A \in \mathbb{R}^{n\times n}$ symmetrisch. Dann können wir A als symmetrische reelle oder als hermitesche komplexe Matrix auffassen. Aufgefasst als reelle Matrix ist A genau dann positiv definit, wenn $x^\top Ax > 0$ für alle $x \in \mathbb{R}^n \setminus \{0\}$. Aufgefasst als komplexe Matrix ist A positiv definit, wenn $z^* Az > 0$ für alle $z \in \mathbb{C}^n \setminus \{0\}$ gilt. Auf den ersten Blick sieht es so aus, als sei diese zweite Bedingung stärker; das ist aber nicht der Fall: Wir können nämlich $z \in \mathbb{C}^n$ schreiben als $z = x + iy$ mit $x, y \in \mathbb{R}^n$. Es gilt dann

$$z^* Az = (x^\top - iy^\top)A(x+iy) = x^\top Ax - iy^\top Ax + ix^\top Ay + y^\top Ay = x^\top Ax + y^\top Ay,$$

und falls $z \neq 0$ (also $x \neq 0$ oder $y \neq 0$), so ist dies positiv.

Der Beweis von Lemma 7.1.56 überträgt sich nun und liefert:

Lemma 7.1.56 (Eigenwert-Kriterium)**.** *Ist $A \in \mathbb{R}^{n\times n}$ symmetrisch und positiv-definit oder $A \in \mathbb{C}^{n\times n}$ hermitesch und positiv-definit, so so gilt* $\operatorname{spec}_{\mathbb{C}}(A) \subseteq (0,\infty) \subseteq \mathbb{R}$*, d.h. alle komplexen Eigenwerte sind reell und positiv. Insbesondere sind* $\det(A)$ *und* $\operatorname{tr}(A)$ *reell und positiv.*

Beweis. Ist $Av = \lambda v$ für ein $\lambda \in \mathbb{C}$ und $v \in \mathbb{C}^n \setminus \{0\}$, so gilt $v^* Av = \lambda v^* v$ und daher

$$\lambda = \frac{v^* Av}{v^* v} \in (0,\infty) \subseteq \mathbb{R}. \qquad \square$$

Wir werden später als eine Anwendung des Spektralsatzes zeigen, dass die Eingewert-Bedingung für positive Definitheit nicht nur notwendig, sondern bereits hinreichend ist.

Bemerkung 7.1.57 (Hauptminoren)**.** Ist (V, B) ein endlichdimensionaler euklidischer oder unitärer Vektorraum und $U < V$ ein Unterraum, so ist auch $B|_{U\times U}$ ein Skalarprodukt. Wählen wir eine Basis von U, so hat daher die zugehörige darstellende Matrix positive reelle Eigenwerte, Spur und Determinante.

[7] Das ist eigentlich eine schlechte Idee, weil der Stern ohnehin schon zu viele Bedeutungen trägt, z.B. im Kontext der dualen und später der adjungierten Abbildung, aber es hat sich leider so eingebürgert.

In Matrizensprache hat dies die folgende Konsequenz: Ist $A = (a_{ij}) \in \mathbb{K}^{n\times n}$ so hat die Einschränkung von B_A auf $\langle e_1,\dots,e_l\rangle$ die darstellende Matrix $(a_{ij})_{1\le i,j\le l}$. Es muss daher gelten, dass

$$H_l^A := \det(a_{ij})_{1\le i,j\le l} > 0 \quad \text{l} = 1, \dots, \text{n}.$$

Die Minoren H_k^A heißen die *Hauptminoren* von A. Ein positiv-definite Matrix hat also positive Hauptminoren.

Beispiel 7.1.58. Die Matrix $A = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}$ ist nicht positiv-definit. Zwar ist ihre Determinante positiv, aber die zweite Hauptminore ist negativ.

Bemerkung 7.1.59 (Komplexe Orthogonalprojektionen)**.** Der Beweis des Hilbertschen Projektionssatzes funktioniert für alle Normen, die die Parallelogrammgleichung erfüllen, also auch für Normen, die von *komplexen* Skalarprodukten kommen. Insbesondere kann man für jeden komplexen Unterraum U eines unitären Vektorraums (V,B) eine Orthogonalprojektion $\pi_U : V \to V$ definieren. Wie im reellen Fall setzen wir dann

$$U^\perp = \{v \in V \mid \forall\, u \in U : B(u,v) = 0\}$$

gilt. Ähnlich wie im reellen Fall zeigt man[8], dass für $x \in V$ dann wie im Reellen $\pi_U(x)$ der eindeutige Punkt in U ist, so dass $x - \pi_U(x) \in U^\perp$ gilt. Daraus folgt dann, wörtlich wie im reellen Fall, dass π_U linear ist, und dass $V = \text{Bild}(\pi_U) \oplus \ker(\pi_U) = U \oplus U^\perp$ gilt. Insbesondere gilt dann $(U^\perp)^\perp = U$ und $\pi_U + \pi_U^\perp = \text{Id}$, und daraus folgt die Projektionsformel (7.1.10) wörtlich wie im Reellen. Auch der Beweis des Gram-Schmidt-Verfahrens überträgt sich wörtlich: Ist $(v_1,\dots,v_n)$ eine Basis von V und definieren wir induktiv

$$w_1 := v_1 \quad \text{und} \quad w_k := v_k - \sum_{j=1}^{k-1} \frac{B(v_3,w_j)}{B(w_j,w_j)} w_j (k = 2,\dots,n),$$

so sind $w_1,\dots,w_n$ paarweise orthogonal und es gilt $\langle v_1,\dots,v_k\rangle = \langle w_1,\dots,w_k\rangle$ für alle $k \in \{1,\dots,n\}$. Insbesondere ist dann $(w_1,\dots,w_n)$ eine OGB, die man durch Normieren zu einer ONB aufwerten kann. Die Beweise von Lemma 7.1.43, Korollar 7.1.44 und Korollar 7.1.45 übertragen sich wörtlich.

Wir halten fest:

Satz 7.1.60 (Orthonormalbases für unitäre Vektorräume)**.** *Es sei (V,B) ein endlichdimensionaler unitärer Vektorraum.*

(i) V besitzt eine ONB bzgl. B, und jede ONB eines Unterraums lässt sich zu einer ONB des gesamten Raums vervollständigen.

[8] Sei $p = \pi_U(x)$ und $u \in U \setminus \{0\}$. Wir setzen wieder $u_0 := u/\|u\|$, so dass $\|u_0\| = 1$, sowie $\lambda := B(p-x,u_0)$ und $q := p - \lambda u_0 \in U$. Es gilt dann

$$\|p-x\|^2 \le \|q-x\|^2 = \|(p-x) - \lambda u_0\|^2 = \|p-x\|^2 - 2\text{Re}(B(p-x,\lambda u_0)) + |\lambda|^2\|u_0\|^2,$$

wobei $B(p-x,\lambda u_0) = \overline{\lambda} B(p-x,u_0) = \overline{\lambda}\lambda = |\lambda|^2$, was bereits reell ist. Dies impliziert, dass

$$0 \le -2\text{Re}(|\lambda|^2) + |\lambda|^2 \cdot 1 \implies |\lambda|^2 = 0 \implies p - x \perp u,$$

und dies gilt auch für $u = 0$. Die umgekehrte Implikation benötigt nur den Pythagoras und funktioniert daher wie im Reellen.

(ii) Ist $(v_1,\dots,v_n)$ *eine ONB von* (V,B)*, so gelten für alle* $x \in V$ *die Formeln*

$$x = \sum_{j=1}^{n} B(x,v_j)v_j \quad \text{und} \quad \|x\|^2 = \sum_{j=1}^{n} |B(x,v_j)|^2.$$

(iii) Ist $(u_1,\dots,u_k)$ *eine ONB eines Unterraums* $U < V$*, so gilt*

$$\pi_U(x) = \sum_{j=1}^{k} B(x,u_j)u_j.$$

Zum Schluss dieses Abschnitts geben wir noch eine überraschende Anwendung von (komplexen) ONBs:

Satz 7.1.61 (Hauptminorenkriterium)**.** *Sei* $A \in \mathbb{R}^{n\times n}$ *symmetrisch oder* $A \in \mathbb{C}^{n\times n}$ *hermitesch. Dann ist A genau dann positiv definit, wenn die Hauptminoren* $H_1^A,\dots,H_n^A$ *reell und positiv sind.*

[15.05.24]

Beweis. Die Notwendigkeit der Bedingung wurde bereits in Bemerkung 7.1.57 eingesehen. Wir nehmen jetzt umgekehrt an, dass die Hauptminoren $H_1^A,\dots,H_n^A$ allesamt reell und positiv sind. Weiter dürfen wir annehmen, dass A eine hermitesche komplexe Matrix ist. Wir zeigen per Induktion nach n, dass A positiv definit ist.

Ist $n=1$, so ist $A=(H_1^A)\in\mathbb{C}^{1\times 1}$ mit $H_1^A>0$, also gilt $z^*Az=H_A^1|z|^2>0$ für alle $z\in\mathbb{C}^1$. Wir nehmen nun an, dass $n\geq 2$ gilt und die Behauptung für $n-1$ bewiesen wurde.

Wir setzen $V:=\langle e_1,\dots,e_{n-1}\rangle<\mathbb{C}^n$. Wir betrachten die Einschränkung von B_A auf V; die darstellende Matrix dieser Sesquilinearform ist $(a_{ij})_{1\leq i,j,\leq n-1}$. Diese ist hermitesch, und ihre Hauptminoren sind $H_1^A,\dots,H_{n-1}^A$, also nach Annahme positiv. Nach Induktionsvoraussetzung ist $B_A|_{V\times V}$ also ein komplexes Skalarprodukt, und es existiert eine ONB $(v_1,\dots,v_{n-1})$ von V. Die darstellende Matrix von B_A bzgl. $(v_1,\dots,v_{n-1},e_n)$ ist dann von der Form

$$A'=\begin{pmatrix}1 & & 0 & *\\ & \ddots & & \vdots\\ 0 & & 1 & *\\ * & \dots & * & *\end{pmatrix}$$

Da A' auch eine darstellende Matrix für B_A ist, genügt es zu zeigen, dass A' positiv definit ist. Da B_A hermitesch ist, ist A' eine hermitesche Matrix, also

$$A'=\begin{pmatrix}1 & & 0 & \overline{b_1}\\ & \ddots & & \vdots\\ 0 & & 1 & \overline{b_{n-1}}\\ b_1 & \dots & b_{n-1} & b_n\end{pmatrix}\quad\text{für gewisse } b_1,\dots,b_{n-1}\in\mathbb{C}, b_n\in\mathbb{R}.$$

Wir setzen nun

$$v_n:=e_n-\sum_{l=1}^{n-1}b_lv_l.$$

Für $j\in\{1,\dots,n-1\}$ gilt dann

$$B_A(v_n,v_j)=B_A(e_n,v_j)-\sum_{j=1}^{n-1}b_lB_A(v_l,v_j)=b_j-\sum_{l=1}^{n-1}b_l\delta_{lj}=0.$$

Es ist also $\mathscr{B}=(v_1,\dots,v_n)$ eine OGB für B_A, und die darstellende Matrix von B_A bzgl. $\mathscr{B}$ ist von der Form

$$A''=\operatorname{diag}(1,\dots,1,\lambda),\quad\text{wobei }\lambda=B_A(v_n,v_n)=\det(A'')$$

Die Matrix A'' ist konjugiert zu A, also existiert ein $P\in\mathrm{GL}_n(\mathbb{C})$ mit $A''=P^\top A\overline{P}$. Es gilt dann

$$\lambda=\det(A'')=\det(P)\det(A)\overline{\det(P)}=|\det(P)|^2H_n^A>0.$$

Setzen wir $v_n':=v_n/\sqrt{\lambda}$, so ist $(v_1,\dots,v_{n-1},v_n')$ eine ONB von B_A. Folglich ist A kongruent zur Einheitsmatrix und daher positiv definit. □

Bemerkung 7.1.62 (Darstellende Matrizen von Skalarprodukten)**.** An dieser Stelle wissen wir zumindest theoretisch, wie sich alle Skalarprodukte auf einem endlichdimensionalen Vektorraum über $\mathbb{R}$ oder $\mathbb{C}$ beschreiben lassen: Nach Wahl einer geordneten Basis entspricht ein Skalarprodukt einer reellen oder komplexen $(n \times n)$-Matrix $A = (a_{ij})$. Die Bedingungen, die diese Matrix erfüllen muss, sind durch explizite Gleichungen und Ungleichungen gegeben: Einerseits muss die Matrix symmetrisch bzw. hermitesch sein (d.h. $a_{ij} = \overline{a_{ji}}$), andererseits müssen gewisse Determinanten von Untermatrizen positiv sein. Für (2×2)-Matrizen kann man diese Bedingungen explizit auflisten: Es muss gelten

$$a_{11} = \overline{a_{11}},\ a_{22} = \overline{a_{22}},\ a_{21} = \overline{a_{12}},\ a_{11} > 0,\ a_{11}a_{22} - a_{12}a_{21} > 0.$$

Das bedeutet gerade, dass

$$A \in \{(a_{ij}) \in \mathbb{C}^{2\times 2} \mid a_{11} \in (0,\infty), a_{12} = \overline{a_{21}} \in \mathbb{C}, a_{22} \in (|a_{12}|^2/a_{11}, \infty)\}.$$

Damit haben wir alle komplexen Skalarprodukte auf $\mathbb{C}^2$ beschrieben. Für große n kann man immer noch Systeme von Gleichungen und Ungleichungen angeben, es wird aber sehr schnell sehr schwierig, solche Systeme explizit zu lösen.

Zusammenfassung von Abschnitt 7.1

(1) Reelle (bzw. komplexe) Skalarprodukte sind spezielle Bilinearformen (bzw. Sesquilinearformen) auf reellen (bzw. komplexen) Vektorräumen, die es erlauben Längen und Abstände (und, im reellen Fall, Winkel) zu definieren. Ein Vektorraum mit einem solchen Skalarprodukt heißt ein euklidischer (bzw. unitärer Vektorraum).

(2) Reelle (bzw. komplexe) Skalarprodukte lassen sich nach Wahl einer Basis durch positivdefinite symmetrische (bzw. hermitesche) Matrizen darstellen. Eine andere Basiswahl liefert eine kongruente Darstellungsmatrix. Positive Definitheit lässt sich mittels des Hauptminoren-Kriteriums überprüfen.

(3) In einem euklidischen oder unitären Vektorraum besitzt jeder Unterraum U ein ausgezeichnetes Komplement, das orthogonale Komplement $U^\perp$. Die Projektion auf U entlang $U^\perp$ (Orthogonalprojektion) bildet jeden Punkt auf den eindeutigen Punkt in U von minimalem Abstand ab.

(4) Jeder endlichdimensionale euklidische oder unitäre Vektorraum besitzt eine ONB, die z.B. mit dem Gram-Schmidt-Verfahren bestimmt werden kann. Die Darstellungsmatrix bzgl. dieser Matrix ist die Einheitsmatrix. In Koordinaten bzgl. einer ONB rechnet man wie mit der Standardbasis (Fourierentwicklung, Plancherel-Formel).

7.2 Orthogonale Zerlegungen

Nach dem wir im letzten Abschnitt reelle und komplexe Skalarprodukte betrachtet haben, wollen wir uns nun allgemeineren Klassen von Bilinearformen bzw. Sesquilinearformen über beliebigen Körpern zuwenden. Historisch gesehen gibt es für diese Verallgemeinerung zwei Motivationen: Das Studium von Bilinearformen über allgemeinen Körpern, insbesondere über den rationalen Zahlen und endlichen Körpern, hat zahlreiche innermathematische Anwendungen

in Algebra, Geometrie und Zahlentheorie. In diesem allgemeinen Kontext macht es natürlich keinen Sinn von „Positivität“ zu reden. Das Studium von reellen Bilinearformen, die entweder nicht symmetrisch oder nicht positiv-definit sind, ist maßgeblich durch Anwendungen in der Physik motiviert: Die Hamiltonsche Formulierung der klassischen Mechanik basiert auf reellen Bilinearformen, die nicht symmetrisch, sondern alternierend nicht. Symmetrische Bilinearformen, die nicht positiv-definit sind, traten in der Physik zuerst in der Relativitätstheorie auf, später auch im Standardmodell der Teilchenphysik.

Beispiel 7.2.1 (Minkowski-Raum)**.** In der speziellen Relativitätstheorie betrachtet man eine 4-dimensionale Raumzeit (modelliert durch den $\mathbb{R}^4$) mit der *Minkowski-Form*

$$B_{3,1} : \mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}, \quad B_{3,1}(v,w) := v_1w_1 + v_2w_2 + v_3w_3 - v_4w_4.$$

Die vierte Koordinate (in der physikalischen Interpretation die „Zeitkoordinate“) verhält sich grundlegend anders als die ersten drei Komponenten (in der physikalischen Interpretation die „Raumkoordinaten“). Allgemeiner definiert man den *Minkowski-Raum* $\mathbb{R}^{n,1}$ als den Vektorraum $\mathbb{R}^{n+1}$ mit der *Minkowski-Form*

$$B_{n,1} : \mathbb{R}^{n+1} \times \mathbb{R}^{n+1} \to \mathbb{R}, \quad B(v,w) := \left(\sum_{i=1}^{n} v_i w_i\right) - v_{n+1}w_{n+1}$$

Diese ist offensichtlich eine symmetrische Bilinearform, aber nicht positiv-definit. In der Relativitätstheorie unterscheidet man zwischen „zeitartigen“ ($B_{n,1}(v,v) < 0$), „lichtartigen“ ($B_{n,1}(v,v) = 0$) und „raumartigen“ ($B_{n,1}(v,v) > 0$) Vektoren v. Für $n = 2$ kann man sich diese Vektoren geometrisch wie folgt vorstellen: Die lichtartigen Vektoren liegen auf einem Doppelkegel („Lichtkegel“) gegeben durch

$$\{v \in \mathbb{R}^3 \mid v_1^2 + v_2^2 = v_3^2\}.$$

Im Inneren des Doppelkegels leben die raumartigen Vektoren, ausserhalb des Kegels die zeitartigen Vektoren.

Das folgende Beispiel spielt in der Theorie der linearen Abbildungen eine wichtige Rolle:

Beispiel 7.2.2 (Spurform)**.** Es sei $\mathbb{K}$ ein Körper und $\sigma : \mathbb{K} \to \mathbb{K}$ ein Körperautomorphismus der Ordnung ≤ 2 (also die Identität oder eine Involution). Wir betrachten den Vektorraum $V := \mathbb{K}^{n\times n}$ der $(n \times n)$-Matrizen über einem Körper $\mathbb{K}$ und setzen σ komponentenweise auf V fort. Die Abbildung $B : V \times V \to \mathbb{K}$ gegeben durch

$$B : V \times V \to \mathbb{K}, \quad (X,Y) \mapsto \operatorname{tr}(X\sigma(Y)),$$

ist dann eine hermitesche σ-Sesquilinearform, genannt die *Spurform* auf $\mathbb{K}^{n\times n}$ bzgl. σ. Linearität in der ersten Variablen folgt unmittelbar aus der Bilinearität der Matrizenmultiplikation und der Linearität der Spur, und dass B hermitesch (und daher semilinear in der zweiten Variable ist) folgt aus der Spuridentität $\operatorname{tr}(XY) = \operatorname{tr}(YX)$.

Für $(K,\sigma) = (\mathbb{R}, \mathrm{Id})$ und $n \geq 2$ ist die Spurform nicht positiv-definit, denn ist X nilpotent, so ist auch X^2 nilpotent und daher gilt $B(X,X) = \operatorname{tr}(X^2) = 0$.

Notation 7.2.3. Ab jetzt sei V ein Vektorraum über einem beliebigen Körper $\mathbb{K}$. Weiter sei $\sigma : \mathbb{K} \to \mathbb{K}$ ein Körperautomorphismus der Ordnung ≤ 2 (also die Identität oder eine Involution) und B eine σ-Sesquilinearform. Wie im Komplexen schreiben wir manchmal $\overline{z} := \sigma(z)$.

Wir nehmen im Folgenden stets an, dass B entweder hermitesch (also $B(v,w) = \sigma(B(w,v))$ für alle $v,w \in V$) oder schief-hermitesch (also $B(v,w) = -\sigma(B(w,v))$) ist. Es gilt dann insbesondere

$$B(v,w) = 0 \iff B(w,v) = 0.$$

Unser jetziges Setting ist zu allgemein, um sinnvoll Längen und/oder Winkel definieren zu können. Wir können aber immer noch über Orthogonalität reden:

Definition 7.2.4. Zwei Vektoren $v,w \in V$ heißen *orthogonal* bzgl. B, falls

$$v \perp w \quad :\iff \quad B(v,w) = 0 \iff B(w,v) = 0.$$

Ein Vektor $v \in V$ heißt *isotrop* bzgl. B, falls $v \perp v$, sonst *anisotrop*. Die Form B heißt *isotrop*, falls ein bzgl. B isotroper Vektor $v \in V \setminus \{0\}$ existiert, sonst *anisotrop*.

Ein Unterraum $U < V$ heißt *total anisotrop*, falls jedes $u \in U \setminus \{0\}$ anisotrop ist, und *total isotrop*[9], falls $B|_{U\times U} = 0$ ist.

Beispiel 7.2.5. (i) Jedes reelle oder komplexe Skalarprodukt ist anisotrop.

(ii) Die Minkowski-Formen sind isotrop, und die isotropen Vektoren sind genau die lichtartigen Vektoren. Geraden durch diese Vektoren sind total isotrope Unterräume, alle anderen Geraden sind total anisotrope Unterräume.

(iii) Es sei nun $\mathbb{K} = \mathbb{R}$ und $\sigma = \mathrm{Id}$.

Wir behaupten, dass in diesem Fall B genau dann anisotrop ist, wenn entweder B oder $-B$ positiv-definit ist.

Falls $\dim V = 1$, so ist dies klar, weil jede Bilinearform $B \neq 0$ positiv- oder negativ-definit ist. Sei nun $\dim V \geq 2$. Ist weder B noch $-B$ positiv definit, so existieren $v,w \in V \setminus \{0\}$ mit $B(v,v) < 0$ und $B(w,w) > 0$, und es existiert eine stetige Funktion $\gamma : [0,1] \to V \setminus \{0\}$ mit $f(0) = v$ und $f(1) = w$. Die Abbildung $f : [0,1] \to \mathbb{R}$, $t \mapsto B(\gamma(t),\gamma(t))$ ist dann stetig mit $f(0) < 0$ und $f(1) > 0$, hat also nach dem Zwischenwertsatz eine Nullstelle t. Das bedeutet aber gerade, dass $\gamma(t)$ ein isotroper Vektor ist!

(iv) Die Bilinearform $B : \mathbb{Q}^2 \times \mathbb{Q}^2 \to \mathbb{Q}$ über $\mathbb{Q}$ gegeben durch $B(v,w) = v_1w_1 - 2v_2w_2$ ist anisotrop. Wäre nämlich $B(v,v) = 0$, also $v_1^2 = 2v_2^2$, und $v \neq 0$, so wäre schon $v_2 \neq 0$ und daher $|v_1/v_2| = \sqrt{2}$ im Widerspruch zur Irrationalität von $\sqrt{2}$. Anders als im Fall von Skalarprodukten ist der Grund für die Anisotropie arithmetisch und hat nichts mit Positivität zu tun.

(v) Wir haben bereits gesehen, dass die Spurform auf $\mathbb{K}^{n\times n}$ für $n \geq 2$ isotrop ist, weil jede nilpotente Matrix ein isotroper Vektor ist. Ist $\mathbb{K}$ ein Unterkörper von $\mathbb{C}$ und σ die Einschränkung der komplexen Konjugation, so sind die isotropen Vektoren sogar *genau* die nilpotenten Matrizen. Zum Beweis dürfen wir annehmen, dass $\mathbb{K} = \mathbb{C}$ gilt; dann hat $A \in \mathbb{C}^{n\times n}$

[9] Manche Bücher über symmetrische Bilinearformen nennen einen Unterraum $U < V$ total isotrop, falls jedes $u \in U$ isotrop ist. Für *symmetrische Bilinearformen über einem Körper der Charakteristik* $\neq 2$ ist das äquivalent zu unserer Definition: Ist $U < V$ total isotrop im Sinne unserer Definition, so ist offensichtlich jedes $u \in U$ isotrop. Ist umgekehrt jeder Vektor isotrop, so gilt

$$0 = B(u+v,u+v) = B(u,u) + 2B(u,v) + B(v,v) = 2B(u,v),$$

und daher ist U total isotrop in unserem Sinne. Im Allgemeinen sind die Definitionen aber nicht äquivalent. Z.B. ist im Falle einer alternierenden Bilinearform jeder Vektor isotrop, aber nicht jeder Unterraum ist total isotrop im Sinne unserer Definition.

komplexe Eigenwerte $\lambda_1,\dots,\lambda_n$ (aufgezählt mit algebraischen Vielfachheiten) und $A\sigma(A)$ hat Eigenwerte $|\lambda_1|^2,\dots,|\lambda_n|^2$. Daher gilt

$$B(A,A) = \operatorname{tr}(A\sigma(A)) = |\lambda_1|^2 + \cdots + |\lambda_n|^2 = 0 \iff \lambda_1 = \cdots = \lambda_n = 0 \iff A \text{ nilpotent.}$$

Die Analogie zwischen nilpotenten Matrizen und lichtartigen Vektoren im Minkowski-Raum hat sich in der modernen Theorie der Matrizen-Algebren als sehr fruchtbar erwiesen.

(vi) Ist B eine *alternierende* Bilinearform, so ist jeder Vektor isotrop. V ist aber trotzdem nicht total isotrop, außer wenn B die Nullform ist.

Definition 7.2.6. Der *Orthogonalraum* zu einem Unterraum $U < V$ ist die Menge

$$U^\perp = \{v \in V \mid \forall\, u \in U : u \perp v\}.$$

Wir im euklidischen oder unitären Fall ist der Orthogonalraum zu einem Unterraum wieder ein Unterraum (Übung!), aber im Allgemeinen ist dieser kein Komplement von U:

Beispiel 7.2.7 (Orthogonalraum einer isotropen Geraden)**.** Im Minkowski-Raum $\mathbb{R}^{2,1}$ betrachten wir die total-isotrope Gerade $U := \langle e_1 + e_3\rangle$. Da $e_1 + e_3$ isotrop ist, gilt $e_1 + e_3 \in U^\perp$. Andererseits ist klar, dass e_2 orthogonal zu $e_1 + e_3$ ist. Andererseits ist $B(e_1, e_1 + e_3) = 1$ und daher $U^\perp \neq \mathbb{R}^{2,1}$. Aus Dimensionsgründen ist daher

$$U^\perp = \langle e_1 + e_3, e_2\rangle$$

eine Ebene, die die Gerade U enthält.

Beispiel 7.2.8. Im letzen Beispiel war der Orthogonalraum von U zwar nicht komplementär zu U, aber er hatte wenigstens die komplementäre Dimension. Auch das ist im Allgemeinen nicht der Fall: Ist B die Nullform, so gilt für jeden Unterraum U, dass $U^\perp = V$. Insbesondere gilt dann $V^\perp = V$.

Definition 7.2.9. Der Orthogonalraum $\operatorname{Rad}(V,B) := V^\perp$ heißt das *Radikal* von (V,B), und B heißt *nicht-ausgeartet*, falls $\operatorname{Rad}(V,B) = \{0\}$.

Proposition 7.2.10 (Nicht-ausgeartete Sesquilinearformen)**.** *Es sei $\mathscr{B}$ eine geordnete Basis von V. Dann sind für eine Sesquilinearform $B : V \times V \to \mathbb{K}$ die folgenden Aussagen äquivalent.*

(i) B ist nicht ausgeartet.

(ii) Für jedes $v \in V \setminus \{0\}$ existiert ein $w \in V$ mit $B(v,w) \neq 0$.

(iii) Die darstellende Matrix $D_{\mathscr{B}}(B)$ ist invertierbar.

Insbesondere hängt (iii) nicht von der Wahl der geordneten Basis ab.

Beweis. (ii) ist nur eine Umformulierung von (i). Wir zeigen (ii)⇔(iii) durch Kontraposition.

Es sei zunächst $\sigma = \mathrm{Id}$ angenommen. Dann entspricht die Bilinearform B einer linearen Abbildung $\Phi_B : V \to V^*$ gegeben durch $\Phi_B(v)(w) = B(v,w)$ und nach Übung 7.1.17) ist $D_{\mathscr{B}}(B) = D_{\mathscr{B}^*,\mathscr{B}}(\Phi_B)$. Diese Matrix ist also genau dann nicht invertierbar für eine (beliebige) geordnete Basis $\mathscr{B}$, wenn $\ker(\Phi_B) \neq \{0\}$ gilt. Nun gilt aber

$$v \in \ker(\Phi_B) \iff \Phi_B(v) = 0 \iff \forall\, w \in V : \Phi_B(v)(w) = 0 \iff \forall\, w \in V : B(v,w) = 0.$$

Daher ist ¬ (iii) äquivalent zu ¬ (ii).

Ist σ eine nicht-triviale Involution, so argumentiert man im Prinzip genauso. Die Abbildungen $\Phi_B(v): V \to \mathbb{K}$, $w \mapsto B(v,w)$ sind allerdings jetzt nicht linear, sondern σ-semilinear. Definiert man nun den Semidualraum $\overline{V}^* := \{f : V \to \mathbb{K} \mid f \text{ ist } \sigma\text{-semilinear}\}$, so korrespondiert B zu einer Abbildung $\Phi_B : V \to \overline{V}^*$. Man argumentiert dann wie im ersten Fall, nur dass man überall V^* durch $\overline{V}^*$ ersetzt und die folgende Übung verwendet. □

Übung 7.2.11. Es sei $(v_1,\dots,v_n)$ eine geordnete Basis von V. Wir betrachten den *Semidualraum* $\overline{V}^* := \{f : V \to \mathbb{K} \mid f \text{ ist } \sigma\text{-semilinear}\}$. Zeigen Sie:

(i) Für $k \in \{1,\dots,n\}$ existiert ein eindeutiges $\overline{v}_k^* \in \overline{V}^*$, so dass

$$\forall\, \lambda_1,\dots,\lambda_n \in \mathbb{K} : \overline{v}_k^*\left(\sum_{j=1}^{n} \lambda_j v_j\right) = \sigma(\lambda_k).$$

(ii) $(\overline{v}_1^*,\dots,\overline{v}_n^*)$ ist eine Basis von $\overline{V}^*$ (genannt die *semiduale Basis* zu $(v_1,\dots,v_n)$). Insbesondere gilt $\dim \overline{V}^* = \dim V$ und jede injektive lineare Abbildung $V \to \overline{V}^*$ ist bijektiv.

(iii) Ist $U < V$ ein Unterraum, so ist die Abbildung $\mathrm{res}_U : \overline{V}^* \to \overline{U}^*$, $f \mapsto f|_U$ surjektiv.

Satz 7.2.12 (Dimensionsformel für Orthogonalräume)**.** *Ist B nicht-ausgeartet und $U \le V$ ein Unterraum, so gilt*

$$\dim V = \dim U + \dim U^\perp \quad \text{und} \quad (U^\perp)^\perp = U.$$

Beweis. Wie im Beweis von Proposition 7.2.10 betrachten wir wieder die lineare Abbildung $\Phi_B : V \to \overline{V}^*$, $\Phi_B(v)(w) = B(v,w)$. Da B nicht-ausgeartet ist, ist diese Abbildung bijektiv. Nach Übung 7.2.11 ist daher die Abbildung

$$\rho := \mathrm{res}_U \circ \Phi_B : V \to \overline{U}^*, \quad \rho(v)(u) := B(v,u)$$

surjektiv. Nun ist aber

$$\ker(\rho) = \{v \in V \mid \forall\, u \in U : B(v,u) = 0\} = U^\perp,$$

und daher nach der Rang-Defekt-Formel

$$\dim V = \dim \mathrm{Bild}(\rho) + \dim \ker(\rho) = \dim \overline{U}^* + \dim U^\perp = \dim U + \dim U^\perp.$$

Zweimaliges Anwenden liefert $\dim(U^\perp)^\perp = \dim U$, und da nach Definition stets $U \subseteq (U^\perp)^\perp$ gilt, folgt die Behauptung. □

Bemerkung 7.2.13. Falls B ausgeartet ist, so kann man mit einer (etwas komplizierteren) Variante dieses Arguments zeigen, dass für jeden Unterraum $U < V$ die Formel

$$\dim V = \dim U + \dim U^\perp - \dim(U \cap V^\perp).$$

gilt. Wir werden diese Formel aber hier nicht benötigen (und daher auch nicht beweisen).

Korollar 7.2.14. *Es sei B nicht-ausgeartet.*

(i) Ist $U < V$ ein Unterraum, so gilt

$$U \cap U^\perp = \{0\} \iff V = U \oplus U^\perp \iff V = U + U^\perp.$$

(ii) Ist $U < V$ total isotrop, so gilt $\dim U \leq (\dim V)/2$.

Beweis. (i) Ist $U \cap U^\perp = \{0\}$, so ist die Summe $U \oplus U^\perp$ direkt. Mit Satz 7.2.12 folgt, dass $\dim U \oplus U^\perp = \dim V$ und daher $U \oplus U^\perp = U + U^\perp = V$. Ist umgekehrt $U + U^\perp = V$, so folgt aus der Dimensionformel, dass $\dim U \cap U^\perp = \dim V - \dim U - \dim U^\perp = 0$, also $U \cap U^\perp = \{0\}$.

(ii) Ist U total isotrop, so gilt $U \subseteq U^\perp$ und daher $\dim U \leq \dim U^\perp$. Mit Satz 7.2.12 folgt, dass $\dim V = \dim U + \dim U^\perp \geq \dim U + \dim U = 2\dim U$. □

Definition 7.2.15. Ein Unterraum $U < V$, der die äquivalenten Bedinungen aus Korollar 7.2.14.(i) erfüllt heißt ein *regulärer Unterraum*.

Nach Definition ist ein Unterraum $U < V$ genau dann regulär, wenn sein Orthogonalraum $U^\perp$ ein Komplement zu U ist. In diesem Fall nennt man dann $U^\perp$ das *orthogonale Komplement* zu U. Nicht-reguläre Unterräume haben nach Definition kein orthogonales Komplement.

Beispiel 7.2.16. Es sei B nicht ausgeartet und $U < V$ ein Unterraum.

(i) Ist $u \in U \cap U^\perp$, so gilt $B(u,u) = 0$, also ist u insbesondere isotrop. Folglich ist jeder total anisotrope Unterraum regulär. Ist V selbst total anisotrop (z.B. weil B ein Skalarprodukt ist), so ist jeder Unterraum regulär.

(ii) Es sei $U = \mathbb{K}v$ eine Gerade mit $v \in V \setminus \{0\}$. Ist v anisotrop, so ist U nach (i) regulär. Man nennt dann U eine *anisotrope Gerade*. Ist hingegen v isotrop, so gilt $U \cap U^\perp = U$, also ist U nicht regulär. Man nennt dann U eine *isotrope Gerade*.

(iii) Der gesamte Raum V ist stets regulär, denn es gilt $V \cap V^\perp = V \cap \{0\} = \{0\}$. Ist B isotrop, so enthält V aber immer eine isotrope Gerade, die nicht regulär ist. *Dies zeigt, dass ein Unterraum eines regulären Unterraums nicht regulär sein muss.*

(iv) Ein total-isotroper Unterraum $U \neq \{0\}$ ist niemals regulär (und besitz daher kein orthogonales Komplement), denn es gilt $U \cap U^\perp$ und daher $U \cap U^\perp = U$.

(v) Ist $U < V$ regulär, so ist auch $U^\perp$ regulär. Nach Satz 7.2.12 ist nämlich

$$U^\perp + (U^\perp)^\perp = U^\perp + U = U + U^\perp = V.$$

Im Folgenden wollen wir uns anschauen, wie wir (V,B) in einfachere Bausteine zerlegen können. Dazu müssen wir zunächst formalisieren, was wir unter einer Zerlegung verstehen.

Konstruktion 7.2.17 (Orthogonale Summe)**.** Es seien $(U_1,B_1),\ldots,(U_n,B_n)$ Paare, die jeweils aus einem endlichdimensionalen $\mathbb{K}$-Vektorraum U_j und einer hermiteschen σ-Sesquilinearform B_j auf U_j bestehen. Es sei nun $U = U_1 \times \cdots \times U_n$ das Produkt dieser Vektorräume. Aus U definieren wir eine Bilinearform B durch

$$B_U((v_1,\ldots,v_n),(w_1,\ldots,w_n)) := B_1(v_1,w_1) + \cdots + B_n(v_n,w_n).$$

Dann heißt (U,B) die *(externe) orthogonale Summe* von $(U_1,B_1),\ldots,(U_n,B_n)$ und wir schreiben

$$(U,B_U) = (U_1,B_1) \perp \ldots \perp (U_n,B_n).$$

Es seien nun $U_1,\ldots,U_n$ Unterräume von V und $B_j := B|_{U_j \times U_j}$. Weiter sei

$$(U,B_U) := (U_1,B_1) \perp \ldots \perp (U_n,B_n).$$

Wir erhalten dann eine lineare Abbildung

$$\iota : U \to V, \quad (u_1, \ldots, u_n) \mapsto u_1 + \cdots + u_n.$$

Wir sagen, dass V die *(interne) orthogonale Summe* von $U_1, \ldots, U_n$ ist und schreiben

$$V = U_1 \perp\!\!\!\oplus \ldots \perp\!\!\!\oplus U_n, \tag{7.2.1}$$

falls ι ein Vektorraum-Isomorphismus ist und $B(\iota(v), \iota(w)) = B_U(v,w)$ für alle $v, w \in U$ gilt. Man nennt diese Darstellung dann eine *orthogonale Zerlegung* von V.

Nach Definition gilt (7.2.1) genau dann, wenn $u_i \perp u_j$ für alle $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ und alle $u_i \in U_i$ und $u_j \in U_j$ gilt, und V als Summe $V = U_1 + \cdots + U_n$ (und daher als *direkte* Summe $V = U_1 \oplus \cdots \oplus U_n$) geschrieben werden kann.

Bemerkung 7.2.18. Ist $V = U_1 \perp\!\!\!\oplus \ldots \perp\!\!\!\oplus U_n$ eine orthogonale Zerlegung und ist $\mathscr{B}$ eine geordnete Basis von V, die durch Aneinanderreihen von geordneten Basen $\mathscr{B}_1, \ldots, \mathscr{B}_n$ von $U_1, \ldots, U_n$ ensteht, so ist

$$D_{\mathscr{B}}(B) = \begin{pmatrix} D_{\mathscr{B}_1}(B|_{U_1 \times U_1}) & & \\ & \ddots & \\ & & D_{\mathscr{B}_n}(B|_{U_n \times U_n}) \end{pmatrix} \implies \det D_{\mathscr{B}}(B) = \prod_{i=1}^{n} \det D_{\mathscr{B}_i}(B|_{U_i \times U_i}).$$

Folglich ist B genau dann nicht-ausgeartet, wenn $B|_{U_1 \times U_1}, \ldots, B|_{U_n \times U_n}$ nicht-ausgeartet sind.

Beispiel 7.2.19. Wir betrachten einige konkrete Beispiele für orthogonale Zerlegungen:

(i) Ist B nicht-ausgeartet und U eine regulärer Unterraum von V, so gilt $V = U \perp\!\!\!\oplus U^\perp$. Insbesondere sind dann $B|_{U \times U}$ und $B|_{U^\perp \times U^\perp}$ nicht-ausgeartet.

(ii) Ist B ausgeartet und V' ein beliebiges Vektorraumkomplement zu $V^\perp$, so gilt $B(v,w) = 0$ für alle $v \in V'$ und $w \in V^\perp$ und daher

$$V = V' \perp\!\!\!\oplus V^\perp.$$

Wir behaupten, dass $B' := B|_{V' \times V'}$ nicht-ausgeartet ist. Zum Beweis sei $u \in \operatorname{Rad}(V', B')$. Dann gilt $u \perp v'$ für alle $v' \in V'$, aber natürlich gilt auch $u \perp w$ für alle $w \in V^\perp$ und daher $u \perp w$ für alle $w \in V' + V^\perp = V$. Dies zeigt, dass $u \in V' \cap V^\perp = \{0\}$. Mittels dieser Zerlegungen können wir uns in vielen Fällen auf das Studium nicht-ausgearteter Formen zurückziehen.

(iii) Ist $(v_1, \ldots, v_n)$ eine geordnete Basis von V, so gilt

$$V = \mathbb{K}v_1 \perp\!\!\!\oplus \ldots \perp\!\!\!\oplus \mathbb{K}v_n \iff \forall\, i, j \in \{1, \ldots, n\} : i \neq j \Rightarrow B(v_i, v_j) = 0.$$

Wie im Fall von Skalarprodukten sagt man dann, dass $(v_1, \ldots, v_n)$ eine *Orthogonalbasis (OGB)* von V ist.

Konstruktion 7.2.20. Ist B nicht-ausgeartet und existiert in V ein anistroper Vektor v_1, so ist $\mathbb{K}v_1$ regulär, und setzen wir $U_1 := (\mathbb{K}v_1)^\perp$, so erhalten wir

$$V = \mathbb{K}v_1 \perp\!\!\!\oplus U_1,$$

wobei U_1 regulär und daher $B|_{U_1 \times U_1}$ nicht ausgeartet ist. Existiert in U_1 ein anisotroper Vektor v_2, so ist $\mathbb{K}v_2$ ein regulärer Unterraum von U_1, also können wir U_1 weiter zerlegen als $U_1 = \mathbb{K}v_2 \oplus U_2$ und erhalten dann

$$V = \mathbb{K}v_1 \oplus \mathbb{K}v_2 \oplus U_2.$$

Falls wir hinreichend viele anisotrope Vektoren finden, so erhalten wir also ein OGB von V. Wir überlegen uns nun, wann dies der Fall ist.

Lemma 7.2.21. *Sei B eine nicht-ausgeartete symmetrische Bilinearform. Ist* $\operatorname{char}(\mathbb{K}) \neq 2$*, so existiert in (V,B) eine anisotrope Gerade.*

Beweis. Nach Annahme existieren $x, y \in V$ mit $B(x,y) \neq 0$. Nach der Polarisierungsidentität gilt dann

$$0 \neq B(x,y) = \frac{1}{2}(B(x+y,x+y) - B(x,x) - B(y,y)),$$

und daher ist mindestens einer der Vektoren $x+y$, x oder y anisotrop und spannt daher eine anisotrope Gerade auf. □

Korollar 7.2.22. *Ist B eine symmetrische Bilinerform und* $\operatorname{char}(\mathbb{K}) \neq 2$*, so besitzt V eine OGB bzgl. B.*

Beweis. Ist B nicht-ausgeartet, so wählen wir mittels Lemma 7.2.21 eine anisotrope Gerade $\mathbb{K}v_1 \subseteq V$ und zerlegen $V = \mathbb{K}v_1 \oplus U_1$. Anschließend wählen wir eine anisotrope Gerade $\mathbb{K}v_2$ in U_1 usw., bis wir eine Zerlegung $\mathbb{K}v_1 \oplus \ldots \oplus \mathbb{K}v_r$ erhalten. Dann ist $(v_1, \ldots, v_r)$ eine OGB.

Ist B ausgeartet, so zerlegen wir $V = V' \oplus V^\perp$ mit $(V', B|_{V' \times V'})$ nicht-ausgeartet. Wir zerlegen dann $V' = \mathbb{K}v_1 \oplus \ldots \oplus \mathbb{K}v_r$ und wählen eine beliebige Basis $(v_{r+1}, \ldots, v_n)$ von $V^\perp$. Dann ist $(v_1, \ldots, v_n)$ eine OGB. □

Korollar 7.2.23. *Ist* $\operatorname{char}(\mathbb{K}) \neq 2$ *und $A \in \mathbb{K}^{n \times n}$ symmetrisch, so existiert $P \in \mathrm{GL}_n(\mathbb{K})$, so dass $P^\top AP$ diagonal ist.*

[17.05.24]

Bemerkung 7.2.24 (Uneindeutigkeit)**.** Für $\lambda \in \mathbb{K}$ definieren wir $[\lambda] := (\mathbb{K}, B_\lambda)$ mit $B_\lambda(v,w) := \lambda vw$. Ist B eine symmetrische Bilinearformen, so existieren $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ mit

$$(V,B) \cong [\lambda_1, \dots, \lambda_n] := [\lambda_1] \perp \dots \perp [\lambda_n].$$

Diese Darstellung ist allerdings nicht eindeutig; dafür gibt es einen banalen und einen tieferen Grund. Zunächst können wir unsere OGB (wie bei Skalarprodukten) „normieren“; wegen $B_\lambda(\mu v, \mu v) = \mu^2 \lambda$ gilt daher $[\lambda] = [\mu^2 \lambda]$. Die Skalare $\lambda_1, \dots, \lambda_n$ sind daher nur bis auf Multiplikation mit einem Quadrat bestimmt.

Im Fall $\mathbb{K} = \mathbb{R}$ können wir z.B. immer erreichen, dass $\lambda_1, \dots, \lambda_n \in \{-1,0,1\}$ gilt. Wir werden später zeigen, dass die so normierten $\lambda_1, \dots, \lambda_n$ dann eindeutig sind.

Für $\mathbb{K} = \mathbb{Q}$ können wir erreichen, dass $\lambda_1, \dots, \lambda_n$ ganze Zahlen sind, in dem wir mit dem Quadrat des Nenners durchmultiplizieren. Wir können dann weiterhin erreichen, dass $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$ *quadratfrei* sind, also keine Vielfachen einer Quadratzahl sind. Selbst mit dieser Normierung ist die Zerlegung aber nicht eindeutig: Für verschiedene Primzahlen $p, q \in \mathbb{N}$ gilt stets $[\pm p] \neq [\pm q]$, aber wir werden noch sehen, dass $[p] \perp [-p] = [q] \perp [-q]$ gilt. (Es ist instruktiv, sich das für $p = 2$ und $q = 3$ von Hand zu überlegen.)

Wie sieht es nun für OGBs bzgl. hermitescher σ-Sesquilinearformen im Fall $\sigma \neq \mathrm{Id}$ aus? Der Beweis im Fall $\sigma = \mathrm{Id}$ basiert auf der Polarisierungsidentität, die in dieser Allgemeinheit nicht gilt. Wir benötigen also eine zusätzliche Annahme.

Definition 7.2.25. Ein Element $i \in \mathbb{K}$ heißt *imaginäre Einheit* bzgl. σ, falls

$$\sigma(i) = -i \quad \text{und} \quad i\sigma(i) = 1.$$

Beispiel 7.2.26. Die komplexe Zahl $i \in \mathbb{C}$ ist eine imaginäre Einheit bzgl. der komplexen Konjugation, aber das ist nicht das einzige Beispiel. So besitzt etwa $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1)$ eine imaginäre Einheit bzgl. der Involution σ, die durch $\sigma([a+bX] = [a-bX])$ gegeben ist (nämlich $i = [X]$).

Übung 7.2.27. Der Körper $\mathbb{K}$ besitze eine imaginäre Einheit i bgzl. σ. Zeigen Sie, dass dann für jede hermitesche σ-Sesquilinearform B die Polarisierungsidentität

$$4B(x,y) = B(x+y,x+y) - B(x-y,x-y) + iB(x+iy,x+iy) - iB(x-iy,x-iy)$$

gilt, und folgern Sie, dass V eine anisotrope Gerade enthält, falls $\mathrm{char}(\mathbb{K}) \neq 2$.

Mittels Polarisierungsidentität folgt wie im symmetrischen Fall:

Korollar 7.2.28. *Es sei* $\mathrm{char}(\mathbb{K}) \neq 2$ *und* σ *besitze eine imaginäre Einheit. Dann existiert zu jeder hermiteschen* σ*-Sesquilinerform eine OGB und für jede Matrix* A *mit* $A^* := \sigma(A)^\top = A$ *existiert eine Matrix* $P \in \mathrm{GL}_n(\mathbb{K})$*, so dass* $P^\top A \sigma(P)$ *diagonal ist.* □

Konstruktion 7.2.29 (Praktische Konstruktion von Orthogonalbasen)**.** Es sei $\mathrm{char}(\mathbb{K}) \neq 2$ und entweder $\sigma = \mathrm{Id}$ oder σ besitze eine imaginäre Einheit. Wie kann man in der Praxis eine OGB zu einer gegebenen hermiteschen σ-Sesquilinearform B bestimmen?

(i) Ist B *anisotrop*, so kann man wie im Fall von (reellen oder komplexen) Skalarprodukten das *Gram–Schmidt-Verfahren* (ohne Normalisierung) auf eine Basis anwenden. Alle Formeln sind wohldefiniert (man teilt nur durch Ausdrücke der Form $B(v,v)$ und es gilt $B(v,v) \in \mathbb{K} \setminus \{0\}$), und auch wenn es keine abstandsminimierenden Projektionen gibt, so kann man doch direkt nachrechnen, dass die resultierende Menge eine OGB ist (Übung!). Ist hingegen B isotrop, so funktioniert dieses Verfahren im Allgemeinen nicht mehr, weil man dabei u.U. durch 0 teilt.

(ii) Ein allgemeines Verfahren, dass auf der *Konstruktion anisotroper Geraden* beruht und sich direkt am obigen Existenzbeweis orientiert, funktioniert so:

(1) Falls $B = 0$, wähle eine beliebige Basis.

(2) Andernfalls finde x, y mit $B(x,y) \neq 0$.

(3) Mindestens ein Vektor aus $\{x, y, x+y\}$ (bzw. $\{x+y, x-y, x-iy, x+iy\}$ im hermiteschen Fall) ist anisotrop. Wähle einen solchen Vektor (z.B. durch Durchprobieren), nenne ihn v_1.

(4) Setze $V_1 := \{v_1\}^\perp$ und $B_1 := B|_{V_1 \times V_1}$. Wende nun (1)-(3) auf (V_1, B_1) an, um einen neuen Vektor v_2 und einen neuen Unterraum V_2 zu erhalten. Mache solange weiter, bis die resultierende Form 0 ist und ergänze dann die gefundene OGB beliebig.

Schritt (1) und (2) sind unproblematisch: Man kann einer beliebig gewählten darstellenden Matrix ja direkt ansehen, ob Sie 0 ist und für welche Basisvektoren v_i, v_j ggf. $B(v_i, v_j) \neq 0$ gilt. Auch Schritt (3) ist rechentechnisch unkritisch. Schritt (4) ist dagegen etwas anstrengend: Um eine Basis von $V_1, V_2, \ldots$ zu bestimmen, muss man jedesmal ein lineares Gleichungssystem lösen, und das ist anstrengend. Wir werden dieses Verfahren daher hier nicht verwenden.

(iii) Ein weitaus schnelleres Verfahren ist der sogenannte *symmetrische (bzw. hermitesche) Gauß-Algorithmus*. Die Grundidee hinter diesem Algorithmus ist, dass jede invertierbare Matrix ein Produkt invertierbarer Elementarmatrizen ist. Ist A eine darstellende Matrix von B, so können wir $P \in \mathrm{GL}_n(\mathbb{R})$ finden mit $P^\top A \sigma(P)$ diagonal. Dannj finden wir Elementarmatrizen $T_1, \ldots, T_k$ mit $P = T_1 \cdots T_k$ und daher

$$T_k^\top (\cdots (T_1^\top A \sigma(T_1)) \cdots) \sigma(T_k) \in \mathrm{Diag}_n(\mathbb{K}).$$

Wir können also an A abwechselnd Zeilenumformungen (entsprechen Linksmultiplikation mit $T_j^\top$ und Spaltenmultiplikationen (entsprechen Rechtsmultiplikation mit $\sigma(T_j)$) anwendenl und A so auf Diagonalform bringen. Die Frage ist nun, wie wir diese Elementarmatrizen finden können. Wir schauen uns das zunächst in einigen Beispielen an.

Beispiel 7.2.30 (Symmetrischer Gauß, einfacher Fall)**.** Wir finden eine OGB zu der hermiteschen Sesquilinearform $B : \mathbb{C}^3 \times \mathbb{C}^3 \to \mathbb{C}$ mit darstellender Matrix (bzgl. der Standardbasis)

$$A := \begin{pmatrix} 1 & 2i & 0 \\ -2i & 3 & -i \\ 0 & i & 2 \end{pmatrix}.$$

Wir erhalten dann

$$A = \begin{pmatrix} 1 & 2i & 0 \\ -2i & 3 & -i \\ 0 & i & 2 \end{pmatrix} \xrightarrow{U_{12}(2i)^\top \cdot} \begin{pmatrix} 1 & 2i & 0 \\ 0 & -1 & -i \\ 0 & i & 2 \end{pmatrix} \xrightarrow{\cdot \overline{U_{12}(2i)}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -i \\ 0 & i & 2 \end{pmatrix}$$
$$\xrightarrow{U_{23}(i)^\top \cdot} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -i \\ 0 & 0 & 3 \end{pmatrix} \xrightarrow{\cdot \overline{U_{23}(i)}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix} =: A'.$$

Es gilt also

$$U_{23}(i)^\top U_{12}(2i)^\top A \overline{U_{12}(2i)U_{23}(i)} = A'.$$

Für $i \neq j$ gilt nun

$$0 = e_i^\top A' e_j = (U_{12}(2i)U_{23}(i)e_i)^\top A(\overline{U_{12}(2i)U_{23}(i)e_j}),$$

und folglich bilden die Spalten von $U_{12}(2i)U_{23}(i)$ eine OGB bzgl. A. Nun gilt

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{U_{23}(i)\cdot} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{U_{12}(2i)\cdot} \begin{pmatrix} 1 & 2i & -2 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} = U_{12}(2i)U_{23}(i).$$

Man beachte die Reihenfolge! Damit haben wir gezeigt, dass

$$\mathscr{B} := \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2i \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ i \\ 1 \end{pmatrix} \right)$$

eine OGB für B mit $D_{\mathscr{B}}(B) = A'$ ist. In Matrizenschreibweise bedeutet dies, dass

$$\begin{pmatrix} 1 & 2i & -2 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}^\top \begin{pmatrix} 1 & 2i & 0 \\ -2i & 3 & -i \\ 0 & i & 2 \end{pmatrix} \begin{pmatrix} 1 & -2i & -2 \\ 0 & 1 & -i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Beispiel 7.2.31 (Symmetrischer Gauß mit diagonaler 0)**.** Das obige Verfahren funktioniert, solange man auf der Diagonale niemals einen Nulleintrag erhält. Dann kann man stets passende Vielfache des Diagonaleintrags von den Zeilen/Spalten abziehen und so Nullzeilen/-spalten schaffen. Der einfachste Fall, wo dies schiefläuft, ist die Bilinearform $B : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ mit darstellender Matrix (bzgl. Standardbasis)

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

Beim „normalen“ Gauß-Algorithmus würde man jetzt einfach die Zeilen vertauschen, aber das führt hier nicht weiter:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \xrightarrow{S_{12}^\top \cdot} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{\cdot S_{12}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

Besser ist es, eine beliebige Zeile und Spalte mit einen von 0 verschiedenen Eintrag zur ersten Zeile und Spalte zu addieren. Im obigen Beispiel ist z.B.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \xrightarrow{U_{21}(1)^\top \cdot} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \xrightarrow{\cdot U_{21}(1)} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\xrightarrow{U_{12}(-1/2)^\top \cdot} \begin{pmatrix} 2 & 1 \\ 0 & -\frac{1}{2} \end{pmatrix} \xrightarrow{\cdot U_{12}(-1/2)} \begin{pmatrix} 2 & 0 \\ 0 & -\frac{1}{2} \end{pmatrix}.$$

Man beachte, dass diese Umformung in Charakteristik 2 nicht funktioniert: Die Matrix A definiert über $\mathbb{F}_2$ die (nicht-ausgeartete) Bilinearform $B(x,y) = x_1y_2 + x_2y_1$, und es gilt $B(x,x) = x_1x_2 + x_2x_1 = 0$ für alle $x \in \mathbb{F}_2$, also bekommt man die 0en auf der Diagonale niemals weg.

Als nächstes schauen wir uns Zerlegungen für Formen an, für die es keine OGB gibt:

Bemerkung 7.2.32 (Zerlegung alternierender Bilinearformen)**.** Es sei nun B eine alternierende Bilinearform mit darstellender Matrix A bzgl. einer beliebigen Basis. Dann ist A *schiefsymmetrisch*, d.h. $A^\top = -A$. Insbesondere sind alle Diagonaleinträge von A stets 0 und wir können daher **keine** OGB für B finden. Wir können V daher nicht in paarweise orthogonale Geraden zerlegen, aber es stellt sich heraus, dass wir V in paarweise orthogonale Geraden und Ebenen zerlegen können.

Zunächst können wir V wie immer zerlegen als $V = V' \oplus V^\perp$ und $V^\perp$ zerlegt sich weiter als orthogonale Summe isotroper Geraden. Wir müssen also nur noch V' zerlegen und dürfen daher annehmen, dass B nicht-ausgeartet ist. Eine nicht-ausgeartete alternierende Bilinearform B bezeichnet man als *symplektische Form*, und man bezeichnet dann (V,B) als *symplektischen Vektorraum*.

Wir betrachten zunächst einen symplektischen Vektorraum der Dimension $\dim V = 2$. Da B nicht-ausgeartet ist, finden wir dann $x, y' \in V$ mit $B(x,y') \neq 0$. Ersetzen wir y' durch $y := y'/B(x,y')$ so gilt $B(x,y) = 1$ und daher $B(y,x) = -1$. Da B alterniered ist, folgt, dass

$$D_{\{x,y\}}(B) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Wir nennen dann (x,y) eine *geordnete symplektische Basis* für V. Es gibt also bis auf Isomorphie genau eine symplektische Ebene.

Wir behaupten nun, dass jeder symplektische Vektorraum (V,B) als orthogonale Summe $V = E_1 \oplus \ldots \oplus E_n$ von symplektischen Ebenen $E_1, \ldots, E_n$ zerfällt. Wählen wir wieder $x, y' \in V$ mit $B(x,y') \neq 0$ und setzen $y' := y/B(x,y')$, so ist nämlich $E_1 := \langle x,y \rangle$ eine symplektische Ebene, und diese ist regulär: Gilt nämlich $v \in E_1 \cap E_1^\perp$, so ist $v = ax + by$ mit $a, b \in \mathbb{K}$ und $b = -B(v,x) = 0$ und $a = B(v,y) = 0$, also $v = 0$. Wir können dann $V = E_1 \oplus E_1^\perp$ zerlegen, und $E_1^\perp$ ist ein symplektischer Vektorraum kleinerer Dimension. Mit Induktion nach $\dim V$ folgt dann die gewünschte Zerlegung.

Wir fassen zusammen:

Satz 7.2.33 (Klassifikation alternierende Bilinearformen)**.** *Es sei B alternierend. Dann existieren symplektische Ebenen $E_1, \ldots, E_r$ und isotrope Geraden $g_1, \ldots, g_k$, so dass*

$$V = E_1 \oplus \ldots \oplus E_r \oplus g_1 \oplus \ldots \oplus g_k. \tag{7.2.2}$$

B ist genau dann nicht-ausgeartet, wenn $k = 0$, und in diesem Fall ist $\dim V = 2r$ gerade.

Die Zahlen r und k sind durch V eindeutig bestimmt: Es ist ja $k = \dim V^\perp$ und $r = 1/2 \cdot \dim V/V^\perp$. Wir nennen k die *Nullität* und r den *Witt-Index* von (V,B). Aus Satz 7.2.33 folgt unmittelbar, dass es in jeder geraden Dimension bis auf Isomorphie genau einen symplektischen Vektorraum gibt (und in ungeraden Dimensionen keinen).

Notation 7.2.34 (Symplektische Basis)**.** Es sei B nicht-ausgeartet und $V = E_1 \oplus \ldots \oplus E_r$ eine Zerlegung in symplektische Ebenen. Ist (e_j, f_j) eine symplektische Basis für E_j, so nennen wir

$$\mathscr{B} := (e_1 \ldots, e_r, f_1, \ldots, f_r)$$

eine *symplektische Basis* von (V,B). Es gilt dann

$$D_{\mathscr{B}}(\omega) = \begin{pmatrix} 0 & \mathbf{1} \\ -\mathbf{1} & 0 \end{pmatrix}. \tag{7.2.3}$$

Gilt umgekehrt (7.2.3), so ist $\mathscr{B}$ eine symplektische Basis. Der Koordinatenisomorphismus zu einer solchen Basis identifiziert also (V,B) mit $(\mathbb{K}^{2n},B_0)$, wobei B_0 die *symplektischen Standardform*

$$B_0 : \mathbb{K}^{2n} \times \mathbb{K}^{2n} \to \mathbb{K}, \quad (x,y) \mapsto x^\top \begin{pmatrix} 0 & \mathbf{1} \\ -\mathbf{1} & 0 \end{pmatrix} y = \sum_{i=1}^{n} x_i y_{n+i} - y_i x_{n+i}$$

ist.

Übung 7.2.35. Es sei (V,B) ein symplektischer Unterraum der Dimension $2r$. Ein total isotroper Unterraum der Dimension r heißt ein *Lagrange-Unterraum* von V, und zwei Lagrange-Unterräume L_+,L_- heißen *gegenüberliegend*, falls $V = L_+ \oplus L_-$. Ein total isotroper Unterraum $L \subseteq V$ heißt *maximal*, wenn es keinen total isotropen Unterraum L' gibt mit $L \subsetneq L' \subseteq V$. Zeigen Sie:

(i) In jedem symplektischen Vektorraum gibt es zwei gegenüberliegende Lagrange-Unterräume.

(ii) Für einen total isotropen Unterraum sind die folgenden Aussagen äquivalent:
   (i) L ist maximaler total isotroper Unterraum.
   (ii) Ist $v \in V$ und $\omega(v,l) = 0$ für jedes $l \in L$, so ist schon $v \in L$.
   (iii) $L^\perp \subseteq L$.
   (iv) $L = L^\perp$.
   (v) L ist ein Lagrange-Unterraum, d.h. $\dim L = r$.

(iii) Jeder total isotrope Unterraum $U < V$ ist in einem Lagrange-Unterraum enthalten.

Eine orthogonale Zerlegung in Ebenen und Geraden ähnlich der in Satz 7.2.33 existiert auch für hermitesche σ-Sesquilinearformern über Körpern der Charakteristik $\neq 2$, und zwar *ohne* dass wir die Existenz einer imaginären Einheit voraussetzen müssen. Selbst im Fall von symmetrischen Bilinearformen hat diese eine Reihe von Vorteilen gegenüber einer orthogonale Zerlegung in Geraden (=OGB). U.A. werden wir später noch sehen, dass diese Zerlegung in einem gewissen Sinne kanonisch ist.

Bis zum Ende dieses Abschnitts sei $\mathbb{K}$ ein Körper der Charakteristik $\neq 2$ und B sei eine *hermitsche* σ-Sesquilinearform. (Der Fall $\sigma = \mathrm{Id}$ ist ausdrücklich erlaubt.)

Beispiel 7.2.36 (Isotrope Standardebene)**.** Auf $\mathbb{K}^2$ definiert

$$B_{\mathrm{std}} : \mathbb{K}^2 \times \mathbb{K}^2 \to \mathbb{K}, \quad (x,y) \mapsto x^\top \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sigma(y) = x_1\sigma(y_2) + x_2\sigma(y_1)$$

eine hermitesche σ-Sesquilinearform. Diese ist isotrop, denn es gilt $B_{\mathrm{std}}(e_1,e_1) = B_{\mathrm{std}}(e_2,e_2) = 0$, aber nicht-ausgeartet. Wir nennen $(\mathbb{K}^2,B_{\mathrm{std}})$ die *isotrope Standardebene* über $(\mathbb{K},\sigma)$.

Definition 7.2.37. Ist $\dim V = 2$, so heißt eine geordnete Basis (v_1, v_2) von V eine *Witt-Basis*[10] von V, falls

$$D_{\mathscr{B}}(B) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ist (v_1, v_2) eine Witt-Basis, so identifiziert der zugehörige Koordinatenisomorphismus also (V, B) mit der isotropen Standardebene.

Proposition 7.2.38 (Klassifikation isotroper Ebenen)**.** *Es sei* $\mathrm{char}(\mathbb{K}) \neq 2$ *und* B *eine nicht-ausgeartete isotrope hermitesche* σ*-Sesquilinearform. Dann existiert ein Unterraum* $E < V$ *mit* $\dim E = 2$*, so dass* $(E, B|_{E\times E})$ *regulär und isomorph zur isotropen Standardebene ist. Ist insbesondere* $\dim V = 2$*, so ist* (V, B) *isomorph zur isotropen Standardebene.*

Beweis. Da B isotrop ist, existiert ein Vektor $v_1 \in V \setminus \{0\}$ mit $B(v_1, v_1) = 0$. Da B nicht-ausgeartet ist, existiert $w_2 \in V$ mit $B(v_1, w_2) \neq 0$. Dieser ist automatisch linear unabhängig von v_1, denn wäre $w_2 = \lambda v_1$ für ein $\lambda \in \mathbb{K}$, so wäre

$$B(v_1, w_2) = B(v_1, \lambda v_1) = \sigma(\lambda) B(v_1, v_1) = 0.$$

Insbesondere ist $\mathscr{B}_0 := (v_1, w_2)$ eine Basis von $E := \langle v_1, w_2 \rangle$, und die darstellende Matrix von $B|_{E\times E}$ bzgl. $\mathscr{B}_0$ ist

$$D_{\mathscr{B}_0}(B|_{E\times E}) = \begin{pmatrix} 0 & \sigma(\lambda) \\ \lambda & \mu \end{pmatrix}, \quad \text{wobei } \lambda := B(v_1, w_2),\ \mu := B(w_2, w_2).$$

Durch geschickten Basiswechsel lässt sich diese darstellende Matrix nun vereinfachen: Zunächst setzen wir $w_2' := \lambda^{-1} \cdot w_2$; dann ist $B(v_1, w_2') = \lambda^{-1} B(v_1, w_2) = 1$, und für $\mathscr{B}_1 := (v_1, w_2')$ gilt daher

$$D_{\mathscr{B}_1}(B|_{E\times E}) = \begin{pmatrix} 0 & 1 \\ 1 & \mu' \end{pmatrix}, \quad \text{wobei } \mu' := B(w_2', w_2').$$

Da $D_{\mathscr{B}_1}(B|_{E\times E})$ hermitesch ist, gilt hier automatisch $\sigma(\mu') = \mu$. Um dieses μ' loszuwerden, setzen wir nun schließlich $v_2 := w_2' - \frac{1}{2}\mu' v_1$. (Hier verwenden wir, dass $\mathrm{char}(\mathbb{K}) \neq 2$ gilt.) Es ist dann

$$B(v_1, v_2) = B\left(v_1, w_2' - \frac{1}{2}\mu' v_1\right) = B(v_1, w_2') - \frac{1}{2}\sigma(\mu') \cdot B(v_1, v_1) = 1 - \frac{1}{2}\sigma(\mu') \cdot 0 = 1,$$

und wegen $\mu' = \sigma(\mu')$ gilt weiter

$$\begin{aligned} B(v_2, v_2) &= B\left(w_2' - \frac{1}{2}\mu' v_1, w_2' - \frac{1}{2}\mu' v_1\right) \\ &= B(w_2', w_2') - \frac{1}{2}\mu' B(v_1, w_2') - \frac{1}{2}\sigma(\mu') B(w_2', v_1) + \frac{1}{4}\mu'\sigma(\mu') B(v_1, v_1) \\ &= \mu' - \frac{1}{2}\mu' - \frac{1}{2}\mu' + 0 \quad = \quad 0. \end{aligned}$$

Dies zeigt, dass (v_1, v_2) eine Witt-Basis ist. Um zu sehen, dass E regulär ist, schreiben wir $v \in E \cap E^\perp$ als $v = a v_1 + b v_2$; dann gilt $b = B(v, v_1) = 0 = B(v, v_2) = a$, also $v = 0$. □

[10] Ernst Witt, dt. Mathematiker (1911-1991)

Beispiel 7.2.39 (Isotrope Standardebenen aus anisotropen Geraden)**.** Es sei $\sigma = \mathrm{Id}$ und $\lambda \in \mathbb{K} \setminus \{0\}$. Mit der Notation aus Bemerkung 7.2.24 ist $[-\lambda,\lambda] = [-\lambda] \oplus [\lambda]$ nicht-ausgeartet und isotrop, denn die darstellende Matrix bzgl. einer geeigneten OGB ist

$$A = \begin{pmatrix} -\lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

und für diese gilt

$$\det(A) = -\lambda^2 \neq 0 \quad \text{und} \quad (1,1)A\begin{pmatrix}1\\1\end{pmatrix} = (1,1)\begin{pmatrix}-\lambda\\ \lambda\end{pmatrix} = 0.$$

Daher ist $[-\lambda,\lambda]$ isomorph zur isotropen Standardebene. Insbesondere besitzt die isotrope Standardebene E über $\mathbb{Q}$ die verschiedenen Zerlegungen

$$E \cong [-1] \perp [1] \cong [-2] \perp [2] \cong [-3] \perp [3] \cong [-5] \perp [5] \cong \ldots.$$

Wenn man eine isotrope Standardebene weiter zerlegt, so handelt man sich dabei also Uneindeutigkeit ein. Insofern sind isotrope Standardebenen minimale kanonische Bausteine.

Satz 7.2.40 (Witt-Zerlegung)**.** *Es sei* $\mathrm{char}(\mathbb{K}) \neq 2$ *und B eine hermitesche σ-Sesquilinearform. Dann existieren Ebenen $E_1,\ldots,E_r$, die isomorph zur isotropen Standardebene sind, und ein total anisotroper Unterraum A, so dass*

$$(V,B) \cong E_1 \perp \ldots \perp E_r \perp A \perp V^{\perp}. \tag{7.2.4}$$

Beweis. Indem wir das Radikal abspalten, dürfen wir annehmen, dass B nicht-ausgeartet ist. Wir nehmen dies ab jetzt an und beweisen die Zerlegung durch Induktion nach $n := \dim V$. Ist $n = 0$, so ist nichts zu zeigen. Sei nun $n \geq 1$. Ist V anisotrop, so setzen wir $A := V$. Andernfalls finden wir nach Proposition 7.2.38 einen regulären Unterraum $E_1 < V$, der isomorph zur isotropen Standardebene ist, und es gilt $V = E_1 \perp V'$. Anwenden der Induktionsvoraussetzung auf V' zeigt dann die Behauptung. □

Bemerkung 7.2.41. Wir werden später noch sehen, dass die Zahl r in (7.2.4) eindeutig bestimmt ist; diese heißt der *Witt-Index* von B. Wir werden auch sehen, dass der *anisotrope Teil* $(A, B|_{A\times A})$ durch B bis auf Isomorphie eindeutig bestimmt ist. Ist $\sigma = \mathrm{Id}$ oder existiert eine imaginäre Einheit für σ, so können wir A durch Wahl einer OGB als orthogonale Summe anisotroper Geraden zerlegen (und analog können wir $V^{\perp}$ als orthogonale Summe isotroper Geraden zerlegen), aber damit zerstören wir die Eindeutigkeit.

Bemerkung 7.2.42 (Witt-Zerlegung im rellen und konjugiert-komplexen Fall)**.** Im Fall von $(\mathbb{K},\sigma) \in \{(\mathbb{R},\mathrm{Id}),(\mathbb{C},\bar{\cdot})\}$ ist $(A, B|_{A\times A})$ definit, und daher isomorph zu $\mathbb{R}^{\dim A}$ bzw. $\mathbb{C}^{\dim A}$ mit dem Standardskalarprodukt oder seinem Negativen. Damit haben wir in diesen beiden Fällen eine Zerlegung in Grundbausteine erreicht. Wir finden also stets eine geordnete Basis, so das die darstellende Matrix von B von der Form

$$\begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & -1 & \\ & & & & & & \ddots \\ & & & & & & & -1 \end{pmatrix}$$

ist. Man nennt eine solche Basis dann auch eine *Witt-Basis* für (V,B).

Beispiel 7.2.43 (Eine explizite Witt-Basis)**.** Es sei $B : \mathbb{C}^3 \times \mathbb{C}^3 \to \mathbb{C}$ die Sesquilinearform aus Beispiel 7.2.30. Die darstellende Matrix bzgl. der Standardbasis was

$$A := \begin{pmatrix} 1 & 2i & 0 \\ -2i & 3 & -i \\ 0 & i & 2 \end{pmatrix},$$

und wir haben bereits gesehen, dass diese kongruent zur Matrix $A' = \operatorname{diag}(1,-1,3)$ ist. Diese Matrix können wir nun weiter umformen:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\xrightarrow{U_{12}(1)^\top \cdot} \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix} \xrightarrow{\cdot \overline{U_{12}(1)}} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\xrightarrow{U_{21}(-1/2)^\top \cdot} \begin{pmatrix} 1/2 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} \xrightarrow{\cdot \overline{U_{21}(-1/2)}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} =: A''$$

Wollen wir nun eine Basis $\mathscr{B}''$ von V mit $D_{\mathscr{B}''}(B) = A''$ finden, so müssen wir alle Elementarumformungen rückwärts an der Einheitsmatrix durchführen, d.h. $\mathscr{B}''$ besteht aus den Spalten der Matrix

$$M'' := U_{12}(2i)U_{23}(i)U_{12}(1)U_{21}(-1/2)\mathbf{1}.$$

Die Matrix $M' := U_{12}(2i)U_{23}(i)\mathbf{1}$ hatten wir schon in Beispiel 7.2.30 berechnet. Nun ist

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{U_{21}(-1/2)} \begin{pmatrix} 1 & 0 & 0 \\ -1/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{U_{12}(1)} \begin{pmatrix} 1/2 & 1 & 0 \\ -1/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

und folglich

$$M'' = M' \begin{pmatrix} 1/2 & 1 & 0 \\ -1/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2i & -2 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & 1 & 0 \\ -1/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 - i & 1 + 2i & -1 \\ -1/2 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}.$$

Die gewünschte Basis ist also

$$\mathscr{B}'' := \left(\begin{pmatrix} 1/2 - i \\ -1/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 + 2i \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ i \\ 1 \end{pmatrix} \right).$$

Wenn wir wollen, so können wir den letzten Vektor noch auf Länge 1 normieren, in dem wir durch $\sqrt{3}$ teilen. Wir erhalten $(\mathbb{C}^3, B) \cong E \perp [1]$.

[29.05.24]

Bemerkung 7.2.44 (Eine allgemeine Strategie?)**.** Im vorigen Beispiel sind wir wie folgt vorgegangen: Wir haben zunächst die Matrix A in eine Diagonalmatrix überführt. Im Fall $\sigma = \mathrm{Id}$ oder wenn eine imaginäre Einheit existiert, können wir das immer mittels symmetrischen Gauß erreichen. Wenn wir wollen, können wir dann die Diagonalanträge noch normalisieren – im reellen oder komplex-konugierten Fall auf ± 1, allgemein gibt es keine bevorzugte Normalisierung. Anschließend machen wir uns auf die Suche nach isotropen Standardebenen. Wenn wir ein Paar von Diagonaleinträgen der Form $(\lambda, -\lambda)$ finden, können wir daraus eine isotrope Standardebene produzieren. Auf diese Weise erzeugen wir so viele hyperbolische Ebenen wie wir können, und hoffen dann, dass das, was übrig bleibt, eine total anisotrope Form ist. Über $\mathbb{R}$ und $\mathbb{C}$ funktioniert das immer, im Allgemeinen ist es aber schwer zu entscheiden, wann eine Diagonalmatrix, die kein Paar von Diagonaleinträgen der Form $(\lambda, -\lambda)$ besitzt, anisotrop ist. Wir illustrieren dies anhand von zwei Beispielen.

Beispiel 7.2.45 (Eine versteckte isotrope Ebene)**.** Über $(\mathbb{K}, \sigma) = (\mathbb{Q}, \mathrm{Id})$ betrachten wir $(V, B) = [2, 2, -1]$. Da 1 und 2 sich über $\mathbb{Q}$ nicht nur um ein Quadrat unterscheiden, sieht man auf den ersten Blick keine isotrope Ebene, und man könnte vermuten, dass der Witt-Index 0 ist. Nun ist aber

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^\top \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \text{also} \quad [2,2] \cong [1,1].$$

Wir erhalten daher $[2, 2, -1] \cong [1, 1, -1] \cong E \perp [1]$, also ist der Witt-Index 1.

Bemerkung 7.2.46 (Historische Einordnung)**.** Beispiel 7.2.45 deutet bereits an, dass eine Klassifikation anisotroper Bilinearformen über allgemeinen Körpern auf Schwierigkeiten stößt: Die anisotropen Ebenen [1,1] und [2,2] über $\mathbb{Q}$ sind isomorph, obwohl die anisotropen Geraden [1] und [2] nicht isomorph sind, und ohne dass es dafür auf den ersten Blick einen erkennbaren Grund gibt. Trotz jahrhundertelangen Bemühungen ist die Klassifikation anisotroper Bilinearformen bis heute nur über sehr speziellen Körpern bekannt. Das ist umso erstaunlicher, als die anisotropen Bilinearformen über $\mathbb{R}$ bis auf Vorzeichen gerade die Skalarprodukte, also die einfachsten Bilinearformen sind! Einer der großen Durchbrüche der Zahlentheorie im frühen 20. Jahrhundert war die Klassifikation der (anisotropen) Bilinearformen über (endlichen Körpererweiterungen von) $\mathbb{Q}$ durch Helmut Hasse[11] und Hermann Minkowski[12]. Selbst die Aussage des Klassifikationssatzes für $\mathbb{K} = \mathbb{Q}$ geht weit über dieser Vorlesung hinaus und benötigt das Konzept der p-adischen Zahlen.

Beispiel 7.2.47 (Positive Charakteristik)**.** Noch „schlimmer“ (oder interessanter) sieht es in positiver Charakteristik aus. Betrachten wir z.B. $\mathbb{K} = \mathbb{F}_3$ mit der Bilinearform $B(x, y) = x_1 y_1 + x_2 y_2 + x_3 y_3$ auf $V := \mathbb{K}^3$. Die darstellende Matrix bzgl. der Standardbasis ist die Einheitsmatrix (also insbesondere $(V, B) \cong [1,1,1]$), also sieht diese Bilinearform auf den ersten Blick wie ein „Skalarprodukt“ aus, aber B ist nicht total anisotrop. Der Vektor $v := e_1 + e_2 + e_3$ ist nämlich ein isotroper Vektor (da $B(v, v) = 3 = 0$). Der Witt-Index der zur Einheitsmatrix gehörenden Bilinearform ist daher 1.

Übung 7.2.48. Wie lautet eine Witt-Zerlegung des Minkowksi-Raums $\mathbb{R}^{n,1}$? Geben Sie auch eine explizite Witt-Basis an.

[11] dt. Mathematiker, 1898–1979
[12] dt. Mathematiker, 1864–1909

Übung 7.2.49 (Witt-Zerlegung der Spurform)**.** Bestimmen Sie eine Witt-Zerlegung der Spurform B auf $\mathbb{K}^{n\times n}$ für $(\mathbb{K},\sigma)\in\{(\mathbb{R},\mathrm{Id}),(\mathbb{C},\bar{\cdot}),(\mathbb{Q},\mathrm{Id})\}$. Auf welche Schwierigkeiten treffen Sie, wenn $\mathbb{K}$ ein endlicher Körper ist?

Zusammenfassung von Abschnitt 7.2

(1) In einem Vektorraum mit hermitescher oder schief-hermitescher Sesquilinearform B hat man ein natürliches Konzept von Orthogonalität, wobei Vektoren zu sich selbst orthogonal („isotrop“) sein können.

(2) Ist B nicht-ausgeartet, so besitzt jeder Unterraum U einen Orthogonalraum $U^\perp$ von komplementärer Dimension. Dieser ist genau dann ein Komplement zu U, wenn $U\cap U^\perp=\{0\}$.

(3) In Charakteristik $\neq 2$ besitzt jeder Vektorraum mit hermitescher Sesquilinearform eine Zerlegung in isotrope Standardebenen, isotrope Geraden und einen Unterraum ohne isotrope Vektoren („Witt-Zerlegung“).

(4) Die isotrope Standardebene kann man (nicht-kanonisch) in anisotrope Gerden zerlegen. Im Fall von symmetrischen Bilinearformen (oder falls es eine imaginäre Einheit gibt) kann man auch den anisotropen Teil (nicht-kanonisch) in anisotrope Geraden zerlegen und erhält so eine orthogonale Zerlegung in Geraden (also eine Orthogonalbasis).

(5) Zur expliziten Berechnung von Witt-Zerlegungen und Orthogonalbasen kann der symmetrische Gauß-Algorithmus vewendet werden.

(6) Es gibt bis auf Isomorphie genau eine symplektische Ebene, und jeder symplektische Vektorraum ist isomorph zur orthogonalen Summe solcher Ebenen.

7.3 Automorphismen

In diesem Abschnitt sei stets $\mathbb{K}$ ein Körper und $\sigma:\mathbb{K}\to\mathbb{K}$ ein Automorphismus der Ordnung ≤ 2. Weiter seien V und V' zwei endlichdimensionale $\mathbb{K}$-Vektorräume und $B:V\times V\to\mathbb{K}$ und $B':V'\times V'\to\mathbb{K}$ zwei σ-Sesqulinearformen, die entweder hermitesch oder schiefhermitesch sind.

Definition 7.3.1. Eine lineare Abbildung $\Phi:V\to V'$ heißt ein *Morphismus* von (V,B) zu (V',B'), falls $B'(\Phi(v),\Phi(w))=B(v,w)$ für alle $v,w\in V$. In diesem Fall schreiben wir $\Phi:(V,B)\to(V',B')$.

Wie üblich nennen wir Φ einen Mono-/Epi-/Iso-/Endomorphismus, wenn Φ injektiv bzw. surjektiv bzw. bijektiv bzw. $V=V'$ und $B=B'$ ist. Ein bijektiver Endomorphismus heißt wiederum ein *Automorphismus*, und (V,B) und (V',B') heißen *isomorph* (geschrieben $(V,B)\cong(V',B')$), falls ein Isomorphismus $\Phi:(V,B)\to(V',B')$ existiert. Man überlegt sich leicht[13], dass die Menge

$$\mathrm{Aut}(V,B):=\{\Phi:(V,B)\to(V,B)\mid\Phi\text{ Automorphismus}\}.$$

eine Untergruppe von $\mathrm{GL}(V)$ ist. Diese heißt die *Automorphismengruppe* von (V,B).

[13] Dass die Verkettung von Automorphismen wieder ein Automorphismus ist, ist unmittelbar klar, aber man muss sich kurz überlegen, warum das Inverse eines Automorphismus ein Automorphismus ist.

Bemerkung 7.3.2 (Morphismen in Matrixzensprache)**.** Es seien $\mathscr{B} = (v_1, \dots, v_n)$ und $\mathscr{B}' = (v'_1, \dots, v'_m)$ geordnete Basen von V bzw. V' und $\Phi : V \to V'$ linear. Weiter seien

$$A := D_{\mathscr{B}}(B), \quad A' := D_{\mathscr{B}'}(B') \quad \text{und} \quad C := D_{\mathscr{B}',\mathscr{B}}(\Phi)$$

Ist $A = (a_{ij})$, $A' = (a'_{ij})$ und $C = (c_{ij})$, so gilt

$$B(\Phi(v_i), \Phi(v_j)) = B\left(\sum_{k=1}^{m} c_{ki} v'_k, \sum_{l=1}^{m} c_{lj} v'_l\right) = \sum_{k=1}^{m}\sum_{l=1}^{m} c_{kj}\sigma(c_{lj}) B(v'_k, v'_l) = \sum_{k=1}^{m}\sum_{l=1}^{m} c_{ki} a'_{kl}, \sigma(c_{lj})$$

und daher ist Φ genau dann ein Morphismus $(V,B) \to (V',B')$, wenn

$$A = C^\top A' \sigma(C). \tag{7.3.1}$$

Als Spezialfall halten wir fest:

Proposition 7.3.3 (Matrizen von Automorphismen)**.** *Sei $\mathscr{B} = (v_1, \dots, v_n)$ eine geordnete Basis von V und $A := D_{\mathscr{B}}(B)$, und sei $\Phi \in \mathrm{GL}(V)$ mit $T := D_{\mathscr{B},\mathscr{B}}(\Phi)$. Dann gilt*

$$\Phi \in \mathrm{Aut}(V,B) \iff T^\top A \sigma(T) = A. \qquad \square$$

Proposition 7.3.4 (Isomorphie-Kriterium)**.** *Die folgenden Aussagen sind äquivalent:*

(i) (V,B) und (V',B') sind isomorph.

(ii) Es existieren Basen $\mathscr{B}$ von V und $\mathscr{B}'$ von V', so dass $D_{\mathscr{B}}(B)$ und $D_{\mathscr{B}'}(B')$ σ-kongruent sind.

Beweis. (i) $\Longrightarrow$ (ii): Sei $\Phi : (V,B) \to (V',B')$ ein Isomorphismus. Ist $\mathscr{B} = (v_1, \dots, v_n)$ eine beliebige Basis von V und $\mathscr{B}' = (\Phi(v_1), \dots, \Phi(v_n))$, so gilt $D_{\mathscr{B}}(B) = D_{\mathscr{B}'}(B')$, denn $B'(\Phi(v_i), \Phi(v_j)) = B(v_i, v_j)$.

(ii) $\Longrightarrow$ (i): Nach Basiswechsel dürfen wir annehmen, dass sogar $D_{\mathscr{B}}(B) = D_{\mathscr{B}'}(B') =: (a_{ij})$ gilt. Ist $\mathscr{B} = (v_1, \dots, v_n)$ und $\mathscr{B}' = (v'_1, \dots, v'_n)$ so existiert ein eindeutiger Vektorraumisomorphismus $\Phi : V \to V'$ mit $\Phi(v_j) = v'_j$ für $j \in \{1, \dots, n\}$. Es gilt dann

$$B'(\Phi(v_i), \Phi(v_j)) = B'(v'_i, v'_j) = a_{ij} = B(v_i, v_j),$$

also ist Φ sogar ein Isomorphismus. $\square$

Bemerkung 7.3.5. Wie im Fall von Vektorräumen und linearen Abbildungen interessieren wir uns auch im Fall von Vektorräumen mit Sesquilinearform für zwei fundamentale Fragen:

(1) *Wann sind zwei gegebene Vektorräume mit Sesquilinearform isomorph?* Das ist das sogenannte *Klassifikationsproblem*. Im Fall von Vektorräumen haben wir gesehen, dass zwei endlichdimensionale Vektorräume genau dann isomorph sind, wenn sie dieselbe Dimension besitzen. Im Fall von Vektorräumen mit Sesquilinearform gibt es nur in Spezialfällen eine vergleichbar einfache Antwort. In Matrizensprache übersetzt lautet das Problem, zu entscheiden ob zwei gegebene (schief-)hermitesche Matrizen σ-kongruent sind.

(2) *Wie lassen sich die Automorphismen eines gegebenen Vektorraums beschreiben?* Das ist das sogenannte *Symmetrieproblem*. Selbst im Fall von Vektorräumen (ohne Sesquilinearform) war die Antwort kompliziert: Jede invertierbare Matrix ist ein Produkt invertierbarer Elementarmatrizen und konjugiert zu einer im wesentlichen eindeutigen Matrix in Jordannormalform. Die Gruppenstruktur der Automorphismengruppe ist sehr kompliziert. Eine Normalformentheorie für Automorphismen werden wir später im Fall von Skalarprodukten mittels des Spektralsatzes herleiten. In diesem Abschnitt beschränken wir uns darauf, in gewissen Fällen ein Erzeugendensystem für die Automorphismengruppe anzugeben.

Notation 7.3.6 (Die klassischen Gruppen)**.** Nicht alle Vektorräume mit Sesquilinearform (und ihre Symmetriegruppen) sind für uns gleichermaßen interessant. Wir interessieren uns besonders für die folgenden Fälle:

(1) Ist B eine nicht-ausgeartete symmetrische Bilinearform, so nennen wir (V,B) einen *orthogonalen Vektorraum*. Typische Beispiele sind euklidische Vektorräume (anisotrop) und Minkowski-Räume (isotrop). Wir nennen die Automorphismen-Gruppe von (V,B) dann die zugehörige *orthogonale Gruppe* und beschreiben diese mit $\mathrm{O}(V,B)$. Die Untergruppe

$$\mathrm{SO}(V,B) := O(V,B) \cap \mathrm{SL}(V,B)$$

heißt die *spezielle orthogonale Gruppe*.

(2) Ist B eine nicht-ausgeartete hermitesche Sesquilinearform mit $\sigma \neq \mathrm{Id}$, so nennen wir (V,B) einen *hermiteschen Vektorraum*. Typische Beispiele sind unitäre Vektorräume. Wir nennen die Automorphismen-Gruppe von (V,B) dann die zugehörige *unitäre Gruppe* und beschreiben diese mit $\mathrm{U}(V,B)$. Die Untergruppe

$$\mathrm{SU}(V,B) := U(V,B) \cap \mathrm{SL}(V,B)$$

heißt die *spezielle unitäre Gruppe*.

(3) Ist B eine nicht-ausgeartete alternierende Bilinearform, also eine symplektische Form, so nennen wir (V,B) einen *symplektischen Vektorraum*. Wir nennen die Automorphismen-Gruppe von (V,B) dann die zugehörige *symplektische Gruppe* und beschreiben diese mit $\mathrm{Sp}(V,B)$.

Die hier aufgelisteten Gruppen (zusammen mit der allgemeinen und speziellen linearen Gruppen) haben für die Entwicklung der modernen Gruppentheorie eine derart wichtige Rolle gespielt, dass sie von Hermann Weyl mit dem Namen „die klassischen Gruppen“ geadelt wurden.

Beispiel 7.3.7 (Was wir schon wissen)**.** Bzgl. des Klassifikationsproblems wissen wir bereits die folgenden Dinge:

(1) Es gibt bis auf Isomorphie in jeder endlichen Dimension genau einen euklidischen bzw. unitären Vektorraum. (Anders gesagt: Jeder euklidische oder unitäre Vektorraum besitzt eine ONB.)

(2) Es gibt in jeder geraden Dimension bis auf Isomorphie genau einen symplektischen Vektorraum (und keinen solchen in ungerader Dimension).

(3) In Charakteristik $\neq 2$ ist jeder orthogonale oder hermitesche Vektoraum isomorph zu einer orthogonalen Summe aus isotropen Standardebenen und einem anisotropen orthogonalen bzw. hermiteschen Vektorraum (Witt-Zerlegung), oder (falls wir im hermitschen Fall zusätzlich die Existenz einer imaginären Einheit annehmen) alternativ isomorph zu einer orthogonalen Summe anisotroper Geraden (OGB). Die Frage der Eindeutigkeit solcher Zerlegungen ist kompliziert - wir werden darauf im nächsten Abschnitt eingehen.

Bzgl. des Symmetrieproblems wissen wir noch sehr wenig, insbesondere fehlen uns konkrete Beispiele für Automorphismen. In den Übugen haben Sie gesehen, dass die orthogonale Gruppe zum Standardskalarprodukt in $\mathbb{R}^2$ aus Spiegelungen an Ursprungsgeraden (Elementen von Determinanten -1) und Drehungen um den Ursprung (Elementen von Determinanten 1) besteht und von den Spiegelungen erzeugt wird. Wir fragen uns nun, wie sich solche Spiegelungen und Drehungen verallgemeinern lassen.

Beispiel 7.3.8 (Spiegelungen an Ursprungsgeraden)**.** Eine Spiegelung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ an einer Ursprungsgeraden hat die folgenden geometrischen Eigenschaften:

- Φ ist linear.
- Φ ist eine Involution, d.h. $\Phi^2 = \mathrm{Id}$, und $\Phi \neq \pm\mathrm{Id}$. Insbesondere ist das Minimalpolynom von Φ gegeben durch $\mu_\Phi(X) = (X-1)(X+1)$.
- Da μ_Φ in Linearfaktoren zerfällt, ist Φ diagonalisierbar, und daher $\mathbb{R}^2 = V_1(\Phi) \oplus V_{-1}(\Phi)$, wobei $V_1(\Phi)$ und $V_{-1}(\Phi)$ die Eigenräume von Φ zu den Eigenwerten 1 und -1 sind. Dabei ist $V_1(\Phi)$ die Menge der Fixpunkte von Φ, also die Gerade, an der Φ spiegelt.
- Die letzte und entscheidende Eigenschaft ist, dass $V_{-1}(\Phi)$ senkrecht auf $V_1(\Phi)$ bzgl. des Standardskalarprodukts steht. Die Menge der Vektoren, die von der Spiegelung auf ihr Negatives abgebildet werden, ist also $V_{-1}(\Phi) = V_1(\Phi)^\perp$.

Ist umgekehrt U eine Ursprungsgerade in $\mathbb{R}^2$, so gilt (bzgl. der Skalarprodukts) $\mathbb{R}^2 = U \oplus U^\perp$, und daher gibt es genau eine lineare Abbildung Φ auf $\mathbb{R}^2$ mit $\Phi|_U = \mathrm{Id}$ und $\Phi|_{U^\perp} = -\mathrm{Id}$, und diese ist gerade die Spiegelung an U.

Diese Konstruktion lässt sich nun sehr weit verallgemeinern.

Konstruktion 7.3.9 (Spiegelungen an regulären Unterräumen)**.** Es sei V ein $\mathbb{K}$-Vektorraum und $B : V \times V \to \mathbb{K}$ eine nicht-ausgeartete σ-Sesquilinearform, die entweder hermitesch oder schief-hermitesch ist. (Am Interessantesten für uns sind symmetrische Bilinearformen, aber die Konstruktion funktioniert ganz allgemein.)

Ist nun $U < V$ ein regulärer Unterraum, so ist auch $U^\perp$ ein regulärer Unterraum und es gilt $V = U \perp U^\perp$. Es existieren daher eindeutige Endomorphismen π_U und $\pi_{U^\perp}$ von V mit

$$\pi_U(u+u') = u \quad \text{und} \quad \pi_{U^\perp}(u+u') = u' \quad \text{und} \quad (u \in U, u' \in U').$$

Im Fall von Skalarprodukten sind das genau die klassischen Orthogonalprojektionen, und auch wenn diese Projektionen im Allgemeinen keine Abstände minimieren, bezeichnen wir sie auch im jetzigen Setting als *Orthogonalprojektionen*.

Wir definieren dann die *Spiegelung an U* als den Endomorphismus

$$s_U := \mathrm{Id} - 2\pi_{U^\perp} : V \to V.$$

Für $u \in U$ und $u' \in U^\perp$ gilt dann $s_U(u+u') = u - u'$, insbesondere ist s_U die eindeutige Involution mit

$$V_1(s_U) = U \quad \text{und} \quad V_{-1}(s_U) = U^\perp.$$

Dies rechtfertigt den Namen „Spiegelung an U“. Die Spiegelung an $U^\perp$ ist dann gegeben durch $s_{U^\perp} = -s_U = \mathrm{Id} - 2\pi_U$.

Proposition 7.3.10. *Ist B nicht-ausgeartet und $U < V$ regulär, so gilt für die Spiegelung s_U, dass*

$$s_U \in \mathrm{Aut}(V,B) \quad \text{und} \quad \det(s_U) = (-1)^{\dim V - \dim U}.$$

Beweis. Es seien $v_1, v_2 \in V$. Für $j \in \{1,2\}$ setzen wir $u_j := \pi_U^\perp(v_j)$ und $u'_j := \pi_{U^\perp}^\perp(v_j)$. Dann gilt

$$\begin{aligned} B(s_U(v_1), s_U(v_2)) &= B(u_1 - u'_1, u_2 - u'_2) = B(u_1,u_2) - B(u'_1,u_2) - B(u_1,u'_2) + B(u'_1,u'_2) \\ &= B(u_1,u_2) + B(u'_1,u'_2) = B(u_1,u_2) + B(u'_1,u_2) + B(u_1,u'_2) + B(u'_1,u'_2) \\ &= B(u_1+u'_1, u_2+u'_2) = B(v_1,v_2), \end{aligned}$$

also $s_U \in \mathrm{Aut}(V,B)$. Der 1-Eigenraum von s_U ist U und der (-1)-Eigenraum ist $U^\perp$. Die geometrischen Vielfachheiten von 1 bzw. -1 sind daher $\dim U$ und $\dim U^\perp$. Da s_U diagonalisierbar ist, sind dies auch die algebraischen Vielfachheiten, und folglich

$$\det(s_U) = 1^{\dim U} \cdot (-1)^{\dim U^\perp} = (-1)^{\dim V - \dim U}. \qquad \square$$

Beispiel 7.3.11 (Hyperebenenspiegelungen)**.** Es sei (V,B) wie in Konstruktion 7.3.9 und $H < V$ eine Hyperebene (d.h. $\dim H = \dim V - 1$). H ist genau dann regulär, wenn $H^\perp$ regulär ist, und aus Dimensionsgründen ist $H^\perp = \mathbb{K}v$ eine Gerade und daher genau dann regulär, wenn sie anisotrop ist. Die regulären Hyperebenen sind also genau die Hyperebenen der Form

$$H = v^\perp := \{u \in V \mid u \perp v\} \quad \text{mit} \quad B(v,v) \neq 0. \tag{7.3.2}$$

Falls B symmetrisch (oder hermitesch mit imaginärer Einheit) und $\mathrm{char}(\mathbb{K}) \neq 2$ ist, dann existieren solche Hyperebenen immer.

Ist H die durch (7.3.2) gegebene reguläre Hyperebene, so gilt $\pi_{H^\perp}(u) = \pi_{\mathbb{K}v}(u) = \frac{B(u,v)}{B(v,v)}v$ und daher

$$s_H(u) = u - 2 \cdot \frac{B(u,v)}{B(v,v)} v.$$

Weiter gilt $\det(s_H) = -1$.

Bemerkung 7.3.12. Ist $\mathbb{K}$ ein Körper der Charakteristik 2, so sind Spiegelungen nicht sehr interessant: Es gilt dann ja $-1 = 1$ und daher ist jede Spiegelung die Identität! Wir nehmen daher ab jetzt an, dass $\mathrm{char}(\mathbb{K}) \neq 2$.

Ist B schiefsymmetrisch, so gibt es zwar interessante Spiegelungen, aber keine Hyperebenenspiegelungen (Warum?). Hyperebenenspiegelungen sind daher vor allem in orthogonalen und hermiteschen Vektorräumen interessant.

Bemerkung 7.3.13 ((Pseudo-)Drehungen)**.** Es sei jetzt (V,B) ein orthogonaler oder hermitescher Vektorraum (über einem Körper der Charakteristik $\neq 2$). Nach Beispiel 7.3.11 sind dann beliebige Produkte von Hyperebenspiegelungen Automorphismen von (V,B). Ist speziell B_0 das Standardskalarprodukt auf $\mathbb{R}^n$, so sind die Produkte von zwei Hyperebenenspiegelungen genau die Drehungen um eine Achse der Kodimension 2 (vgl. die Übungen) und die Identität. In allgemeinen orthogonalen oder hermiteschen Vektorräumen bezeichnet man Produkte von genau *zwei* Hyperebenenspielgelungen daher gelegentlich auch als *Pseudodrehungen*. Man beachte, dass Pseudodrehungen die Determinante 1 haben.

Bemerkung 7.3.14 (Bahnen der orthogonalen Gruppe)**.** Es sei (V,B) ein orthogonaler Vektorraum und $v,w \in V$. Existiert ein $\Phi \in \mathrm{O}(V,B)$ mit $\Phi(v) = w$, so muss insbesondere

$$B(v,v) = B(w,w) \tag{7.3.3}$$

gelten. Umgekehrt gelte (7.3.3) - kann man dann stets ein $\Phi \in \mathrm{O}(V,B)$ finden, das v auf w abbildet? Die Antwort lautet „Nein!“, denn ist $v \neq 0$ ein isotroper Vektor, so kann man v natürlich

nicht mittels eines Automorphismus auf den Nullvektor abbilden. Um diesen Fall auszuschließen, nehmen wir nun an, dass

$$B(v,v) = B(w,w) \neq 0 \tag{7.3.4}$$

gilt. Wir unterscheiden dann zwei Fälle:

FALL 1: $v - w$ ist anisotrop.

Dann rechnet man nach, dass $s_{(v-w)^\perp}(v) = w$ gilt. Man findet also eine Hyperebenenspiegelung, die v auf w abbildet. Falls B total anisotrop ist, kann man also je zwei anisotrope Vektoren deselben „Länge“ durch eine Hyperebenenspiegelung aufeinander abbilden. (In der euklidischen Ebene tut man diese durch Spiegelung an der Mittelsenkrechten!)

FALL 2: $v - w$ ist isotrop

In diesem Fall rechnet man (unter Verwendung der Annahme, dass $B(v,v) = B(w,w) \neq 0$) nach, dass w und $v+w$ anisotrop sind und $s_{w^\perp} \circ s_{(v+w)^\perp}(v) = w$ gilt. Man findet also eine Pseudodrehung, die v auf w abbildet.

Damit haben wir gezeigt:

Korollar 7.3.15. *Es sei (V,B) ein orthogonaler Vektorraum und $v \in V$ ein anisotroper Vektor. Dann gilt*

$$\mathrm{Bahn}_{\mathrm{O}(V,B)}(v) := \{\Phi(v) \mid \Phi \in \mathrm{O}(V,B)\} = \{w \in V \mid B(w,w) = B(v,v)\}. \qquad \square$$

Für $R \in \mathbb{K}$ heißt die Menge $S_R(V,B) := \{v \in V \mid B(v,v) = R\}$ eine *Pseudosphäre* von (V,B). Für $R \neq 0$ sind diese also genau die Bahnen von $\mathrm{O}(V,B)$. Die Pseudosphäre $S_0(V,B)$ kann aus mehreren Bahnen bestehen (z.B. ist $\{0\}$ immer eine Bahn, aber im isotropen Fall nicht ganz $S_0(V,B)$).

Beispiel 7.3.16. Motiviert durch Korollar 7.3.15 schauen wir uns nun an, wie Pseudosphären in konkreten Beispielen aussehen:

(i) Sei $V = \mathbb{R}^n$ und $B = B_0$ das Standardskalarprodukt. Für $R \geq 0$ ist $S_R(\mathbb{R}^n, B_0)$ die Sphäre vom Radius $\sqrt{R}$ um den Ursprung, und für $R < 0$ ist $S_R(\mathbb{R}^n, B_0) = \emptyset$. In diesem Sinne verallgemeinern also Pseudosphären die gewöhnlichen Sphären. Korollar 7.3.15 besagt in diesem Zusammenhang, dass man mittels einer Transformation aus $\mathrm{O}(\mathbb{R}^n, B_0)$ jeden Punkt auf einer Sphäre auf jeden anderen Punkt derselben Sphäre abbilden kann.

(ii) Sei $V = \mathbb{R}^2$ und B die anisotrope Bilinearform gegeben durch $B(x,y) = x_1y_1 + 2x_2y_2$. Für $R > 0$ ist dann $S_R(\mathbb{R}^n, B)$ eine Ellipse um den Ursprung, die für $R = 0$ zum Ursprung degeneriert. Für $R < 0$ ist $S_R(\mathbb{R}^n, B) = \emptyset$. Man nennt daher (V,B) auch eine *elliptische Ebene*.

(iii) Sei $V = \mathbb{R}^2$ und $B = B_{1,1}$ die Minkowski-Form, d.h. die isotrope Bilinearform gegeben durch $B(x,y) = x_1y_1 - x_2y_2$. Für $R \neq 0$ ist dann $S_R(\mathbb{R}^n, B)$ eine Hyperbel mit zwei Ästen, die für $R = 0$ zum Koordinatenkreuz degeneriert. Man nennt daher (V,B) auch eine *hyperbolische Ebene*[14]. Speziell für $R = 1$ erhalten wir die *Einheitshyperbel* $H := S_1(\mathbb{R}^n, B)$ (vgl. Abbildung 7.1). Diese ist gegeben durch

$$H = H_- \sqcup H_+ \quad \text{mit} \quad H_\pm := \left\{x \in H \mid x_1^2 - x_2^2 = 1 \text{ und } \pm x_1 > 0\right\},$$

[14] Der Begriff „hyperbolische Ebene“ hat leider in der Geometrie zwei Bedeutungen. In der Geometrie der Bilinearformen ist damit eine Ebene gemeint, deren Pseudosphären Hyperbeln sind. In der Differentialgeometrie ist damit ein ganz anderes geometrisches Objekt gemeint, und die Wikipedia-Seite von „Hyperbolische Ebene“ beschreibt dieses andere Objekt.

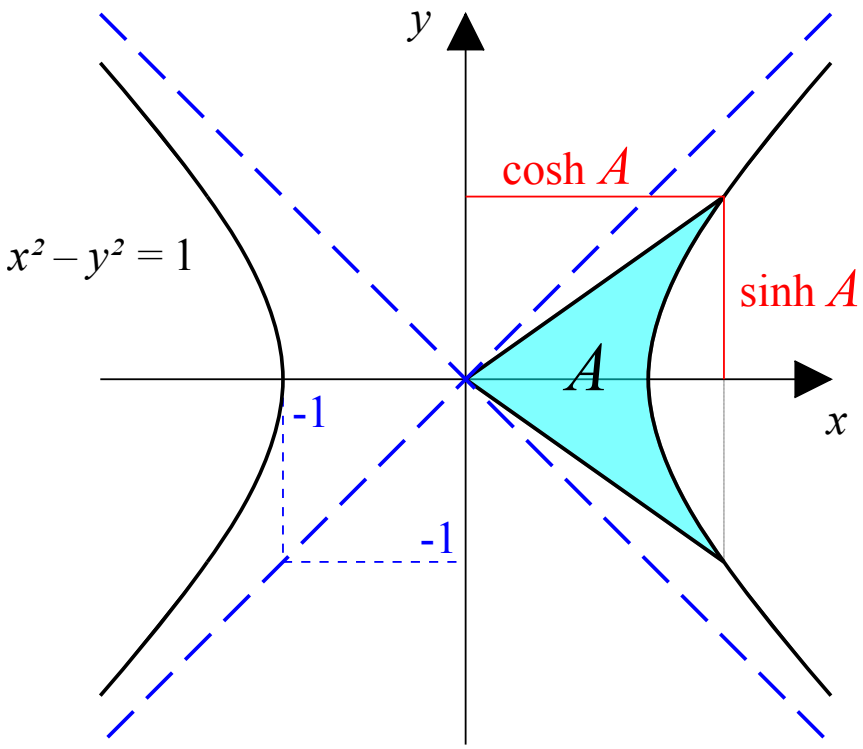


Abbildung 7.1: Parametrisierung der Einheitshyperbel
(Quelle:https://de.wikipedia.org/wiki/Hyperbelfunktion)

wobei H_- den linken Ast und H_+ den rechten Ast bezeichnet. Genauso, wie man die Punkte auf dem Einheitskreis durch trigonometrische Funktionen parametrisieren kann, kann man die Punkte auf den beiden Ästen der Einheitshyperbel durch Hyperbelfunktionen parametrisieren: Ist $\cosh(x) = \frac{1}{2}(e^x + e^{-x})$ und $\sinh(x) := \frac{1}{2}(e^x - e^{-x})$, so gilt (Übung!)

$$H_+ = \left\{ \begin{pmatrix} \cosh(t) \\ \sinh(t) \end{pmatrix} \mid t \in \mathbb{R} \right\} \quad \text{und} \quad H_- = \left\{ \begin{pmatrix} -\cosh(t) \\ \sinh(t) \end{pmatrix} \mid t \in \mathbb{R} \right\}.$$

Diese Parametrisierung ist dadurch eindeutig bestimmt, dass die Verbindungsstrecken vom Ursprung zu $\begin{pmatrix} \cosh(t) \\ \sinh(t) \end{pmatrix}$ und $\begin{pmatrix} \cosh(-t) \\ \sinh(-t) \end{pmatrix} = \begin{pmatrix} \cosh(t) \\ -\sinh(t) \end{pmatrix}$ mit dem Hyperbelast H_+ eine Fläche vom Flächeninhalt t einschließt (vgl. Abbildung 7.1).

Pseudosphären sind Beispiele für Quadriken, und reelle 2-dimensionale Pseudosphären sind sogenannte Kegelschnitte. Wir werden Quadriken und Kegelschnitte später klassifizieren.

Beispiel 7.3.17 (Hyperbolische Pseudodrehungen)**.** Wir bestimmen die orthogonale Gruppe der Minkowski-Ebene $\mathbb{R}^{1,1} = (\mathbb{R}^2, B_{1,1})$, wobei $B_{1,1}(x,y) = x_1y_1 - x_2y_2$. Bzgl. der Standardbasis hat $B_{1,1}$ die darstellende Matrix $D := \operatorname{diag}(1,-1)$. Ist $A \in \mathrm{GL}_2(\mathbb{R})$ eine invertierbare Matrix und $\Phi_A(x) := Ax$, so gilt $\Phi_A \in \mathrm{SO}(\mathbb{R}^2, B)$ genau dann, wenn $\det(A) = 1$ und $A^\top DA = D$. Nun ist aber

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Longrightarrow \det(A) = ad - bc \quad \text{und} \quad A^\top DA = \begin{pmatrix} a^2 - c^2 & ab - cd \\ ab - cd & b^2 - d^2 \end{pmatrix}.$$

In diesem Fall ist also Φ_A orthogonal genau dann, wenn

$$\begin{cases} ad - bc &= 1, \\ a^2 - c^2 &= 1, \\ b^2 - d^2 &= -1, \\ ab - cd &= 0. \end{cases} \tag{7.3.5}$$

Die zweite und dritte Gleichung bedeuten, dass $x := \begin{pmatrix} a \\ c \end{pmatrix}$ und $y := \begin{pmatrix} d \\ b \end{pmatrix}$ auf der Einheitshyperbel H liegen. Wir nehmen zunächst an, dass $a \geq 0$, so dass x auf dem rechten Ast H_+ liegt. Dies bedeutet gerade, dass

$$a = \cosh(t) \quad \text{und} \quad c = \sinh(t) \quad \text{für ein } t \in \mathbb{R}.$$

Dass y auf der Einheitshyperbel liegt, bedeutet andererseits, dass

$$d = \pm\cosh(s) \quad \text{und} \quad b = \sinh(s) \quad \text{für ein } s \in \mathbb{R},$$

wobei es für das Vorzeichen von d zwei Möglichkeiten gibt. Die erste und vierte Gleichung von (7.3.5) liefern dann

$$\pm\cosh(t)\cosh(s) - \sinh(t)\sinh(s) = 1 \quad \text{und} \quad \cosh(t)\sinh(s) \mp \sinh(t)\cosh(s) = 0.$$

Die zweite dieser Gleichungen liefert

$$\sinh(t) = \pm\cosh(t) \cdot \frac{\sinh(s)}{\cosh(s)},$$

und Einsetzen in die erste Gleichung liefert dann

$$\begin{aligned} & \pm\cosh(t)\cosh(s) \mp \cosh(t)\cdot\frac{\sinh^2(s)}{\cosh(s)} = 1 \\ \Longrightarrow\quad & \cosh(t)\cdot(\cosh^2(s)-\sinh^2(s)) = \pm\cosh(s) \\ \Longrightarrow\quad & \cosh(t) = \pm\cosh(s). \end{aligned}$$

Dies zeigt, dass das Vorzeichen ein „+“ sein muss und dass $s = \pm t$ ist. Falls $a \geq 0$ ist, haben wir also die notwendige Bedingung

$$a = \cosh(t), \quad b = \sinh(t), \quad c = \sinh(\pm t) = \pm\sinh(t) \quad \text{und} \quad d = \cosh(\pm t) = \cosh(t).$$

Falls $c = -\sinh(t)$, so ist

$$1 = \det(A) = \cosh^2(t) + \sinh^2(t) = (\cosh(t)^2 - \sinh^2(t)) + 2\sinh^2(t) = 1 + 2\sinh^2(t) \Longrightarrow \sinh^2(t) = 0.$$

Dies impliziert $t = 0$, also gilt auch in diesem Fall $c = \sinh(t)$. Unter der Annahme $a \geq 0$ erhalten wir also die notwendige Bedingung

$$A = \begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix} \quad \text{mit } t \in \mathbb{R}. \tag{7.3.6}$$

Ist hingegen $a \leq 0$, so können wir dieses Argument auf die Matrix $-A$ anwenden (weil A die Gleichung $A^\top DA = D$ genau dann löst, wenn $-A$ diese Gleichung löst). Es gilt dann

$$A = -\begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix} \quad \text{mit } t \in \mathbb{R}. \tag{7.3.7}$$

Jede Matrix in $\mathrm{SO}(\mathbb{R}^{1,1})$ muss daher von der Form (7.3.6) oder (7.3.7) sein. Umgekehrt rechnet man leicht nach, dass diese Matrizen (7.3.5) erfüllen. Es gilt daher

$$\mathrm{SO}(\mathbb{R}^{1,1}) = \left\{ \Phi_A \in \mathrm{GL}(\mathbb{R}^2) \mid \exists\, t \in \mathbb{R} :\ A = \pm\begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix} \right\}$$

Wir werden später noch sehen, dass alle Elemente von $\mathrm{SO}(\mathbb{R}^{1,1})$ Pseudodrehungen sind - man nennt diese Elemente daher auch *hyperbolische Pseudodrehungen*. Die darstellenden Matrizen solcher Pseudodrehungen sind den Drehmatrizen sehr ähnlich, nur nur dass hier statt den trigonometrischen Funktionen die Hyperbelfunktionen verwendet werden und alle Vorzeichen gleich sind. Je nach Vorzeichen von A gilt entweder

$$\Phi_A(e_1) = \begin{pmatrix} \cosh(t) \\ \sinh(t) \end{pmatrix} \quad \text{oder} \quad \Phi_A(e_1) = \begin{pmatrix} -\cosh(t) \\ -\sinh(t) \end{pmatrix} = \begin{pmatrix} -\cosh(-t) \\ \sinh(-t) \end{pmatrix}.$$

Dies zeigt insbesondere, dass man e_1 mittels einer hyperbolischen Pseudodrehung auf jeden beliebigen anderen Punkt der Einheitshyperbel abbilden kann (genau wie man e_1 mittels einer euklidischen Drehung auf jeden beliebigen anderen Punkt des Einheitskreises abbilden kann).

[31.05.24]

Bemerkung 7.3.18 (Bahnen der speziellen orthogonalen Gruppe)**.** Im Beispiel 7.3.17 haben wir gesehen, dass in $\mathbb{R}^{1,1}$ bereits die spezielle orthogonale Gruppe ausreicht um beliebige Punkte einer Pseudosphäre $S_R(V,B)$ mit $R \neq 0$ aufeinander abzubilden. Dies gilt auch ganz allgemein: Ist (V,B) ein orthogonaler Vektorraum und $v \in V$ ein anisotroper Vektor, so ist $v^\perp$ regulär und erhält daher einen anisotropen Vektor u. Es ist dan $H = u^\perp$ eine reguläre Hyperebene mit $v \in H$, und daher $s_H(v) = v$. Ist nun $w \in V$ ein anderer Vektor mit $B(v,v) = B(w,w) \neq 0$, so finden wir nach Korollar 7.3.15 ein $\Phi \in \mathrm{O}(V,B)$ mit $\Phi(v) = w$, und daher auch $(\Phi \circ s_H)(v) = w$. Einer der beiden Automorphismen Φ oder $\Phi \circ s_H$ hat dann die Determinante 1, und folglich gilt

$$\mathrm{Bahn}_{\mathrm{SO}(V,B)}(v) := \{\Phi(v) \mid \Phi \in \mathrm{SO}(V,B)\} = \{w \in V \mid B(w,w) = B(v,v)\}. \tag{7.3.8}$$

Satz 7.3.19 (Satz von Cartan[15]-Dieudonné[16])**.** *Es sei (V,B) ein orthogonaler Vektorraum und* $\mathrm{char}(\mathbb{K}) \neq 2$*. Dann existiert ein $N \in \mathbb{N}$, so dass jedes $\Phi \in \mathrm{O}(V,B)$ als Produkt von höchstens N Spiegelungen an regulären Hyperebenen geschrieben werden kann.*

Fassen wir die Identität als „Produkt von 0 Spiegelungen“ auf, so ist die optimale Konstante N im Satz von Cartan-Dieudonné gegeben durch $N = \dim V$. Wir beweisen den Satz hier nur mit der schwächeren Konstante $N = 2\dim V$.

Beweis von Satz 7.3.19. Sei $g \in \mathrm{O}(V,B)$. Wir zeigen durch Induktion nach $n := \dim V$, dass g ein Produkt von höchstens $2n$ Hyperebenenspiegelungen ist.

Sei zunächst $\dim V = 1$ und $v \in V \setminus \{0\}$. Lineare Abbildungen von V nach V und Bilinearformen auf V werden also bzgl. der Basis $\mathscr{B} := (v)$ dann durch (1×1)-Matrizen dargestellt. Sei also $D_{\mathscr{B}}(B) = (\lambda)$ und $\Phi : V \to V$ linear mit $D_{\mathscr{B}}(\Phi) = (\mu)$. Da B nicht-ausgeartet ist, muss gelten $\lambda \neq 0$. Es gilt dann

$$\Phi \text{ orthogonal} \iff (\mu)^\top(\lambda)(\mu) = (\lambda) \iff \mu^2\lambda = \lambda \overset{\lambda\neq 0}{\iff} \mu^2 = 1 \iff \mu \in \{-1,1\} \iff \Phi \in \{-\mathrm{Id}, \mathrm{Id}\}.$$

Die einzige Hyperebene in V ist $H = \{0\}$ und es gilt $s_H = -\mathrm{Id}$. Folglich ist jede orthogonale Abbildung ein Produkt von höchstens $2 = 2n$ Spiegelungen (in Wahrheit sogar von höchstens $1 = n$ Spiegelungen.)

Sei nun $\dim V = n \geq 2$ und $g \in \mathrm{O}(V,B)$. Wir wählen eine OGB $\mathscr{B} = (v_1, \ldots, v_n)$ von V. Es gilt dann $D_{\mathscr{B}}(B) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ und - da B nicht-ausgeartet ist - ist die Determinante $\lambda_1 \cdots \lambda_n$ nicht 0. Insbesondere gilt $B(v_1, v_1) = \lambda_1 \neq 0$, und $W := v_1^\perp = \langle v_2, \ldots, v_n \rangle$ ist ein regulärer Unterrraum von V, d.h. $(W, B|_{W\times W})$ ist ein orthogonaler Vektorraum der Dimension $n-1$.

Es sei nun $v := g(v_1)$ und $w := v_1$. Da g orthogonal ist, gilt dann $B(v,v) = B(w,w) \neq 0$. Nach Bemerkung 7.3.14 existiert also entweder eine Hyperebenenspiegelung s mit $s(v) = w$ oder es existieren zwei Hyperebenenspiegelungen s_1, s_2 mit $s_1 \circ s_2(v) = w$. Im ersten Fall setzen wir $h := s \circ g$, und im zweiten Fall setzen wir $h := s_1 \circ s_2 \circ g$. Es gilt dann

$$h(v_1) = s(g(v_1)) = s(v) = w = v_1 \quad \text{bzw.} \quad h(v_1) = (s_1 \circ s_2)(g(v_1)) = s_1 \circ s_2(v) = w = v_1,$$

also in beiden Fällen $h(v_1) = v_1$. Da h orthogonal ist, gilt dann aber auch $h[W] \subseteq W$. d.h. W ist h-invariant. Da h orthogonal ist, ist auch der induzierte Endomorphismus h_W orthogonal, d.h. $h_W \in \mathrm{O}(W, B|_{W\times W})$. Nach Induktionsvoraussetzung kann h_W daher als Produkt von höchstens $2n-2$ Hyperebenenspiegelungen in W geschrieben werden kann.

[15] Élie Cartan (1869–1951), frz. Mathematiker

[16] Jean Dieudonné (1906-1992), frz. Mathematiker und Schriftführer der Gruppe Bourbaki, die Mitte des 20. Jahrhunderts die Grundlagen der modernen Mathematik erstmals in enzyklopädischer Form niederlegte

Ist H_W eine Hyperebene in W, so ist H_W orthogonal (bzgl. $B|_{W\times W}$) zu einem anisotropen Vektor $w_0 \in W$ und $H := w_0^\perp$ ist dann eine Hyperebene in V, die H_W und v_1 enthält. Es gilt dann

$$s_H(\lambda v_1 + w) = \lambda v_1 + s_{H_W}(w) \quad (\lambda \in \mathbb{K}, w \in W),$$

d.h. die Hyperebenenspiegelungen in W setzen sich zu Hyperebenenspiegelungen in V fort, die v_1 fixieren. Ist h_W ein Produkt von Hyperebenenspiegelungen in W, so ist h wegen $h(v_1) = v_1$ das Produkt der entsprechend fortgesetzten Hyperebenenspiegelungen in V. Es ist daher h ein Produkt von höchstens $(2n-2)$ Hyperebenenspiegelungen, und da entweder $g = s \circ h$ oder $g = s_2 \circ s_1 \circ h$ gilt, ist g ein Produkt von höchstens $2n$ Hyperebenenspiegelungen. □

Bemerkung 7.3.20 (Folgerungen aus dem Satz von Cartan-Dieudonné)**.** Unser Beweis des Satzes on Cartan-Dieudonné impliziert noch die folgenden Aussagen:

(1) Die orthogonale Gruppe wird von Spiegelungen an regulären Hyperebenen erzeugt. Da diese die Determinante -1 besitzen, folgt mit der Multiplikativität der Determinante, dass $\det[\mathrm{O}(V,B)] = \{-1,1\}$ gilt. Man sieht dies auch sehr einfach direkt: Ist $\mathscr{B}$ eine geordnete Basis von V und besitzen B und $\Phi \in \mathrm{O}(V,B)$ die darstellenden Matrizen A bzw. T bzgl. $\mathscr{B}$, so gilt $T^\top A T = A$ und daher $\det(T^2)\det(A) = \det(A)$, also $\det(T^2) = 1$ und daher $\det(T) \in \{\pm 1\}$.

(2) Im Induktionsschritt des Beweises von Satz 7.3.19 haben wir entweder Fall 1 oder Fall 2 aus Bemerkung 7.3.14 verwendet. verwendet, je nachdem, ob $v - w$ anisotrop oder isotrop war. Ist B total anisotrop, so sind wir immer im ersten dieser beiden Fälle, und brauchen daher immer nur eine Spiegelung (statt zwei), um v auf w abzubilden. Daher zeigt unser Beweis im total anisotropen Fall, dass jede orthogonale Abbildung ein Produkt von höchstens $\dim V$ (statt $2\dim V$) Hyperebenenspiegelungen ist. Diese schärfere Schranke gilt auch allgemein, aber der allgemeine Beweis benötigt zusätzliche Ideen.

(3) Es sei nun $\Phi \in \mathrm{SO}(V,B)$. Nach dem Satz von Cartan-Dieudonné existieren dann Hyperebenenspiegelungen $s_1, \dots, s_m$ mit $m \le 2\dim V$ (bzw. eigentlich $m \le \dim V$), so dass $\Phi = s_1 \cdots s_m$. Wegen $1 = \det(\Phi) = \prod \det(s_j) = (-1)^m$ ist $m = 2k$ gerade, und daher ist $\Phi = (s_1 s_2) \cdots (s_{2k-1} s_{2k})$ das Produkt von $k \le \dim V$ (bzw. eigentlich $k \le \lfloor \dim V/2 \rfloor$) Pseudodrehungen. Ist $\dim V \le 3$, so ist also jedes Element von $\mathrm{SO}(V,B)$ eine Pseudodrehung, aber ab Dimension 4 ist das nicht länger der Fall.

(4) Speziell gilt: Jedes Element von $\mathrm{SO}(\mathbb{R}^2, B_0)$ oder $\mathrm{SO}(\mathbb{R}^3, B_0)$ eine Drehung (um den Ursprung bzw. um eine Ursprungsgerade). Insbesondere sind Produkte von Drehungen wieder Drehungen. Ab Dimension 4 ist das nicht mehr der Fall. Das ist ein Beispiel dafür, dass wir uns nicht zu sehr auf unsere niedrig-dimensionale Intuition verlassen sollten.

(5) Ist $B_{1,1}$ die Minkowksi-Form und $\mathbb{R}^{1,1} = (\mathbb{R}^2, B_{1,1})$ die Minkowski-Ebene (also ein Modell der isotropen Standard-Ebene), so sind alle Elemente von $\mathrm{SO}(\mathbb{R}^2, B)$ Pseudodrehungen. Dies zeigt, dass die Produkte von zwei Hyperebenenspiegelungen in der Minkowski-Ebene genau die hyperbolischen Pseudodrehungen sind, was den Namen „hyperbolische Pseudodrehung“ nachträglich rechtfertigt.

Bemerkung 7.3.21 (Bewegungsgruppen)**.** In Korollar 7.1.49 haben wir gesehen, dass die Isometrien des euklidischen Raums durch die Gruppe der euklidischen Bewegungen gegeben ist.

Dies motiviert ein näheres Studium dieser Gruppe. Allgemeiner kann man zu jedem orthogonalen Vektorraum (V,B) die zugehörige *Bewegungsgruppe* $\mathrm{Mot}(V,B)$ studieren. Diese ist definiert als die Menge aller Abbildungen der Form

$$\Phi : V \to V, \quad \Phi(v) = \Phi_0(v) + w$$

mit $\Phi_0 \in \mathrm{O}(V,B)$ und $w \in V$, und man rechnet leicht nach, dass dies tatsächlich eine Gruppe unter Verkettung von Abbildungen ist. Dazu ist die folgende Beschreibung hilfreich: Nach Wahl einer Basis dürfen wir annehmen, dass $V = \mathbb{K}^n$ gilt; dann ist jedes $\Phi \in \mathrm{Mot}(V,B)$ von der Form

$$\Phi(v) = \Phi_{A,w}(v) = Aw + v$$

für eine bzgl. B orthogonale Matrix A und einen Vektor w. Wir definieren dann die *erweiterte Matrix* zu $\Phi_{A,w}$ als

$$M(\Phi_{A,w}) := \begin{pmatrix} A & w \\ 0 & 1 \end{pmatrix} \in \mathbb{K}^{(n+1)\times(n+1)}.$$

Es folgt dann aus

$$(\Phi_{A_1,w_1} \circ \Phi_{A_2,w_2})(v) = A_1(A_2 v + w_2) + w_1 = A_1A_2w + (w_1 + A_1w_2),$$

dass

$$M(\Phi_{A_1,w_1} \circ \Phi_{A_2,w_2}) = \begin{pmatrix} A_1A_2 & w_1 + A_1w_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A_1 & w_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A_2 & w_2 \\ 0 & 1 \end{pmatrix},$$

und daher liefert die Abbildung $M : \mathrm{Mot}(V,B) \to \mathrm{GL}_{n+1}(\mathbb{K})$ einen injektiven Gruppenhomomorphismus. Man kann also mit Bewegungen rechnen wie mit Matrizen.

Da die orthogonale Gruppe von Spiegelungen an regulären Hyperebenen erzeugt wird, wir die zugehörige Bewegungsgruppe von solchen Spiegelungen und Translationen erzeugt.

Konstruktion 7.3.22 (Affine Hyperebenenspiegelugen)**.** Es sei (V,B) ein orthogonaler Vektorraum über einem Körper der Charakteristik $\neq 2$. Ist $U < V$ ein regulärer Unterraum und $v \in V$, so nennen wir $v+U$ eine *regulären affinen Unterraum*. Ist U eine reguläre Hyperebene, so nennen wir $v+U$ entsprechend eine *reguläre affine Hyperebene*. In der Schule haben Sie Spiegelungen an affine Geraden und Ebenen im $\mathbb{R}^2$ und $\mathbb{R}^3$ gesehen. Ganz allgemein definiert man die *affine Hyperebenenspiegelung* an einer regulären affinen Hyperebene $v+U$ durch

$$s_{v+U}(w) := s_U(w - v) + v.$$

Man rechnet nach, dass dies eine Bewegung von (V,B) mit $s_{v+U}|_{v+U} = \mathrm{Id}$ ist, die nur von $v+U$ (also nicht von der Wahl von v) abhängt.

Bemerkung 7.3.23 (Ausblick)**.** In den Übungen werden Sie zeigen, dass man jede Translation als Produkt von affinen Hyperebenenspiegelungen schreiben kann. Daraus folgt dann, dass die Bewegungsgruppe $\mathrm{Mot}(V,B)$ von Spiegelungen an regulären affinen Hyperebenen erzeugt wird. Insbesondere ist jede Isometrie des n-dimensionalen euklidischen Raums ein Produkt von Spiegelungen an Hyperebenen. Im Fall der euklidischen Ebene kann man zeigen, dass drei Geradenspiegelungen ausreichen, um jede beliebige Bewegung zu erzeugen. Dies ist der berühmte Dreispiegelungssatz der euklidischen Geometrie – mehr dazu in der Vorlesung ELEMENTARE GEOMETRIE.

Bemerkung 7.3.24 (Spiegelungen in hermiteschen Vektorräumen)**.** Auch in hermiteschen Vektorräumen kann man Spiegelungen an regulären Hyperebenen definieren. Diese sind aber weniger nützlich, weil sie nicht ausreichen, um die unitäre Gruppe zu erzeugen. Beispielsweise gibt es in $(\mathbb{C}^1, B_0)$ nur eine Hyperebenenspiegelung (nämlich $z \mapsto -z$), aber

$$U(\mathbb{C}^1, B_0) = \{(w) \in \mathbb{C}^{1\times 1} \mid |w|^2 = 1\}$$

ist der Einheitskreis und besitzt daher unendlich viele Elemente.

Allgemein müssen Produkte von Hyperebenenspiegelungen immer die Determinante 1 oder -1 besitzen. Was kann man über Determinanten allgemeiner unitärer Abbildungen sagen? Dazu sei (V,B) ein hermitescher Vektorraum über $(\mathbb{K},\sigma)$ und $\mathscr{B}$ eine geordnete Basis von V. Besitzen B und $\Phi \in \mathrm{U}(V,B)$ die darstellenden Matrizen A bzw. T bzgl. $\mathscr{B}$, so gilt

$$T^\top A\sigma(T) = A \implies \det(T)\det(A)\sigma(\det(T)) = \det(A) \implies \det(T)\sigma(\det(T)) = 1.$$

Anders als im orthogonalen Fall folgt daraus aber nicht, dass $\det(T) \in \{\pm 1\}$ gilt, sondern die Determinante kann wie oben gesehen im Allgemeinen beliebige Werte λ mit $\lambda\sigma(\lambda) = 1$ annehmen.

Bemerkung 7.3.25 (Unitäre Gruppen komplex-hermitescher Vektorräume)**.** Wir betrachten nun einen hermiteschen Vektorraum (V,B) über dem Körper der komplexen Zahlen (mit komplexer Konjugation). Fassen wir V als *reellen* Vektorraum auf, so ist

$$B_\mathbb{R} : V \times V \to \mathbb{R}, (v,w) \mapsto \mathrm{Re}((B(v,w)) = \frac{1}{2}(B(v,w) + \overline{B(v,w)}) = \frac{1}{2}(B(v,w) + B(w,v))$$

eine symmetrische reelle Bilinearform. Für alle $v \in V$ gilt dann

$$B(v,v) = \overline{B(v,v)} \implies B(v,v) \in \mathbb{R} \implies B(v,v) = \overline{B(v,v)} = \mathrm{Re}(B(v,v)) = B_\mathbb{R}(v,v) \tag{7.3.9}$$

Falls $\Phi \in \mathrm{GL}(V)$ die Form B erhält, so erhält Φ auch $B_\mathbb{R}$, und daher gilt

$$\mathrm{U}(V,B) \subseteq \mathrm{O}(V,B_\mathbb{R}). \tag{7.3.10}$$

Jedes Element von $\mathrm{U}(V,B)$ kann daher als Produkt von Spiegelungen an *reellen* Hyperebenen in $(V,B_\mathbb{R})$ geschrieben werden, nicht aber als Produkt von Spiegelugen an komplexen Hyperebenen in (V,B).

Welche Elemente von $\mathrm{O}(V,B_\mathbb{R})$ sind nun unitär? Ist eine Abbildung $\Phi : V \to V$ komplex-linear, so muss man aus Φ sowohl reelle Skalare als auch i herausziehen können. Die Abbildung Φ ist also genau dann komplex-linear, wenn sie reell-linear ist und $\Phi(iv) = i\Phi(v)$ für alle $v \in V$ gilt. Definieren wir $J : V \to V$, $v \mapsto iv$, so bedeutet letzteres gerade, dass $\Phi \circ J = J \circ \Phi$ gilt. Die Abbildung J heißt die *komplexe Struktur* von V, und wegen $B(J(v)), J(w)) = B(iv, iw) = B(v,w)$ gilt $J \in \mathrm{O}(V,B_\mathbb{R})$. Wir behaupten nun, dass

$$\mathrm{U}(V,B) = \{\Phi \in \mathrm{O}(V,B_\mathbb{R}) \mid \Phi \circ J = J \circ \Phi\} \tag{7.3.11}$$

gilt, dass also $\mathrm{U}(V,B)$ der Zentralisator der komplexen Struktur J in $\mathrm{O}(V,B_\mathbb{R})$ ist. Die Inklusion $\subseteq$ ist nach dem oben Gesagten klar, und ist $\Phi \in \mathrm{O}(V,B_\mathbb{R})$ mit $\Phi \circ J = J \circ \Phi$, so ist Φ komplex-linear und nach (7.3.9) gilt $B(\Phi(v), \Phi(v)) = B(v,v)$ für alle $v \in V$. Mittels Polarisierung folgt daher, dass Φ unitär ist, also gilt (7.3.11).

Bemerkung 7.3.26 (Symplektische Gruppen)**.** Unsere Resultate über orthogonale Gruppen lassen sich nicht auf symplektische Gruppen übertragen: Da es in symplektischen Vektorräumen keine anisotropen Geraden gibt, gibt es auch keine regulären Hyperebenen, an denen man spiegeln könnte, und es gibt auch keine sinnvolle Definition von Pseudosphären. Daher ist erst einmal nicht klar, wie man an Beispiele für symplektische Automorphismen kommen kann. Wir werden in den Übungen eine mögliche Konstruktion konstruieren, die wir hier nur kurz skizzieren:

Ist (V,B) ein symplektischer Vektorraum, so betrachtet man die Menge $\mathscr{L}$ der maximalen isotrope Unterräume (also „Lagrange-Unterräume“) von V. Ist $L \in \mathscr{L}$ und $\Phi \in \mathrm{Sp}(V,B)$, so ist $L' := \Phi(L) \in \mathscr{L}$ (Warum?), und daher liefert Φ einen Vektorraumisomorphismus $L \to L'$. Sind umgekehrt $L,L' \in \mathscr{L}$, so kann man sich überlegen, dass jede sich jede injektive lineare Abbildung $L \to L'$ zu einem $\Phi \in \mathrm{Sp}(V,B)$ fortsetzt. Das liefert dann viele Beispiele für symplektische Abbildungen. Wir werden diese Konstruktion im Detail in den Übungen behandeln.

Zusammenfassung von Abschnitt 7.3

(1) Die Automorphismen eines orthogonalen, hermiteschen oder symplektischen Vektorraums bilden eine Gruppe, genannt die zuhgeörige orthogonale, hermitesche oder symplektische Gruppe.

(2) Die möglichen Matrixeinträge der Automorphismen bzgl. einer festen Basis werden durch eine System quadratischer Gleichungen beschrieben, das aber nur in sehr kleinen Dimensionen explizit gelöst werden kann.

(3) Beispiele für Automorphismen sind Produkte von Spiegelungen an regulären Unterräumen, insbesondere Spiegelungen an regulären Hyperebenen und Pseudodrehungen.

(4) Orthogonale Gruppen werden von Spiegelungen an regulären Hyperebenen erzeugt, spezielle orthogonale Gruppen von Pseudodrehungen. Die zugehörigen Bewegungsgruppen werden von Spiegelungen an affinen regulären Hyperebenen erzeugt.

(5) Unitäre Gruppen komplex-hermitescher Vektorräume entstehen aus orthogonalen Gruppen als Zentralisatoren der komplexen Struktur. Sie werden nicht von Spiegelungen erzeugt.

7.4 Witt-Theorie für orthogonale Vektorräume

Wir kehren nun zu der Frage zurück, wann zwei orthogonale Vektorräume isomorph zueinander sind. Die Grundlagen der entsprechenden Theorie wurde in den 1930er Jahren von Ernst Witt geschaffen.

Es sei ab jetzt $\mathbb{K}$ ein Körper der Charakteristik $\neq 2$. Sind $\lambda_1,\dots,\lambda_n \in \mathbb{K}^\times$ so schreiben wir wie zuvor

$$[\lambda_1,\dots,\lambda_n] := (\mathbb{K}^n, B_{\lambda_1,\dots,\lambda_n}) \quad \text{mit} \quad B_{\lambda_1,\dots,\lambda_n}(v,w) = \lambda_1 v_1 w_1 + \dots + \lambda_n v_n w_n.$$

Jeder orthogonale Vektorraum über $\mathbb{K}$ besitzt eine OGB und ist daher isomorph zu einem dieser orthogonalen Vektorräume. Nach Definition gilt

$$[\lambda_1,\dots,\lambda_n] \cong [\lambda_1] \perp \dots \perp [\lambda_n].$$

Lemma 7.4.1 (Wittsches Kürzungslemma)**.** *Sind $n \geq 2$ und $\lambda_1,\dots,\lambda_n,\mu_1,\dots,\mu_n \in \mathbb{K}^\times$, so gilt*

$$([\lambda_1,\dots,\lambda_n] \cong [\mu_1,\dots,\mu_n]) \wedge (\lambda_1 = \mu_1) \quad \Longrightarrow \quad ([\lambda_2,\dots,\lambda_n] \cong [\mu_2,\dots,\mu_n]).$$

Beweis. Es sei $B := B_{\lambda_1,\dots,\lambda_n}$ und $B' := B_{\mu_1,\dots,\mu_n}$. Nach Annahme existiert ein Isomorphismus $\Phi : (\mathbb{K}^n, B) \to (\mathbb{K}^n, B')$, und es sei $v := \Phi(e_1)$. Es gilt dann

$$B'(v,v) = B(e_1,e_1) = \lambda_1 = \mu_1 = B'(e_1,e_1).$$

Nach Korollar 7.3.15 existiert dann ein $\Psi \in O(\mathbb{K}^n, B')$ mit $\Psi(v) = e_1$. Dann ist

$$\Phi' := \Psi \circ \Phi : (\mathbb{K}^n, B) \to (\mathbb{K}^n, B')$$

ein Isomorphismus mit $\Phi'(e_1) = e_1$. Setzen wir $W := \langle e_2,\dots,e_n\rangle$, so gilt insbesondere

$$\Phi'[W] = \Phi'[e_1^{\perp_B}] = e_1^{\perp_{B'}} = W.$$

Schränken wir nun Φ' aus $W := \langle e_2,\dots,e_n\rangle$, so erhalten wir einen injektiven Endomorphismus $\Phi'' : (W, B|_{W\times W}) \to (W, B'_{W\times W})$, der aus Dimensionsgründen schon surjektiv, also ein Isomorphismus ist. Es gilt also

$$[\lambda_2,\dots,\lambda_n] \cong (W, B|_{W\times W}) \cong (W, B'_{W\times W}) \cong [\mu_2,\dots,\mu_n]. \qquad \square$$

Korollar 7.4.2 (Wittscher Kürzungssatz)**.** *Für orthogonale $\mathbb{K}$-Vektorräume (V_j, B_j) gilt*

$$(V_1,B_1) \perp (V_2,B_2) \cong (V_1,B_1) \perp (V_3,B_3) \Longrightarrow (V_2,B_2) \cong (V_3,B_3).$$

Beweis. Es sei $V_j \cong [\lambda_1^{(j)},\dots,\lambda_{n_j}^{(j)}]$. Unsere Annahme besagt dann, dass

$$[\lambda_1^{(1)},\dots,\lambda_{n_1}^{(1)},\lambda_1^{(2)},\dots,\lambda_{n_2}^{(2)}] \cong [\lambda_1^{(1)},\dots,\lambda_{n_1}^{(1)},\lambda_1^{(3)},\dots,\lambda_{n_3}^{(3)}].$$

Die Behauptung folgt dann, indem wir Lemma 7.4.1 n_1-mal anwenden. $\square$

Korollar 7.4.3 (Eindeutigkeit der Witt-Zerlegung)**.** *Es sei (V,B) ein orthogonaler $\mathbb{K}$-Vektorraum, und es seien*

$$V = E_1 \perp \dots \perp E_r \perp A = E'_1 \perp \dots \perp E'_s \perp A'$$

zwei Witt-Zerlegungen von V. Dann gilt $r = s$ und $(A, B|_{A\times A}) \cong (A', B|_{A'\times A'})$.

Beweis. Wäre $r > s$, so könnten wir durch s-maliges Anwenden von Korollar 7.4.2 auf beiden Seiten die orthogonale Summe von s hyperbolischen Ebenen kürzen. Es gäbe dan einen Isomorphismus

$$E_{s+1} \perp \dots \perp E_r \perp A \cong A',$$

wobei die linke Seite isotrop und die rechte Seite anisotrop ist. Dieser Widerspruch zeig, dass $r \leq s$, und mit einem symmetrischen Argument sieht man $s \leq r$, also $r = s$. Wenden wir nun Korollar 7.4.2 r mal an, so folgt $A \cong A'$. $\square$

Nach Korollar 7.4.3 ist also jeder orthogonale Vektorraum bis auf Isomorphie eindeutig durch seinen *Witt-Index* r und seinen *anisotropen Teil* eindeutig bestimmt. Die Klassifikation der anisotropen Teile führt auf das Studium der sogenannten *Witt-Gruppe* eines Körpers. Theoretisch wird dieses Problem durch gewisse Invarianten gelöst - das wurde 1970 von Milnor vermutet und von 1996 von Voevodsky bewiesen, wofür im 2002 der höchste Preis der Mathematik, die Fields-Medaille, verliehen wurde. Diese Invarianten tatsächlich zu berechnen, ist aber im Allgemeinen schwierig. In jedem Fall ist der Witt-Index die einfachste und wichtigste Invariante einer symmetrischen Bilinearform. Wir wollen nun noch eine andere Interpretation des Witt-Index geben, basierend auf dem folgenden Lemma:

Lemma 7.4.4. *Es sei (V,B) ein orthogonaler Vektorraum und $U < V$ total isotrop mit geordneter Basis $(u_1,\dots,u_m)$. Dann existieren $u'_1,\dots,u'_m \in V$ mit den folgenden Eigenschaften:*

(i) $U' := \langle u'_1,\dots,u'_m\rangle$ *ist total isotrop.*

(ii) $H_j := \langle u_j,u'_j\rangle$ *ist eine reguläre isotrope Ebene mit Witt-Basis* (u_j,u'_j).

(iii) $U \oplus U' = H_1 \perp\!\!\!\perp \dots \perp\!\!\!\perp H_m$.

Beweis. Wir beweisen das Lemma durch Induktion nach m. Den Fall $m = 1$ haben wir bereits im Beweis von Proposition 7.2.38 gezeigt.

Es sei nun $m \geq 2$ und $W := \langle u_2,\dots,u_m\rangle$. Wäre $W^\perp \subseteq u_1^\perp$, so wäre $\mathbb{K}u_1 = (u_1^\perp)^\perp \subseteq (W^\perp)^\perp = W$, also $u_1 \in W$, Widerspruch. Folglich finden wir $w' \in W^\perp$ mit $B(u_1,w') \neq 0$. Durch Normalisieren dürfen wir annehmen, dass $B(u_1,w') = 1$ gilt. Für $\alpha \in \mathbb{K}$ gilt dann $B(u_1,w'+\alpha u_1) = 1$ und

$$B(w'+\alpha u_1, w'+\alpha u_1) = B(w',w') + 2\alpha B(w',u_1) + \alpha^2 B(u_1,u_1) = B(w',w') + 2\alpha.$$

Setzen wir speziell $u'_1 := w' - B(w',w')/2u_1 \in W^\perp$, so folgt $B(u_1,u'_1) = 1$ und $B(u'_1,u'_1) = 0$. Folglich ist H_1 eine reguläre isotrope Ebene mit Witt-Basis (u_1,u'_1) und es gilt $V = H_1 \perp\!\!\!\perp H_1^\perp$ mit $W \subseteq H_1^\perp$. Wenden wir nun die Induktionsvorraussetzung auf $u_2,\dots,u_m \in H_1^\perp$ an, so finden wir nach Induktionsvoraussetzung $u'_2,\dots,u'_m$ mit den gewünschten Eigenschaften. □

Korollar 7.4.5. *Der Witt-Index eines orthogonalen Vektorraums ist die maximale Dimension eines total isotropen Unterraums von V.* □

Bemerkung 7.4.6 (Der ausgeartete Fall)**.** In der obigen Version des Wittschen Kürzungssatzes hatten wir angenommen, dass die Formen B_1,B_2 und B_3 nicht-ausgeartet waren. Wir wollen uns nun noch überlegen, dass diese Annahme gar nicht nötig ist. Es seien also B_1,B_2,B_3 symmetrische Bilinearformen auf $\mathbb{K}$-Vektorräumen V_1,V_2,V_3, wobei wir ausdrücklich erlauben, dass diese ausgeartet sind. Wir fragen uns nun, unter welchen Voraussetzungen die Implikation

$$(V_1,B_1) \perp\!\!\!\perp (V_2,B_2) \cong (V_1,B_1) \perp\!\!\!\perp (V_3,B_3) \quad \Longrightarrow \quad (V_2,B_2) \cong (V_3,B_3) \tag{7.4.1}$$

gilt. Wir wissen bereits, dass dies der Fall ist, wenn B_1, B_2 und B_3 nicht-ausgeartet sind.

Lemma 7.4.7. (7.4.1) *gilt, falls* (V_1,B_1) *total isotrop und* (V_2,B_2) *nicht-ausgeartet ist.*

Beweis. In Matrizensprache besagt dass Lemma gerade, dass Matrizen A_2 und A_3 schon kongruent sind, falls nur

$$A'_2 = \begin{pmatrix} 0 & 0 \\ 0 & A_2 \end{pmatrix} \quad \text{und} \quad A'_3 = \begin{pmatrix} 0 & 0 \\ 0 & A_3 \end{pmatrix},$$

kongruent sind und A_2 invertierbar ist. Die Annahme besagt, dass eine invertierbare Matrix

$$T := \begin{pmatrix} W & X \\ Y & Z \end{pmatrix} \quad \text{mit} \quad A'_2 = T^\top A'_3 T = \begin{pmatrix} * & * \\ * & Z^\top A_3 Z \end{pmatrix}.$$

existiert. Dies impliziert aber gerade, dass

$$A_2 = Z^\top A_3 Z, \quad \text{insbesondere} \quad \det(Z)^2 \det(A_3) = \det(A_2) \neq 0.$$

Letzteres zeigt, dass Z invertierbar ist, also sind A_2 und A_3 kongruent. □

[04.06.24]

Korollar 7.4.8. (7.4.1) *gilt, falls* (V_1, B_1) *total isotrop ist.*

Beweis. Sind R_2 und R_3 die Radikale von V_2 und V_3 und W_2 und W_3 beliebige Komplemente. Für $j \in \{2,3\}$ haben wir

$$V_1 \perp V_j = (V_1 \perp R_j) \perp W_j,$$

wobei $V_1 \perp R_j$ total anisotrop und W_j regulär ist. Das Radikal von $V_1 \perp V_2$ ist daher $V_1 \perp R_j$, und da $V_1 \perp V_2 \cong V_1 \perp V_3$ folgt die Isomorphie der Radikale, also $V_1 \perp R_1 \cong V_1 \perp R_3$, insbesondere $\dim R_1 = \dim R_3$. Anwenden von Lemma 7.4.7 liefert nun,

$$(V_1 \perp R_2) \perp W_2 \cong (V_1 \perp R_3) \perp W_3 \implies W_2 \perp W_3.$$

Da R_1 und R_3 total isotrop von derselben Dimension sind, gilt auch $R_2 \cong R_3$ und daher $V_2 \cong V_3$. □

Korollar 7.4.9 (Wittscher Kürzungssatz, starke Form)**.** (7.4.1) *gilt immer.*

Beweis. Wir zerlegen $V_j = R_j \oplus W_j$ als Radikal plus Komplement für $j = \{1,2,3\}$. Es gilt dann

$$(R_1 \perp R_2) \perp (W_1 \perp W_2) \cong (R_1 \perp R_3) \perp (W_2 \perp W_3),$$

wobei die Radikale $R_1 \perp R_2$ bzw. $R_1 \perp R_3$ wieder dieselbe Dimension haben müssen und mittels Korollar 7.4.8 gekürzt werden können. Es gilt dann $W_1 \perp W_2 \cong W_1 \perp W_3$ und daher $W_2 \cong W_3$ nach Korollar 7.4.2. Wegen $\dim R_2 = \dim R_3$ gilt auch $R_2 \cong R_3$, also $V_2 \cong V_3$. □

Bemerkung 7.4.10 (Eindeutigkeit der Witt-Zerlegung im ausgearteten Fall)**.** Ist B eine ausgeartete Bilinearform auf einem $\mathbb{K}$-Vektorraum V, so folgt aus Korollar 7.4.9, dass die Witt-Zerlegung

$$V \cong E_1 \perp \ldots \perp E_r \perp A \perp V^\perp$$

eindeutig im folgenden Sinne ist: Der *Witt-Index* r und die *Nullität* $\dim V^\perp$ sind durch V eindeutig bestimmt, und der *anisotrope Teil* A ist bis auf Isomorphie durch V eindeutig bestimmt. Die maximale Dimension eines isotropen Unterraums von V ist dann $r + \dim V^\perp$.

Wir schauen uns nun die Klassifikation der orthogonalen Vektorräume über $\mathbb{R}$ und $\mathbb{C}$ an.

Bemerkung 7.4.11 (Reelle Bilinearformen und Signatur)**.** Es sei B eine Bilinearform auf einem reellen Vektorraum V und A eine darstellende Matrix von B bzgl. einer beliebigen Basis. Mittels symmetrischen Gauß können wir A zunächst auf Diagonalform bringen und anschließend alle Diagonaleinträge auf 0, 1 oder -1 normalisieren. Es existieren daher $r_+, r_-, r_0 \in \mathbb{N} \cup \{0\}$ mit $r_+ + r_- + r_0 = \dim V$, so dass

$$(V, B) \cong [\underbrace{1, \ldots, 1}_{r_+}, \underbrace{-1, \ldots, -1}_{r_-}, \underbrace{0, \ldots, 0}_{r_0}],$$

und B ist genau dann nicht-ausgeartet, wenn $r_0 = 0$. Wir überlegen uns nun, dass die Zahlen r_+, r_- und r_0 durch B eindeutig bestimmt sind, also nicht von der Wahl der darstellenden Matrix abhängen. Für die *Nullität* $r_0 = \dim V^\perp$ ist das klar, und für r_+ und r_- folgt dies aus dem folgenden Lemma.

Lemma 7.4.12. $r_\pm = \max\{\dim U \mid U \leq V,\ \pm B|_{U\times U} \textit{ positiv definit}\}$.

Beweis. Wir zeigen die Aussage für r_+, die Aussage für r_- zeigt man analog. Wir dürfen annehmen, dass $(V,B) = [1,\dots,1,-1,\dots,-1]$. Dann ist B auf $\langle e_1,\dots,e_{r_+}\rangle$ positiv-definit, also gilt „≤“. Wäre das Maximum echt größer, so gäber es einen Unterraum U der Dimension $> r_+$ mit $B|_{U\times U}$ positiv-definit. Aus Dimensionsgründen wäre dann aber $U \cap \langle e_{r_++1},\dots,e_{\dim V}\rangle \neq \{0\}$, und wäre $v \neq 0$ ein Vektor aus diesem Schnitt, so wäre einerseits $B(v,v) > 0$ und andererseits $B(v,v) \leq 0$, was ein Widerspruch ist. □

Definition 7.4.13. Das Tripel (r_+,r_-,r_0) heißt die *Signatur* von B (oder von (V,B)).

Beispiel 7.4.14 (Signatur und Witt-Index)**.** Wie lautet die Witt-Zerlegung eines reell-orthogonalen Vektorraums der Signatur (r_+,r_-,r_0)? Wir unterscheiden zwei Fälle:

FALL 1: $r_+ \geq r_-$.

In diesem Fall ist die Witt-Zerlegung gegeben durch

$$(V,B) \cong [\underbrace{1,-1]\perp\dots\perp[1,-1}_{r_-}]\perp(\underbrace{1,\dots,1}_{r_+-r_-})\perp[\underbrace{0,\dots,0}_{r_0}]],$$

und (V,B) hat Witt-Index r_-, Nullität r_0 und anisotropen Teil $(\mathbb{R}^{r_+-r_-},B_0)$, wobei B_0 das Standardskalarprodukt ist.

FALL 2: $r_+ < r_-$.

In diesem Fall ist die Witt-Zerlegung gegeben durch

$$(V,B) \cong \underbrace{[1,-1]\perp\dots\perp[1,-1}_{r_+}]\perp(\underbrace{-1,\dots,-1}_{r_--r_+})\perp[\underbrace{0,\dots,0}_{r_0}]],$$

und (V,B) hat Witt-Index r_+, Nullität r_0 und anisotropen Teil $(\mathbb{R}^{r_--r_+},-B_0)$, wobei B_0 das Standardskalarprodukt ist.

Man kann die beiden Fällen wie folgt zusammenfassen:

- r_0 ist die Nullität von (V,B).
- $r := \min\{r_+,r_-\}$ ist der Witt-Index von (V,B).
- Der anisotrope Teil von (V,B) hat Dimension $|r_+ - r_-|$. Er ist positiv-definit, wenn $r_+ > r_-$ und negativ-definit, wenn $r_- > r_+$.
- Der Witt-Index von (V,B) ist durch die Signatur eindeutig bestimmt, und der anisotrope Teil ist bist auf Isomorphie durch die Signatur bestimmt.

Mittels der Eindeutigkeit der Witt-Zerlegung folgt daraus der folgende Satz.

Korollar 7.4.15 (Trägheitssatz von Sylvester[17])**.** *Sind B und B' zwei Bilinearformen auf $\mathbb{R}$-Vektorräumen V und V', so gilt genau dann $(V,B) \cong (V',B')$, wenn B und B' dieselbe Signatur haben. Insbesondere gibt es bis auf Isomorphie genau $(n+1)$ orthogonale $\mathbb{R}$-Vektorräume der Dimension n.* □

[17] Der Satz hat nichts mit Neujahrsmüdigkeit zu tun, sondern ist nach dem englischen Mathematiker James Joseph Sylvester (1814-1897) benannt.

Notation 7.4.16. Man schreibt häufig $\mathbb{R}^{p,q}$ für den bis auf Isomorphie eindeutigen orthogonalen reellen Vektorraum mit Signatur $(p,q,0)$. Für $q=1$ erhalten wir genau die Minkowksi-Räume, diese haben also Witt-Index 1 und sind daher die „einfachsten" isotropen orthogonalen Vektorräume. Analog schreibt man häufig

$$\mathrm{O}(p,q) := \left\{ A \in \mathbb{R}^{(p+q)\times(p+q)} \mid A^\top \begin{pmatrix} \mathbf{1}_p & 0 \\ 0 & -\mathbf{1}_q \end{pmatrix} A = \begin{pmatrix} \mathbf{1}_p & 0 \\ 0 & -\mathbf{1}_q \end{pmatrix} \right\} \cong \mathrm{O}(\mathbb{R}^{p,q}).$$

Beispiel 7.4.17 (Bilinearformen über algebraische abgeschlossenen Körpern)**.** Es sei $\mathbb{K}$ ein Körper, in dem jedes Element eine Quadratwurzel hat. Beispiele hierfür[18] sind algebraisch abgeschlossene Körper, insbesondere $\mathbb{C}$. Es gilt dann $[\lambda] \cong [\mu]$ für alle $\lambda, \mu \in \mathbb{K}^\times$. Ist (V,B) ein orthogonaler $\mathbb{K}$-Vektorraum von gerader Dimension, so gilt daher

$$(V,B) \cong [1,\dots,1] \cong [1,-1,\dots,1,-1] \cong [1,-1] \perp \dots \perp [1,-1]$$

und daher hat V Witt-Index $\dim V/2$ und anisotropen Teil $\{0\}$. Hat V dagegen ungerade Dimension so gilt

$$(V,B) \cong [1,\dots,1] \cong [1,-1] \perp \dots \perp [1,-1] \perp [1],$$

alsi hat V Witt-Index $\lfloor \dim V/2 \rfloor$ und anisotropen Teil $[1]$. Es gibt dann also in jeder Dimension genau einen orthogonalen $\mathbb{K}$-Vektorraum. Ausgeartete Bilineaformen sind entsprechend durch die Dimension und die Nullität (oder äquivalent dazu, den Rang einer beliebigen darstellenden Matrix) eindeutig festgelegt.

Das ist an dieser Stelle alles, was wir zur Klassifikation orthogonaler Vektorräume sagen wollen. Wir diskutieren nun noch eine weitere Anwendung des Wittschen Kürzungssatzes.

Korollar 7.4.18. *Es seien (V_1,B_1) und (V_2,B_2) orthogonale Vektorräume und $U_1 \le V_1$ und $U_2 \le V_2$ reguläre Unterräume. Ist $f : (U_1, B_1|_{U_1\times U_1}) \to (U_2, B_2|_{U_2\times U_2})$ ein Isomorphismus, so existiert ein Isomorphismus $F : (V_1,B_1) \to (V_2,B_2)$ mit $F|_{U_1} = f$.*

Beweis. Da U_1 und U_2 regulär sind, gilt $V_1 = U_1 \perp U_1^\perp$ und $V_2 = U_2 \perp U_2^\perp$. Aus der Annahme und dem Wittschen Kürzungssatz folgt

$$(U_1 \perp U_1^\perp \cong U_2 \perp U_2^\perp) \wedge (U_1 \cong U_2) \implies U_1^\perp = U_2^\perp.$$

Es existiert also ein Isomorpismus $g : U_1^\perp \to U_2^\perp$ und wir setzen $F := f \oplus g$. Dann ist F injektiv (und daher bijektiv) und für $u \in U_1, u' \in U_1^\perp$ gilt einerseits

$$B_2(F(u+u'),F(u+u')) = B_2(f(u)+g(u'),f(u)+g(u')) = B_2(f(u),f(u)) + 0 + 0 + B_2(g(u'),g(u')),$$

und da f und g Morphismen sind, gilt andererseits

$$B_1(u+u',u+u') = B_1(u,u) + 0 + 0 + B_1(u',u') = B_2(f(u),f(u)) + B_2(g(u),g(u')).$$

Folglich ist F ein Isomorphismus. □

Korollar 7.4.19. *Ist (V,B) ein orthogonaler Vektorraum und $U < V$ ein regulärer Unterraum, so setzt sich jeder Monomorphismus $f : U \hookrightarrow V$ zu einem $F \in \mathrm{O}(V,B)$ fort.* □

[18] Es gibt auch andere Körper mit dieser Eigenschaft, z.B. die Menge aller komplexen Zahlen, die man ausgehend von 0 und 1 mit Zirkel und Lineal konstruieren kann.

Mittels Lemma 7.4.4 können wir die Regularitätsannahme an U loswerden:

Satz 7.4.20 (Wittscher Fortsetzungssatz)**.** *Ist (V,B) ein orthogonaler Vektorraum und $U < V$ ein beliebiger Unterraum, so setzt sich jeder Monomorphismus $f : U \hookrightarrow V$ zu einem $F \in \mathrm{O}(V,B)$ fort.*

Beweis. Wir zerlegen $U = R \oplus W$ in sein Radikal R und ein Komplement W. Dann ist R ein total isotroper Unterraum von $W^\perp$. Wir wählen nun eine Basis $u_1,\dots,u_m$ von R und finden $u'_1,\dots,u'_m$ und U' wie in Lemma 7.4.4. Wir können dasselbe Lemma auch auch $f(u_1),\dots,f(u_m) \in f[W]^\perp$ anwernden und finden dann n $v_1,\dots,v_m \in f[W]^\perp$, so dass $B(f(u_i),v_j) = \delta_{ij}$ und $B(v_i,v_j) = 0$. Wir können nun f fortsetzen zu einem Monomorphismus

$$F_1 : (R_1 \oplus U') \oplus W_1 \to V,$$

indem wir $F_1(u'_j) := v'_j$ setzen. Da $(R_1 \oplus U') \oplus W_1$ regulär ist, können wir dann F_1 mittels Korollar 7.4.19 zu einem $F \in \mathrm{O}(V,B)$ fortsetzen. □

Man kann den Satz auch so formulieren: *Ist $f : U_1 \to U_2$ ein Isomorphismus zwischen zwei Unterräumen $U_1, U_2 < V$, so existiert ein $F \in \mathrm{O}(V,B)$ mit $F|_{U_1}^{U_2} = f$.* Als Spezialfall halten wir fest:

Korollar 7.4.21. *Sind $U_1, U_2 < V$ mit $(U_1, B|_{U_1\times U_1}) \cong (U_2, B|_{U_2\times U_2})$, so existiert ein $\Phi \in \mathrm{O}(V,B)$ mit $\Phi[U_1] = U_2$.* □

Beispiel 7.4.22 (Viele Symmetrien)**.** Wir betrachten einige Spezialfälle:

(i) Sind g_1, g_2 zwei Geraden im Lichtkegel des Minkowski-Raums $\mathbb{R}^{n,1}$, so existiert ein $\Phi \in \mathrm{O}(\mathbb{R}^{n,1})$ mit $\Phi[g_1] = g_2$.

(ii) Allgemeiner gilt: Ist (V,B) ein orthogonaler Vektorraum vom Witt-Index r und $j \in \{1,\dots,r\}$, dann existiert mindestens ein total isotroper Unterraum der Dimension j, und sind $U_1, U_2 < V$ zwei solche Unterräume, so existiert ein $\Phi \in \mathrm{O}(V,B)$ mit $\Phi[U_1] = U_2$.

(iii) Sind E_1 und E_2 zwei reguläre isotrope Ebenen in V, so existiert ein $\Phi \in \mathrm{O}(V,B)$ mit $\Phi[E_1] = E_2$.

(iv) Ist $\mathbb{K}$ algebraisch abgeschlossen, so existiert für beliebige k-dimensionale Unterräume U_1 und U_2 von $\mathbb{R}^n$ ein $\Phi \in \mathrm{O}(\mathbb{R}^n,B)$ mit $\Phi[U_1] = U_2$. Ist hingegen $\mathbb{K} = \mathbb{R}$, so existiert ein solches Φ genau dann, wenn $B|_{U_1\times U_1}$ und $B|_{U_2\times U_2}$ dieselbe Signatur besitzen.

(v) Als Spezialfall erhalten wir: Ist B eine Skalarprodukt auf $\mathbb{R}^n$, so existiert für beliebige k-dimensionale Unterräume U_1 und U_2 von $\mathbb{R}^n$ ein $\Phi \in \mathrm{O}(\mathbb{R}^n,B)$ mit $\Phi[U_1] = U_2$.

Teile der Witt-Theorie lassen sich (unter Zusatzannahmen) auf hermitesche Vektorräume übertragen. Wir behandeln hier der Einfachheit halber nur den komplexen Fall. Für den Rest dieses Abschnitts sei $\mathbb{K} = \mathbb{C}$ und σ die komplexe Konjugation. Weiter sei stets B eine Sesquilinearform auf einem komplexen Vektorraum V. Wir schreiben $[\lambda_1,\dots,\lambda_n] := (\mathbb{C}^n, B_{\lambda_1,\dots,\lambda_n})$, wobei $B_{\lambda_1,\dots,\lambda_n}$ die Sesquilinearform mit $B_{\lambda_1,\dots,\lambda_n}(w,z) = \lambda_1 w_1 \overline{z_1} + \dots + \lambda_n w_n \overline{z_n}$ ist.

Bemerkung 7.4.23 (Signatur im Komplexen)**.** Ist A eine darstellende Matrix von B bzgl. einer beliebigen Basis, so können wir A mittels symmetrischen Gauß zunächst auf Diagonalform bringen und anschließend alle Diagonaleinträge auf 0, 1 oder -1 normalisieren. Es existieren daher $r_+, r_-, r_0 \in \mathbb{N} \cup \{0\}$ mit $r_+ + r_- + r_0 = \dim V$, so dass

$$(V,B) \cong [\underbrace{1,\dots,1}_{r_+},\underbrace{-1,\dots,-1}_{r_-},\underbrace{0,\dots,0}_{r_0}].$$

Wir im reellen Fall ist das Tripel (r_+, r_-, r_0) durch B eindeutig bestimmmt (r_0 ist die Dimension des Radikals und $r_\pm$ sind die maximalen Dimensionen eines Unterraums auf dem B positiv/negativ definit ist) und heißt die *Signatur* von B (oder von (V,B)).

In unserem Beweis des Wittschen Kürzungssatzes haben wir maßgeblich verwendet, dass wir zwei anisotrope Vektoren derselben „Länge"mittels einer Spiegelung oder Pseudodrehung aufeinander abbilden können. Wir haben bereits gesehen, dass uns Spiegelungen und Pseudodrehungen im Komplexen nicht weit bringen. Trotzdem gilt der folgenden Satz:

Lemma 7.4.24. *Es sei B nicht-ausgesartet und es seien $v,w \in V$ mit $B(v,v) = B(w,w) = R \neq 0$. Dann existiert ein $\Phi \in \mathrm{U}(V,B)$ mit $\Phi(v) = w$.*

Beweis. Indem wir v und w mit $\sqrt{|R|}$ multiplizieren, dürfen wir annehmen, dass $B(v,v) = B(w,w) \in \{-1,1\}$ gilt. Wir ergänzen $v_1 := v$ und $w_1 := w$ zu OGBen $(v_1,\dots,v_n)$ und $(w_1,\dots,w_n)$, wobei wir nach Normalisieren annehmen dürfen, dass $B(v_j,v_j) \in \{-1,1\}$ und $B(w_j,w_j) \in \{-1,1\}$ gilt. Die Anzahl der Vektoren v_j mit $B(v_j,v_j) = 1$ ist wegen der Wohldefiniertheit der Signatur gleich der Anzahl der Vektoren w_j mit $B(w_j,w_j) = 1$. Nach Umsortieren dürfen wir daher annehmen, dass $B(v_i,v_j) = B(w_i,w_j)$ für alle $i,j \in \{1,\dots,n\}$ gilt. Dann existiert eine eindeutig bestimmte lineare Abbildung $\Phi : V \to V$ mit $\Phi(v_i) = w_i$, und diese ist unitär und erfüllt $\Phi(v) = w$. □

Der Beweis von Lemma 7.4.1 überträgt sich nun: Statt Korollar 7.3.15 verwendet man einfach Lemma 7.4.24. Der Rest des Beweises des Wittschen Kürzungssatzes überträgt sich wörtlich. Wir erhalten:

Korollar 7.4.25 (Wittscher Kürzungssatz)**.** *Sind B_1,B_2,B_3 hermitesche Formen auf $\mathbb{C}$-Vektorräumen V_1,V_2,V_3, so gilt $(V_1,B_1) \oplus (V_2,B_2) \cong (V_1,B_1) \oplus (V_3,B_3) \implies (V_2,B_2) \cong (V_3,B_3)$.*

Dieser hat die üblichen Konsequenzen:

Satz 7.4.26 (Wittscher Fortsetzungssatz)**.** *Ist (V,B) ein hermitescher Vektorraum über $\mathbb{C}$ und $U < V$ ein beliebiger Unterraum, so setzt sich jeder Monomorphismus $f : U \hookrightarrow V$ zu einem $F \in \mathrm{U}(V,B)$ fort.*

Korollar 7.4.27 (Eindeutigkeit der Wittzerlegung)**.** *Ist B eine hermitesche Form auf einem $\mathbb{C}$-Vektorraum V und sind*

$$V = E_1 \oplus \dots \oplus E_r \oplus A \oplus V_0 = E_1' \oplus \dots \oplus E_{r'}' \oplus A' \oplus V_0'$$

zwei Witt-Zerlegungen von V, so gilt $r = r'$, $A \cong A'$ und $V_0 \cong V_0'$.

Wie im reellen Fall gilt: Ist (r_+,r_-,r_0) die Signatur von W, so ist $r_0 = \dim V^\perp$ und $\min\{r_+,r_-\}$ ist der Witt-Index. Weiter ist $B|_{A\times A}$ positiv-definit, wenn $r_+ > r_-$, und negativ definit, wenn $r_- > r_+$. Die Witt-Zerlegung legt also die Signatur eindeutig fest, und wir erhalten:

Korollar 7.4.28 (Trägheitssatz von Sylvester)**.** *Sind B und B' zwei Sesquilinearformen auf $\mathbb{C}$-Vektorräumen V und V', so gilt genau dann $(V,B) \cong (V',B')$, wenn B und B' dieselbe Signatur haben. Insbesondere gibt es bis auf Isomorphie genau $(n+1)$ hermitesche $\mathbb{C}$-Vektorräume der Dimension n.* □

Man beachte: Es gibt bis auf Isomorphie (n+1) hermitesche Vektorräume der Dimension n über $\mathbb{C}$ (klassifiziert durch die Signatur), aber nur einen orthogonalen Vektorraum!

Notation 7.4.29. Man schreibt häufig $\mathbb{C}^{p,q}$ für den bis auf Isomorphie eindeutigen hermiteschen $\mathbb{C}$-Vektorraum mit Signatur $(p,q,0)$. Analog schreibt man häufig

$$\mathrm{U}(p,q) := \left\{ A \in \mathbb{C}^{(p+q)\times(p+q)} \mid A^\top \begin{pmatrix} \mathbf{1}_p & 0 \\ 0 & -\mathbf{1}_q \end{pmatrix} A = \begin{pmatrix} \mathbf{1}_p & 0 \\ 0 & -\mathbf{1}_q \end{pmatrix} \right\} \cong \mathrm{U}(\mathbb{C}^{p,q}).$$

Zusammenfassung von Abschnitt 7.4

Im Folgenden seien alle Vektorräume über einem Körper der Charakteristik $\neq 2$ definiert.

(1) Werden zwei Vektorräume mit Bilinearformen (oder komplexen Sesquilinearformen) isomorph, nachdem man zu beiden denselben Vektorraum mit Bilinearform (bzw. Sequilinearform) addiert hat, so waren sie schon vorher isomorph (Wittscher Kürzungssatz).

(2) Sind zwei Unterräume eines orthogonalen (oder komplex-hermiteschen) Vektorraums isomorph, so gibt es einen Automorphismus des gesamten Raums, der die beiden aufeinander abbildet. Insbesondere existiert ein solcher für zwei total-isotrope Unterräume derselben Dimension.

(3) Die Witt-Zerlegung eines Vektorraums ist eindeutig, d.h. der Witt-Index und die Nullität sind eindeutig bestimmt und der anisotrope Teil ist eindeutig bis auf Isomorphismus.

(4) Reell-orthogonale und komplex-hermitesche Vektorräume sind durch ihre Signatur eindeutig bestimmmt. Komplex-orthogonale Vektorräume sind bereits durch ihre Dimension eindeutig bestimmmt.

8 Der Spektralsatz und seine Folgerungen

8.1 Normale Endomorphismen

Es sei $\mathbb{K}$ ein Körper und $\sigma \in \mathrm{Aut}(\mathbb{K})$ mit $\sigma^2 = \mathrm{Id}$.

Definition 8.1.1. Es seien V und W zwei $\mathbb{K}$-Vektorräume und B_V bzw. B_W zwei hermitesche Sesquilinearformen auf V bzw. W. Eine lineare Abbildung $\Phi : V \to W$ heißt *adjungiert* zu einer linearen Abbildung $\Psi : W \to V$ (bzgl. B_V und B_W), falls

$$B_W(\Phi(v), w) = B_V(v, \Psi(w)) \text{ für alle } v \in V, w \in W. \tag{8.1.1}$$

Lemma 8.1.2 (Eindeutigkeit der Adjungierten)**.** *Es sei B_V nicht-ausgeartet.*

(i) Ist $\Phi \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ adjungiert zu $\Psi \in \mathrm{Hom}_{\mathbb{K}}(W,V)$ (bzgl. B_V und B_W), so ist auch Ψ adjungiert zu Φ (bzgl. B_W und B_V).

(ii) Zu jedem $\Phi \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ existiert höchstens ein $\Psi \in \mathrm{Hom}_{\mathbb{K}}(W,V)$, das zu Φ adjungiert ist.

Beweis. (i) Aus (8.1.1) folgt für alle $v \in V$ und $w \in W$, dass

$$B_V(\Psi(w), v) = \overline{B_V(v, \Psi(w))} = \overline{B_W(\Phi(v), w)} = B_W(w, \Phi(v)).$$

(ii) Angenommen $\Psi_1, \Psi_2 \in \mathrm{Hom}_{\mathbb{K}}(W,V)$ sind beide adjungiert zu Φ. Dann gilt für alle $v \in V$ und $w \in W$, dass

$$B_V(v, \Psi_1(w) - \Psi_2(w)) = B_V(v, \Psi_1(w)) - B_V(v, \Psi_2(w)) = B_V(\Phi(v), w) - B_V(\Phi(v), w) = 0.$$

Da $v \in V$ beliebig war und B_V nicht-ausgeartet ist, folgt, dass $\Psi_1(w) - \Psi_2(w) = 0$ für alle $w \in W$ und daher $\Psi_1 = \Psi_2$ ist. □

Proposition 8.1.3 (Existenz der Adjungierten)**.** *Gilt $\dim V < \infty$ und ist B_V nicht-ausgeartet, so besitzt jedes $\Phi \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ eine adjungierte Abbildung Ψ.*

Bevor wir die Proposition beweisen, betrachten wir zwei Klassen von Beispielen:

Beispiel 8.1.4 (Adjungierte eines Isomorphismus)**.** Es sei $\Phi \in (V, B_V) \to (W, B_W)$ ein Isomorphismus. Es gilt dann

$$B_W(\Phi(v), w) = B_W(\Phi(v), \Phi(\Phi^{-1}(w))) = B_V(v, \Phi^{-1}(w)).$$

In diesem Fall ist also die Adjungiert von Φ gerade die Inverse.

Beispiel 8.1.5 (Adjungierte bzgl. Skalarprodukt)**.** Es sei $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und es seien B_V und B_W Skalarprodukte auf endlichdimensionalen $\mathbb{K}$-Vektorräumen V und W. Wir wählen ONBen $\mathscr{B}_V$ und $\mathscr{B}_W$ von V und W. Es seien nun $\Phi \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ und $\Psi \in \mathrm{Hom}_{\mathbb{K}}(W,V)$ mit darstellenden Matrizen

$$A := D_{\mathscr{B}_W, \mathscr{B}_V}(\Phi) \quad \text{und} \quad B := D_{\mathscr{B}_V, \mathscr{B}_W}(\Psi),$$

und $v \in V$ und $w \in W$ mit Koordinatenvektoren $x := [v]_{\mathscr{B}_V}$ und $y := [w]_{\mathscr{B}_W}$. Dann gilt

$$B_W(\Phi(v), w) = (Ax)^\top \overline{y} = x^\top A^\top \overline{y} \quad \text{und} \quad B_V(v, \Psi(w)) = x^\top \overline{B}\overline{y}.$$

Folglich sind Φ und Ψ genau dann adjungiert, wenn $B = A^* = \overline{A}^\top$ gilt.

Bemerkung 8.1.6 (Zur Notation)**.** Aus Beispiel 8.1.5 leitet sich eine etwas unglückliche Notation für adjungierte lineare Abbildungen her: Ist $\Phi : V \to W$ eine lineare Abbildung zwischen endlichdimensionalen $\mathbb{K}$-Vektorräumen mit Skalarprodukt (für ein $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$), so bezeichnet man die zugehörige adjungierte lineare Abbildung mit $\Phi^* : W \to V$. Einerseits ist das durchaus sinnvoll, denn mit dieser Notation gilt ja

$$D_{\mathscr{B}_V, \mathscr{B}_W}(\Phi^*) = D_{\mathscr{B}_W, \mathscr{B}_V}(\Phi)^*.$$

für beliebige ONBs $\mathscr{B}_V$ und $\mathscr{B}_W$. Andererseits ist dies aber auch etwas unglücklich[1], weil wir ja mit Φ^* auch schon die duale Abbildung zu Φ bezeichnet haben. Aus dem Kontext wird aber stets klar sein, ob mit Φ^* die Adjungierte oder die duale Abbildung gemeint ist.

[1] Die Verwendung derselben Notation ist insofern gerechtfertigt, als man die adjungierte Abbildung unter den Identifikationen von V mit V^* und W mit W^* vermittels B_V und B_W mit der dualen Abbildung identifizieren kann, aber verwirrend ist das trotzdem.

[07.06.24]

Beweis von Proposition 8.1.3. Für ein festes $w \in W$ betrachten wir die Abbildung $\Phi_w : V \to \mathbb{K}$, $v \mapsto B_W(\Phi(v), w)$. Diese ist linear und definiert daher ein Element von V^*.

Da B_V nicht-ausgeartet ist, ist die Abbildung $\Phi_{B_V} : V \to V^*$, $v \mapsto B_V(v, \cdot)$ injektiv, und da V endlichdimensional ist auch surjektiv. Es existiert daher ein eindeutig bestimmtes $v' \in V$ mit $\Phi_w = \Phi_{B_V}(v')$. Setzen wir $\Psi(w) := v'$, so gilt dann also

$$B_V(v, \Psi(w)) = B_V(v, v') = \Phi_{B_V}(v')(v) = \Phi_w(v) = B_W(\Phi(v), w) \quad \text{für alle } v \in V, w \in W,$$

und es bleibt zu zeigen, dass Ψ linear ist. Sind nun $w_1, w_2 \in W$ und $\lambda, \mu \in \mathbb{K}$, so gilt für alle $v \in V$, dass

$$\begin{aligned} B_V(v, \Psi(\lambda w_1 + \mu w_2)) &= B_W(\Phi(v), \lambda w_1 + \mu w_2) = \sigma(\lambda) B_W(\Phi(v), w_1) + \sigma(\mu) B_W(\Phi(v), w_2) \\ &= \sigma(\lambda) B_V(v, \Psi(w_1)) + \sigma(\mu) B_V(v, \Psi(w_2)) = B_V(v, \lambda\Psi(w_1) + \mu\Psi(w_2)), \end{aligned}$$

und da B_V nicht-ausgeartet ist, folgt, dass $\Psi(\lambda w_1 + \mu w_2) = \lambda\Psi(w_1) + \mu\Psi(w_2)$). □

Für eine abstrakteren Beweis von Proposition 8.1.3 mit weniger Rechnungen, basierend auf der Beziehung zwischen adjungierten und dualen Abbildungen, sei auf die Übungen verwiesen.

Für den Rest dieses Abschnitts sei $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und es sei B ein Skalarprodukt auf einem endlichdimensionalen $\mathbb{K}$-Vektorraum V. Als Spezialfall von Beispiel 8.1.5 erhalten wir:

Korollar 8.1.7 (Adjungierte eines Endomorphismus)**.** *Ist $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ und $\mathscr{B}$ eine ONB von V bzgl. B, so ist die Adjungierte Φ^* von Φ bzgl. B und B eindeutig bestimmt durch die Gleichung*

$$D_{\mathscr{B}}(\Phi^*) = D_{\mathscr{B}}(\Phi)^*.$$ □

Wir kommen nun zu der zentralen Definition dieses Kapitels; die wahre Bedeutung dieser Definition wird sich erst im nächsten Abschnitt erweisen.

Definition 8.1.8. Ein Endomorphismus $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ heißt *normal* (bzgl. B), falls Φ und Φ^* vertauschen, d.h.

$$\Phi \circ \Phi^* = \Phi^* \circ \Phi.$$

Analog nennen wir eine (komplexe oder reelle) Matrix A *normal*, falls $AA^* = A^*A$. Ein Endomorphismus ist also normal, wenn seine darstellende Matrix bzgl. einer beliebigen ONB normal ist.

Beispiel 8.1.9 (Beispiele für normale Endomorphismen)**.** Es gibt eine Reihe von einfachen Bedingungen, die die Normalität eines Endomorphismus $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ (bzgl. B) garantieren.

(i) Es sei Φ eine orthogonale (im Fall $\mathbb{K} = \mathbb{R}$) bzw. unitäre (im Fall $\mathbb{K} = \mathbb{C}$) lineare Abbildung. Nach Beispiel 8.1.4 gilt dann $\Phi^* = \Phi^{-1}$, und folglich

$$\Phi \circ \Phi^* = \mathrm{Id} = \Phi^* \circ \Phi.$$

Orthogonale bzw. unitäre Endomorphismen sind also stets normal.

(ii) Ein Endomorphismus Φ heißt *selbstadjungiert*, falls $\Phi = \Phi^*$. Dies bedeutet gerade, dass Φ bzgl. einer beliebigen ONB durch eine symmetrische (falls $\mathbb{K} = \mathbb{R}$) bzw. hermitesche (falls $\mathbb{K} = \mathbb{C}$) Matrix dargestellt wird. Ist Φ selbstadjungiert, so gilt

$$\Phi \circ \Phi^* = \Phi^2 = \Phi^* \circ \Phi,$$

also ist Φ normal.

(iii) Es sei $\Phi := \lambda \cdot \mathrm{Id}$ für ein $\lambda \in \mathbb{K}$. Dann gilt für alle $v, w \in V$, dass

$$B(\Phi(v), w) = B(\lambda v, w) = \lambda B(v, w) = B(v, \overline{\lambda} w),$$

also ist $\Phi^*(v) = \overline{\lambda} \cdot v$. Folglich ist Φ normal, denn es gilt

$$\Phi \circ \Phi^* = |\lambda|^2 \cdot \mathrm{Id} = \Phi^* \circ \Phi.$$

Andererseits ist Φ genau dann selbstadjungiert, wenn λ reell ist, und Φ ist orthogonal/unitär genau dann, wenn $|\lambda| = 1$. Es gibt also normale Abbildungen, die weder selbstadjungiert noch unitär sind.

Weitere Beispiele erhalten wir mittels der folgenden Beobachtung:

Übung 8.1.10. Es sei (V, B) ein endlichdimensionaler $\mathbb{K}$-Vektorraum mit Skalarprodukt und $\Phi, \Psi \in \mathrm{End}_{\mathbb{K}}(V)$. Zeigen Sie:

(i) Es gilt $(\Phi^*)^* = \Phi$, und ist Φ normal, so ist auch Φ^* normal.

(ii) $(\Phi \circ \Psi)^* = \Psi^* \circ \Phi^*$.

(iii) Für $\lambda \in \mathbb{K}$ gilt $(\lambda\Phi)^* = \overline{\lambda}\Phi^*$ und $(\Phi + \Psi)^* = \Phi^* + \Psi^*$.

(iv) Sind Φ und Ψ normal und vertauschen, so ist jede Linearkombination von Φ und Ψ normal.

Bevor Sie auf die Idee kommen, dass vielleicht jeder Endomorphismus normal sein könnte, hier ein Gegenbeispiel:

Beispiel 8.1.11 (Ein nicht-normaler Endomorphismus)**.** Wir werden noch sehen, dass jeder normale Endomorphismus über $\mathbb{C}$ diagonalisierbar ist, also sind von 0 verschiedene nilpotente Endomorphismen niemals normal. In einfachen Fällen kann man das von Hand überprüfen: Betrachten wir $\mathbb{C}^2$ mit dem Standardskalarprodukt und den Endomorphismus

$$\Phi : \mathbb{C}^2 \to \mathbb{C}^2, \quad \Phi(v) := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} v,$$

so ist Φ nicht normal, denn es gilt

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

Bemerkung 8.1.12. Historisch ist der Begriff einer normalen Abbildung aus dem Bemühen entstanden, die Spektralsätze für symmetrische/hermitesche Matrizen und orthogonale/unitäre Matrizen unter einen Hut zu bekommen. Erst später wurde klar, dass die Klasse der normalen Endomorphismen unter den Endomorphismen euklidischer und unitärer Vektorräume eine sehr spezielle Rolle spielt.

Wir erinnern daran, dass eine Matrix genau dann unitär ist (d.h. $A^* = A^{-1}$), wenn ihre Spalten bzw. Zeilen eine ONB bzgl. des Standardskalarprodukts bilden. Wir wollen nun eine ähnliche Charakterisierung für normale Matrizen finden.

Lemma 8.1.13 (Normale Matrizen)**.** *Es sei $A \in \mathbb{C}^{n\times n}$ mit Spalten $a_1,\dots,a_n$. Weiter sei B_0 das Standardskalarprodukt auf $\mathbb{C}^n$ und es seien $b_1,\dots,b_n$ die Spalten von A^*. Dann gilt*

$$A \text{ normal} \iff \forall\, i,j \in \{1,\dots,n\}:\ B_0(a_i,a_j) = B_0(b_i,b_j).$$

Insbesondere gilt dann für alle $i \in \{1,\dots,n\}$, dass $\|a_i\| = \|b_i\|$.

Beweis. Nach Definition gilt

$$A = (a_1,\dots,a_n) = \begin{pmatrix} b_1^* \\ \dots \\ b_n^* \end{pmatrix} \quad \text{und} \quad A^* = (b_1,\dots,b_n) = \begin{pmatrix} a_1^* \\ \dots \\ a_n^* \end{pmatrix}.$$

Daraus folgt, dass

$$A^*A = \begin{pmatrix} a_1^* \\ \dots \\ a_n^* \end{pmatrix} (a_1,\dots,a_n) = (a_i^* a_j)_{1\le i,j\le n} = (\overline{B_0(a_i,a_j)})_{1\le i,j\le n}.$$

Analog gilt

$$AA^* = \begin{pmatrix} b_1^* \\ \dots \\ b_n^* \end{pmatrix} (b_1,\dots,b_n) = (b_i^* b_j)_{1\le i,j\le n} = (\overline{B_0(b_i,b_j)})_{1\le i,j\le n}.$$

Daraus folgt die Behauptung. □

Korollar 8.1.14 (Normale Dreiecksmatrizen)**.** *Für alle $A \in \mathbb{C}^{n\times n}$ gilt*

$$A \text{ normale obere Dreiecksmatrix} \iff A \text{ Diagonalmatrix}.$$

Beweis. „⟸“: Ist A diagonal, so auch A^* und daher vertauschen A und A^*.

„⟹“: Es sei A eine normale obere Dreiecksmatrix, also

$$A = \begin{pmatrix} a_{11} & \dots & \dots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} \quad \text{und} \quad A^* = \begin{pmatrix} \overline{a_{11}} & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ \overline{a_{1n}} & \dots & \dots & \overline{a_{nn}} \end{pmatrix}$$

Wenden wir Lemma 8.1.13 auf die ersten Spalten an, so folgt

$$|a_{11}|^2 = |a_{11}|^2 + \dots + |a_{1n}|^2 \implies a_{12} = \dots = a_{1n} = 0.$$

Wenden wir das Lemma nun nach und nach auf alle Spalten an, so folgt ganz analog, dass alle Nichtdiagonaleinträge 0 sein müssen. □

Wir überlegen uns nun noch einige grundlegende Abbildungseigenschaften adjungierter und normaler Endomorphismen.

Lemma 8.1.15 (Orthogonalkomplemente invarianter Unterräume)**.** *Ist* $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *und* $U < V$ *ein* Φ*-invarianter Unteraum, so ist* $U^{\perp}$ *invariant unter* Φ^**.*

Beweis. Es seien $u \in U$ und $v \in U^{\perp}$. Es gilt dann $\Phi(u) \in U$ (wegen der Φ-Invarianz von U), und daher

$$B(u, \Phi^*(v)) = B(\Phi(u), v) = 0.$$

Da $u \in U$ beliebig war, folgt, dass $\Phi^*(v) \in U^{\perp}$. □

Proposition 8.1.16 (Kern der Adjungierten)**.** *Es sei* (V, B) *ein endlichdimensionaler* $\mathbb{K}$*-Vektorraum mit Skalarprodukt und* $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *normal. Dann gilt*

$$\ker(\Phi) = \ker(\Phi^*).$$

Beweis. Sei $v \in V$. Dann gilt $\Phi^*(\Phi(v)) = \Phi(\Phi^*(v))$, und daher

$$\begin{aligned} \|\Phi(v)\|^2 &= B(\Phi(v), \Phi(v)) = B(v, \Phi^*(\Phi(v))) = B(v, \Phi(\Phi^*(v))) \\ &= B(\Phi^*(v), \Phi^*(v)) = \|\Phi^*(v)\|^2. \end{aligned}$$

Insbesondere ist $\Phi(v) = 0 \iff \|\Phi(v)\|^2 = 0 \iff \|\Phi^*(v)\|^2 = 0 \iff \Phi^*(v) = 0$. □

Beispiel 8.1.11 zeigt, dass diese Aussage für nicht-normale Endomorphismen im Allgemeinen falsch ist, denn in diesem Beispiel ist $\ker(\Phi) = \mathbb{K}e_1$ und $\ker(\Phi^*) = \mathbb{K}e_2$.

Korollar 8.1.17 (Spektrum der Adjungierten)**.** *Es sei* (V, B) *ein endlichdimensionaler* $\mathbb{K}$*-Vektorraum mit Skalarprodukt und* $\Phi \in \mathrm{End}_{\mathbb{K}}(V)$ *normal. Dann gilt*

$$\mathrm{spec}(\Phi^*) = \{\overline{\lambda} \mid \lambda \in \mathrm{spec}(\Phi)\},$$

und ist $\lambda \in \mathrm{spec}(\Phi)$*, so gilt für die zugehörigen Eigenräume, dass*

$$V_{\lambda}(\Phi) = V_{\overline{\lambda}}(\Phi^*).$$

Beweis. Sei $\lambda \in \mathbb{K}$ und $\Psi := \lambda \cdot \mathrm{Id}$; dann ist Ψ normal (mit $\Psi^*(v) = \overline{\lambda}v$, vgl. Beispiel 8.1.9) und vertauscht mit Φ, also ist $\Psi - \Phi$ normal (mit $(\Psi - \Phi)^* = \Psi^* - \Phi^*$, vgl. Übung 8.1.10). Nach Proposition 8.1.16 gilt daher

$$\ker(\lambda \cdot \mathrm{Id} - \Phi) = \ker(\Psi - \Phi) = \ker(\Psi^* - \Phi^*) = \ker(\overline{\lambda} \cdot \mathrm{Id} - \Phi^*).$$

Insbesondere gilt

$$\lambda \in \mathrm{spec}(\Phi) \iff \ker(\lambda \cdot \mathrm{Id} - \Phi) \neq \{0\} \iff \ker(\overline{\lambda} \cdot \mathrm{Id} - \Phi^*) \neq \{0\} \iff \overline{\lambda} \in \mathrm{spec}(\Phi^*),$$

und in diesem Fall stimmen die Eigenräume überein. □

Beispiel 8.1.18 (Spektren spezieller normaler Endomorphismen)**.** Wir betrachten wieder die üblichen Spezialfälle:

(i) Ist Φ ein selbstadjungierter Endomorphismus eines euklidischen oder unitären Vektorraums (also $\Phi = \Phi^*$) , so gilt für alle $\lambda \in \mathrm{spec}_{\mathbb{C}}(\Phi)$, dass

$$V_{\lambda}(\Phi) = V_{\overline{\lambda}}(\Phi^*) = V_{\overline{\lambda}}(\Phi) \implies \lambda = \overline{\lambda},$$

also ist $\mathrm{spec}_{\mathbb{C}}(\Phi) \subseteq \mathbb{R}$. Insbesondere ist Φ auch im reellen Fall automatisch trigonalisierbar.

(ii) Ist Φ ein unitärer Automorphismus eines unitären Vektorraums (also $\Phi^* = \Phi^{-1}$), so gilt analog $|\lambda| = 1$ für jedes $\lambda \in \mathrm{spec}_{\mathbb{C}}(\Phi)$.

(iii) Ist Φ ein orthogonaler Automorphismus eines euklidischen Vektorraums (also $\Phi^* = \Phi^{-1}$), so gilt analog $\lambda \in \{\pm 1\}$ für jedes $\lambda \in \mathrm{spec}_{\mathbb{R}}(\Phi)$.

In Matrizensprache besagt dies gerade:

(i) Ist $A \in \mathbb{C}^{n\times n}$ hermitesch bzw. $A \in \mathbb{R}^{n\times n}$ symmetrisch, so ist $\mathrm{spec}_{\mathbb{C}}(A) \subseteq \mathbb{R}$, und A ist (auch im reellen Fall) trigonalisierbar.

(ii) Ist $A \in \mathbb{C}^{n\times n}$ unitär, so gilt $|\lambda| = 1$ für jedes $\lambda \in \mathrm{spec}_{\mathbb{C}}(\Phi)$.

(iii) Ist $A \in \mathbb{R}^{n\times n}$ orthogonal, so gilt $\lambda \in \{\pm 1\}$ für jedes $\lambda \in \mathrm{spec}_{\mathbb{R}}(\Phi)$.

Zusammenfassung von Abschnitt 8.1.

(1) Jede Abbildung zwischen endlichdimensionalen orthogonalen oder hermiteschen Vektorräumen besitzt eine Adjungierte.

(2) Im Fall von euklidischen oder unitären Vektorräumen ist die darstellende Matrix der Adjungierten bzgl. einer ONB gerade die adjungierte Matrix zur darstellenden Matrix bzgl. dieser ONB.

(3) Endomorphismen, die mit ihrer Adjungierten vertauschen, heißen normal. Orthogonale/unitäre und selbstadjungierte Endomorphismen sind Beispiele für solche Endomorphismen.

(4) Ist Φ ein normaler Endomorphismus, so sind die Eigenwerte von Φ^* die komplexkonjugierten der Eigenwerte von Φ und die entsprechenden Eigenräume stimmen überein.

8.2 Unitäre Diagonalisierbarkeit und Spektralkalkül

In diesem Abschnitt untersuchen wir eine Verschärfung von Diagonalisierbarkeit für komplexe Matrizen (bzw. Endomorphismen). Wir erinnern daran, dass eine Matrix $A \in \mathbb{C}^{n\times n}$ genau dann diagonalisierbar ist, wenn $\mathbb{C}^n$ eine Basis aus Eigenvektoren für A besitzt. Es bezeihne B_0 das Standardskalarprodukt auf $\mathbb{C}^n$.

Proposition 8.2.1 (Unitäre Diagonalisierbarkeit)**.** *Für eine Matrix $A \in \mathbb{C}^{n\times n}$ sind äquivalent:*

(i) Es existiert eine Matrix $S \in \mathrm{U}_n(\mathbb{C})$, so dass $S^{-1}AS$ diagonal ist.

(ii) Es existiert eine Matrix $S \in \mathrm{U}_n(\mathbb{C})$, so dass $S^{-1}AS$ eine normale obere Dreiecksmatrix ist.

(iii) $\mathbb{C}^n$ besitzt eine ONB aus Eigenvektoren von A (bzgl. des Standardskalarprodukt)

(iv) Sind $\lambda_1, \ldots, \lambda_k$ die verschiedenen Eigenwerte von A und $V_{\lambda_1}(A), \ldots, V_{\lambda_k}(A)$ die zugehörigen Eigenräume, so gilt

$$(\mathbb{C}^n, B_0) = V_{\lambda_1}(A) \perp\!\!\!\perp \ldots \perp\!\!\!\perp V_{\lambda_k}(A).$$

(v) A ist diagonalisierbar und die Eigenräume von A zu verschiedenen Eigenwerten sind orthogonal zueinander (bzgl. des Standardskalarprodukt).

Beweis. (i)$\Longleftrightarrow$(ii): Dies folgt sofort aus Korollar 8.1.14.

(ii)$\Longleftrightarrow$(iii): Es sei $S \in \mathbb{C}^{n\times n}$ mit Spalten $v_1,\dots,v_n$. Dann bilden $v_1,\dots,v_n$ genau dann eine Basis aus Eigenvektoren von A, wenn $S^{-1}AS$ diagonal ist, und diese Basis ist genau dann eine ONB, wenn S unitär ist.

(iii)$\Rightarrow$(iv): Es sei $(v_1,\dots,v_n)$ eine ONB aus Eigenvektoren. Nach Umsortieren dürfen wir annehmen, dass $v_1,\dots,v_{j_1}$ zum Eigenwert λ_1 gehören, $v_{j_1+1},\dots,v_{j_2}$ zum Eigenwert λ_2 gehören usw. Da $(v_1,\dots,v_n)$ eine Basis ist gilt dann

$$\mathbb{C}^n = \langle v_1,\dots,v_{j_1}\rangle \oplus \cdots \oplus \langle v_{j_{k-1}+1},\dots,v_n\rangle \subseteq V_{\lambda_1}(A)\oplus\cdots\oplus V_{\lambda_k}(A) \subseteq \mathbb{C}^n.$$

Dies impliziert, dass $V_{\lambda_1} = \langle v_1,\dots,v_{j_1}\rangle$ usw., also ist $\mathbb{C}^n = V_{\lambda_1}(A)\oplus\cdots\oplus V_{\lambda_k}(A)$, und wegen $B_0(v_i,v_j) = 0$ für alle $i \neq j$ stehen die Eigenräume senkrecht aufeinander.

(iv)$\Rightarrow$(v): Wegen $\mathbb{C}^n = V_{\lambda_1}(A)\oplus\cdots\oplus V_{\lambda_k}(A)$ ist A diagonalisierbar, also gilt (v).

(v)$\Rightarrow$(iii) Da A diagonalisierbar ist, erhalten wir eine Basis von $\mathbb{C}^n$, die sich aus Basen der Eigenräume zusammensetzt. Wenden wir nun auf jede dieser Basen das Gram-Schmidt-Verfahren an, so erhalten wir eine ONB für jeden Eigenraum, und die verschiedenen ONBs stehen paarweise senkrecht aufeinander. Wir können diese daher zu einer ONB von $\mathbb{C}^n$ zusammenfügen. □

Definition 8.2.2. Eine Matrix $A \in \mathbb{C}^{n\times n}$, die die äquivalenten Bedingungen aus Proposition 8.2.1 erfüllt, heißt *unitär diagonalisierbar*. Wir nennen A *unitär ähnlich* zu einer Matrix B, falls ein $S \in \mathrm{U}_n(\mathbb{C})$ existiert mit $B = S^{-1}AS$. A heißt *unitär trigonalisierbar*, wenn A unitär ähnlich zu einer oberen Dreiecksmatrix ist.

Nach Definition ist eine Matrix A genau dann unitär diagonalisierbar, wenn sie unitär äquivalent zu einer Diagonalmatrix ist.

Lemma 8.2.3. *Sind $A,B \in \mathbb{C}^{n\times n}$ unitär äquivalent, so gilt*

$$A \text{ normal} \iff B \text{ normal}.$$

Beweis. Ist A normal und $B = S^{-1}AS = S^*AS$ mit $S \in \mathrm{U}_n(\mathbb{C})$, so gilt

$$\begin{aligned} B^*B &= (S^*AS)^*S^*AS = S^*A^*(SS^*)AS = S^*A^*AS = S^*AA^*S \\ &= S^*A(SS^*)A^*S = S^*AS(S^*AS)^* = BB^*, \end{aligned}$$

also ist B normal. Aus Symmmetriegründen gilt auch die Umkehrung. □

Proposition 8.2.4 (Unitäre Trigonalisierbarkeit)**.** *Jedes $A \in \mathbb{C}^{n\times n}$ ist unitär trigonalisierbar.*

Beweis. Da $\mathbb{C}$ algebraisch abgeschlossen ist, zerfällt das charakteristische Polynom von A, also ist A trigonalisierbar. Wir finden also eine obere Dreiecksmatrix $O \in \mathbb{C}^{n\times n}$ und $T \in \mathrm{GL}_n(\mathbb{C})$ mit $T^{-1}AT = O$. Es seien $v_1,\dots,v_n$ die Spalten von O. Wir wenden auf $v_1,\dots,v_n$ das Gram-Schmidt-Verfahen an, und erhalten so eine ONB $(w_1,\dots,w_n)$ von $\mathbb{C}^n$. Die Matrix S mit Spalten $(w_1,\dots,w_n)$ ist dann unitär und es existieren $\lambda_{ij} \in \mathbb{C}$ mit

$$w_1 = \lambda_{11}v_1,\ \dots,\ w_n = \lambda_{n1}v_1 + \cdots + \lambda_{nn}v_n \quad \text{und} \quad \lambda_{ij} = 0 \text{ für } i < j.$$

Folglich ist $\Lambda = (\lambda_{ij})$ eine obere Dreiecksmatrix mit $S = T\Lambda$, und es gilt

$$S^{-1}AS = T\Lambda^{-1}AT\Lambda = \Lambda^{-1}T^{-1}AT\Lambda = \Lambda^{-1}O\Lambda.$$

Da O und Λ obere Dreiecksmatrizen sind, ist auch $\Lambda^{-1}O\Lambda$ eine obere Dreiecksmatrix. □

Satz 8.2.5 (Komplexer Spektralsatz, Erste Form)**.** *Für $A \in \mathbb{C}^{n\times n}$ gilt*

$$A \text{ unitär diagonalisierbar} \iff A \text{ normal}.$$

Beweis. „$\Longrightarrow$“: Nach Korollar 8.1.14 ist jede Diagonalmatrix normal. Mit Lemma 8.2.3 folgt daraus, dass auch jede Matrix, die unitär ähnlich zu einer Diagonalmatrix (also unitär diagonalisierbar) ist, normal ist.

„$\Longleftarrow$“: Nach Lemma 8.2.4 existiert $S \in \mathrm{U}_n(\mathbb{C})$, so dass $S^{-1}AS$ eine obere Dreiecksmatrix ist. Ist A normal, so ist nach Lemma 8.2.3 auch $S^{-1}AS$ normal, also eine normale obere Dreiecksmatrix. Nach Proposition 8.2.1.(ii) ist A dann unitär diagonalisierbar. □

In der Literatur finden sich zahlreiche verschiedene Beweise des Spektralsatzes, die verschiedene Verallgemeinerungen besitzen. Der obige kurze Beweis des Spektralsatzes geht auf SCHUR[2] zurück.

[2] Issai Schur (1875-1941), dt.-russ.-jüd. Mathematiker

[12.06.24]

Beispiel 8.2.6 (Eine unitäre Diagonalisierung)**.** Wir betrachten die Matrix

$$A := \begin{pmatrix} -\frac{1}{2} & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & -\frac{1}{2} \end{pmatrix} \tag{8.2.1}$$

Da A hermitesch ist, ist A normal. Um eine Orthonormalbasis aus Eigenvektoren von A zu bestimmen, gehen wir wie folgt vor:

SCHRITT 1: Das charakteristische Polynom von Φ bzw. A ist gegeben durch

$$\begin{aligned} \chi_\Phi(X) \quad = \quad \chi_A(X) \quad &= \quad \det\begin{pmatrix} X+\frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & X+1 & 0 \\ -\frac{1}{2} & 0 & X+\frac{1}{2} \end{pmatrix} \\ &= \quad \left(X+\frac{1}{2}\right)\cdot\det\begin{pmatrix} X+1 & 0 \\ 0 & X+\frac{1}{2} \end{pmatrix} - \frac{1}{2}\cdot\det\begin{pmatrix} 0 & -\frac{1}{2} \\ X+1 & 0 \end{pmatrix} \\ &= \quad \left(X+\frac{1}{2}\right)^2(X+1) - \frac{1}{4}(X+1) \quad = \quad (X+1)\cdot\left(X^2+X+\frac{1}{4}-\frac{1}{4}\right) \\ &= \quad (X+1)(X^2+X) \quad = \quad X\cdot(X+1)^2. \end{aligned}$$

Folglich ist

$$\operatorname{spec}_{\mathbb{C}}(A) \quad = \quad \{0,-1\}.$$

SCHRITT 2: Wir bestimmen die Eigenräume von A. Der Eigenraum zu $\lambda_1 := 0$ ist gegeben durch

$$V_{\lambda_1}(A) = \ker\begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} = \ker\begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \langle v_1 \rangle, \quad \text{wobei} \quad v_1 := \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Der Eigenraum zu $\lambda_2 := -1$ ist gegeben durch

$$V_{\lambda_2}(A) = \ker\begin{pmatrix} -\frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & 0 \\ -\frac{1}{2} & 0 & -\frac{1}{2} \end{pmatrix} = \ker\begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \langle v_2, v_3 \rangle, \quad \text{wobei} \quad v_2 := \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ und } v_3 := \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}.$$

SCHRITT 3: Wir finden ONBs zu jedem Eigenraum. Da $V_{\lambda_1}(A)$ eindimensional ist, ist (v_1) bereits eine geordnete OGB. Normalisieren führt auf den Vektor

$$w_1 := \frac{v_1}{B_0(v_1,v_1)^{\frac{1}{2}}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Es ist dann (w_1) eine ONB von $V_{\lambda_1}(A)$. Für $V_{\lambda_2}(A)$ bestimmen wir ausgehend von (v_2, v_3) eine geordnete ONB mittels beschleunigtem Gram-Schmidt-Verfahren. Der Vektor v_2 ist bereits normalisiert, wir setzen also $w_2 := v_2$. Wir finden dann einen zu w_2 orthogonalen Vektor durch

$$u_3 := v_3 - B_0(v_3,w_2)w_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} - 0\cdot\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}.$$

Normalisieren führt auf

$$w_3 := \frac{u_3}{B_0(u_3,u_3)^{\frac{1}{2}}} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\0\\1\end{pmatrix}.$$

Damit ist (w_1,w_2,w_3) eine ONB aus Eigenvektoren von A. Inbesondere gilt

$$\mathbb{C}^3 = \mathbb{C}w_1 \perp\!\!\!\perp (\mathbb{C}w_2 \perp\!\!\!\perp \mathbb{C}w_3) = V_{\lambda_1}(A) \perp\!\!\!\perp V_{\lambda_2}(A),$$

und setzen wir

$$S := \begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}}\\ 0 & 1 & 0\\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\end{pmatrix},$$

so ist $S \in \mathrm{U}_3(\mathbb{C})$ unitär mit

$$S^{-1}AS = \mathrm{diag}(0,-1,-1), \quad \text{wobei} \quad S^{-1} = S^* = \begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\\ 0 & 1 & 0\\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\end{pmatrix}.$$

Wir haben also Φ bzw. A unitär diagonalisiert.

Wofür ist der Spektralsatz gut? Zunächst einmal erhalten wir die offensichtliche Folgerung:

Korollar 8.2.7 (Normal impliziert diagonalisierbar)**.** *Jede normale (also insbesondere jede unitäre oder hermitesche) Matrix ist diagonalisierbar.* □

Beachte, dass es viel einfacher ist, eine Matriz auf Normalität zu überprüfen als z.B. zu testen, ob die algebraischen und geometrischen Vielfachheiten übereinstimmen. Sie ist allerdings auch nur hinreichend und nicht notwendig für Diagonalisierbarkeit.

Bemerkung 8.2.8 (Praktisches Diagonalisieren normaler Matrizen)**.** Es ist häufig effizienter eine normale Matrix unitär zu diagonalisieren, als sie einfach nur zu diagonalisieren. Das klingt zunächst paradox: Es ist doch mehr Aufwand, eine unitäre Matrix S mit $S^{-1}AS$ diagonal zu finden, als *irgendeine* Matrix T mit $T^{-1}AT$ diagonal?! Das Problem ist aber, dass es für eine allgemeine Matrix T aufwendig ist, die Inverse T^{-1} zu bestimmen!

Wenn man eine Matrix T mit $T^{-1}AT$ diagonal gefunden hat, dann ist es nicht schwer, eine unitäre Matrix S mit $S^{-1}AS$ diagonal zu bestimmen – das ist ja nur Gram-Schmidt, und wenn man Glück hat, haben die Eigenräume kleine Dimensionen. Es gilt dann aber $T^* = T^{-1}$, d.h. man kann die Inverse direkt hinschreiben! (Dieser Trick funktioniert natürlich nur, wenn T normal ist.)

Der komplexe Spektralsatz für Matrizen hat Anwendungen sowohl für Endomorphismen als auch für Sesquilinearformen. Wenden wir den Spektralsatz auf die darstellende Matrix eines Endomorphismus eines unitären Vektorraums bzgl. einer ONB an, so erhalten wir:

Korollar 8.2.9 (Komplexer Spektralsatz, Zweite Form)**.** *Ist* (V,B) *ein unitärer Vektorraum und ist* $\Phi \in \mathrm{End}(V) \setminus \{0\}$*, so sind äquivalent:*

(i) Φ *ist normal.*

(ii) V *besitzt eine ONB bzgl.* B *aus Eigenvektoren von* Φ*.*

(iii) Φ *ist diagonalisierbar und die Eigenräume zu den verschiedenen Eigenwerte von* Φ *sind paarweise orthogonal bzgl.* B.

(iv) Sind $\lambda_1,\dots,\lambda_k$ *die verschiedenen Eigenwerte von* Φ*, so gilt*

$$(V,B) = V_{\lambda_1}(\Phi) \perp\!\!\!\perp \dots \perp\!\!\!\perp V_{\lambda_k}(\Phi).$$

Kombinieren wir Korollar 8.2.9 mit Beispiel 8.1.18 so erhalten wir:

Korollar 8.2.10 (Unitäre Normalformen spezieller Endomorphismen)**.** *Es sei* (V,B) *ein unitärer Vektorraum.*

(i) Ist $\Phi \in \mathrm{U}(V,B)$*, so existiert eine ONB* $\mathscr{B}$ *von* V *bzgl.* B *und* $t_1,\dots,t_n \in \mathbb{R}$ *mit*

$$D_{\mathscr{B}}(\Phi) = \operatorname{diag}(e^{it_1},\dots,e^{it_n}).$$

(ii) Ist $\Phi \in \mathrm{End}(V)$ *selbstadjungiert, so existiert eine ONB* $\mathscr{B}$ *von* V *bzgl.* B *und* $t_1,\dots,t_n \in \mathbb{R}$ *mit*

$$D_{\mathscr{B}}(\Phi) = \operatorname{diag}(t_1,\dots,t_n). \qquad \square$$

Identifizieren wir $\mathbb{C}$ mit $\mathbb{R}^2$ via $a+ib \mapsto (a,b)^\top$, so entspricht die Abbildung $\mathbb{C} \to \mathbb{C}$, $z \mapsto e^{it}$ einer Drehung um den Winkel t im mathematisch positiven Sinne. Unitäre Endomorphismen sind also durch Produkte solcher Drehungen in zueinander orthogonalen Kopien von $\mathbb{C}$ gegeben. Selbstadjungierte Endomorphismen sind entsprechende durch (reelle) Streckungen/Stauchungen in paarweise orthogonalen Kopien von $\mathbb{C}$ gegeben. Die Eigenwerte $e^{it_1},\dots,e^{it_n}$ bzw. $t_1,\dots,t_n$ sind dabei durch Φ bis auf Reihenfolge eindeutig bestimmt.

Der Spektralsatz hat nicht nur Konsequenzen für die Klassifikation unitärer und selbstadjungierter Endomorphismen, sondern auch für die Klassifikation hermitescher Sesquilinearformen.

Bemerkung 8.2.11 (Anwendung auf hermitesche Formen)**.** Sei B eine hermitesche Sesquilinearform auf einem komplexen Vektorraum V. Wir wählen eine Basis $\mathscr{B}$ und erhalten eine hermitesche Matrix $A = D_{\mathscr{B}}(B)$. Nach dem Spektralsatz existiert dann eine Matrix S mit $S^{-1}AS = \operatorname{diag}\lambda_1,\dots,\lambda_n$, wobei $\lambda_1,\dots,\lambda_n$ die Eigenwerte von A (mit geometrischen Vielfachheiten) sind. Da A hermitesch ist, sind $\lambda_1,\dots,\lambda_n$ reell. Setzen wir $T := \overline{S}$, so erhalten wir

$$T^\top AT = S^*AS = S^{-1}AS = \operatorname{diag}\lambda_1,\dots,\lambda_n.$$

Die Spalten von T bilden also eine OGB von (V,B)! Indem wir diese Spalten normieren, können wir $\lambda_1,\dots,\lambda_n$ auf -1 oder 0 oder 1 normieren. Wir erhalten eine 1 (bzw. -1 bzw. 0) genau dann, wenn λ_j positiv (bzw. negativ bzw. 0) ist. Damit haben wir den folgenden Satz bewiesen.

Satz 8.2.12 (Signatursatz)**.** *Ist* $B : V \times V \to \mathbb{C}$ *eine hermitesche Sesquilinearform,* $\mathscr{B}$ *eine Basis von* V *und* $A = D_{\mathscr{B}}(B)$*, so sind die Signatur* (r_+,r_-,r_0) *und der Witt-Index* r *von* B *wie folgt gegeben:*

(i) $r_0 = \operatorname{def}(A)$.

(ii) $r_+ = \sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(0,\infty)} \dim V_\lambda(A)$ *und* $r_- = \sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(-\infty,0)} \dim V_\lambda(A)$.

(iii) $r = \min\left\{\sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(0,\infty)} \dim V_\lambda(A), \sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(-\infty,0)} \dim V_\lambda(A)\right\}$. $\square$

Als Spezialfall halten wir fest:

Korollar 8.2.13 (Eigenwertkriterium)**.** *Eine hermitesche Matrix A ist genau dann positiv-definit (bzw. positiv-semidefinit), wenn alle Eigenwerte von A positiv (bzw. nicht-negativ) sind.* □

Beispiel 8.2.14. Es sei A wie in (8.2.1) und $B : \mathbb{C}^3 \times \mathbb{C}^3 \to \mathbb{C}, (v,w) \mapsto v^\top A\overline{w}$. Wir haben in Beispiel 8.2.6 gesehen, dass

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}^* A \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} = \operatorname{diag}(0,-1,-1)$$

gilt. Folglich ist

$$\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right)$$

eine OGB für B, und B hat Signatur (0,2,1) und Witt-Index 0.

Der Spektralsatz gibt also auch eine neue Methode, um OGBen zu bestimmen. Diese ist in der Regel aber nicht schneller als der symmetrische Gauß-Algorithmus. Zur Bestimmung der Signatur ist der Spektralsatz aber dem symmetrischen Gaußalgorithmus vorzuziehen. Dazu muss man ja nur das charakteristische Polynom von A bestimmen. (Man beachte, dass die algebraischen und geometrischen Vielfachheiten der Eigenwerte übereinstimmen, da A diagonalisierbar ist!)

Bemerkung 8.2.15 (Schiefhermitesche Formen)**.** Jede schiefhermitesche Matrix A (d.h. $A \in \mathbb{C}^{n\times n}$ mit $A^* = -A$) ist normal (denn $AA^* = -A^2 = A^*A$) und ist λ ein Eigenwert von A, so gilt $V_\lambda(A) = V_{\overline{\lambda}}(A^*) = V_{-\overline{\lambda}}(A)$, also $\lambda = -\overline{\lambda}$, d.h. $\lambda \in \mathbb{R}i$. Wenden wir dies auf die darstellende Matrix A einer schief-hermitesche Sesquilinearform $B : V \times V \to \mathbb{C}$ auf einem $\mathbb{C}$-Vektorraum V an, so sehen wir, dass B eine Orthogonalbasis $(v_1,\dots,v_n)$ besitzt, wobei notwendigerweise $B(v_j,v_j) \in \mathbb{R}i$ für alle $j \in \{1,\dots,n\}$ gilt.

Wir geben nun noch eine dritte Formulierung des Spektralsatzes. Diese ist für endlichdimensionale Vektorräume zum gewöhnlichen Spektralsatz äquivalent, aber sie verallgemeinert sich besser auf gewisse unendlichdimensionale Vektorräume mit Skalarprodukt. Unendlichdimensionale Verallgemeinerungen des Spektralsatzes spielen eine zentrale Rolle in der mathematischen Formulierung der Quantenmechanik; mehr dazu in einer Vorlesung über FUNKTIONALANALYSIS (oder MODERNE THEORETISCHE PHYSIK I).

Bemerkung 8.2.16 (Erinnerung)**.** Wir benötigen zwei Resultate aus den Übungen; es sei dazu (V,B) ein unitärer Vektorraum.

(i) Ein Endomorphismus $\pi \in \operatorname{End}(V)$ ist genau dann eine Orthogonalprojektion (nämlich die Orthogonalprojektion auf $\operatorname{Bild}(\pi)$ mit Kern $\operatorname{Bild}(\pi)^\perp$, wenn $\pi = \pi^* = \pi^2$ gilt.

(ii) Ein Endomorphismus $\Phi \in \operatorname{End}(V)$ ist genau dann diagonalisierbar, wenn paarweise verschiedene $\lambda_1,\dots,\lambda_k \in \mathbb{C}$ und Endomorphismen $\pi_1,\dots,\pi_k$ von V mit den folgenden Eigenschaften existieren:

(S1) $\pi_j^2 = \pi_j$ und $\pi_j \neq 0$ für alle $j \in \{1,\dots,k\}$.

(S2) $\pi_i \circ \pi_j = 0$ für alle $i, j \in \{1, \dots, k\}$ mit $i \neq j$.

(S3) $\Phi = \sum_{j=1}^{k} \lambda_j \pi_j$.

In diesem Fall sind $\lambda_1, \dots, \lambda_k$ genau die verschiedenen Eigenwerte von Φ und für $j \in \{1, \dots, n\}$ gilt $\mathrm{Bild}(\pi_j) = V_{\lambda_j}(\Phi)$.

Wir geben nun ein analoges Kriterium für unitäre Diagonalisierbarkeit:

Satz 8.2.17 (Komplexer Spektralsatz, Dritte Form)**.** *Es sei (V, B) ein unitärer Vektorraum und $\Phi \in \mathrm{End}(V)$. Dann ist Φ genau dann unitär diagonalisierbar, wenn paarweise verschiedene $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ und Endomorphismen $\pi_1, \dots, \pi_k$ von V mit den folgenden Eigenschaften existieren:*

(U1) $\pi_j^2 = \pi_j^* = \pi_j$ *und* $\pi_j \neq 0$ *für alle* $j \in \{1, \dots, k\}$.

(U2) $\pi_i \circ \pi_j = 0$ *für alle* $i, j \in \{1, \dots, k\}$ *mit* $i \neq j$.

(U3) $\Phi = \sum_{j=1}^{k} \lambda_j \pi_j$.

Im diesem Fall sind $\lambda_1, \dots, \lambda_k$ die Eigenwerte von Φ und für $j \in \{1, \dots, n\}$ gilt $\mathrm{Bild}(\pi_j) = V_{\lambda_j}(\Phi)$*, insbesondere sind die Paare $(\lambda_1, \pi_1), \dots, (\lambda_k, \pi_k)$ durch Φ bis auf Reihenfolge eindeutig bestimmt.*

Beweis. Falls $\lambda_1, \dots, \lambda_k, \pi_1, \dots, \pi_k$ existieren, die (U1) und (U3) erfüllen, so gilt

$$\Phi^* = \sum_{j=1}^{k} \overline{\lambda}_j \pi_j^* = \sum_{j=1}^{k} \overline{\lambda}_j \pi_j.$$

Gilt zusätzlich noch (U2), so erhalten wir

$$\Phi \circ \Phi^* = \left(\sum_{i=1}^{k} \lambda_i \pi_i \right) \circ \left(\sum_{j=1}^{k} \overline{\lambda}_j \pi_j \right) = \sum_{i,j=1}^{k} \lambda_i \overline{\lambda}_j \underbrace{\pi_i \circ \pi_j}_{=\delta_{ij}\pi_i} = \sum_{j=1}^{k} |\lambda_j|^2 \pi_j = \left(\sum_{i=1}^{k} \overline{\lambda}_i \pi_i \right) \circ \left(\sum_{j=1}^{k} \lambda_j \pi_j \right) = \Phi^* \circ \Phi,$$

also ist Φ normal und daher nach dem 2. Spektralsatz unitär diagonalisierbar.

Umgekehrt sei Φ unitär diagonalisierbar mit verschiedenen Eigenwerten $\lambda_1, \dots, \lambda_k$ und es sei π_j die Orthogonalprojektion auf $V_{\lambda_j}(\Phi)$. Nach Bemerkung 8.2.16 gilt dann (U1). Sind nun $i, j \in \{1, \dots k\}$ verschieden, so gilt $V_{\lambda_i}(\Phi) \perp V_{\lambda_j}(\Phi)$ und daher $\mathrm{Bild}(\pi_j) \subseteq \ker(\pi_i)$ und daher gilt (U2). Ist nun $v \in V$, so gilt

$$V = V_{\lambda_1}(\Phi) \oplus \dots \oplus V_{\lambda_k}(\Phi) \implies v = \sum_{j=1}^{k} \pi_j(v) \implies \Phi(v) = \sum_{j=1}^{k} \Phi(\pi_j(v)) = \sum_{j=1}^{k} \lambda_j \pi_j(v),$$

und daher (U3). Dies zeigt die Äquivalenz der beiden Bedingungen, und die Charakterisierung der λ_j und π_j folgt dann aus Bemerkung 8.2.16. □

Mann kann (U1)–(U3) auch so formulieren: Es gibt eine eindeutig bestimmte Abbildung

$$P : \mathrm{spec}_{\mathbb{C}}(\Phi) \to \{\pi \in \mathrm{End}(V) | \pi = \pi^* = \pi^2\} \tag{8.2.2}$$

mit $P(\lambda) \circ P(\mu) = 0$ für alle $\lambda \neq \mu$, so dass

$$\Phi = \sum_{\lambda \in \mathrm{spec}_{\mathbb{C}}(\Phi)} \lambda P(\lambda). \tag{8.2.3}$$

Definition 8.2.18. Die Abbildung P aus (8.2.2) heißt die *Spektralschar* von Φ und die Zerlegung (8.2.3) heißt die *Spektralzerlegung* von Φ.

Wie eingangs erwähnt kann man (unter geeigneten Voraussetzungen) auch gewissen Endomorphismen vollständiger unendlichdimensionaler unitärer Räume (sogenannter *Hilberträume*) eine Spektralschar (also eine projektorwertige Funktion auf dem Spektrum) zuordnen. In der Spektralzerlegung muss man dann im Allgemeinen die Summe durch ein Integral ersetzen. Wir hoffen, dass Sie das wiedererkennen, wenn Sie in einigen Semestern die Funktionalanalysis (oder Quantenmechanik) hören.

Konstruktion 8.2.19 (Spektralkalkül)**.** Es sei (V,B) ein unitärer Vektorraum und $\Phi \in \mathrm{End}(V)$ normal mit Spektralzerlegung $\Phi = \sum_{j=1}^{k} \lambda_j \pi_j$. Ist $f : \mathrm{spec}_{\mathbb{C}}(\Phi) \to \mathbb{C}$ eine beliebige Funktion, so definieren wir

$$f(\Phi) := \sum_{j=1}^{k} f(\lambda_j)\pi_j.$$

Nach der 3. Version des Spektralsatzes ist dies wieder normal[3] und es gilt

$$\mathrm{spec}_{\mathbb{C}}(f(\Phi)) = f[\mathrm{spec}_{\mathbb{C}}(\Phi)]. \tag{8.2.4}$$

Bezeichnet $\mathrm{Abb}(\mathrm{spec}_{\mathbb{C}}(\Phi),\mathbb{C})$ die Menge der komplexwertigen Abbildungen auf $\mathrm{spec}_{\mathbb{C}}(\Phi)$, so erhalten wir also eine Abbildung

$$\mathrm{Ev}_\Phi : \mathrm{Abb}(\mathrm{spec}_{\mathbb{C}}(\Phi),\mathbb{C}) \to \mathrm{End}_{\mathbb{C}}(V), \quad f \mapsto f(\Phi).$$

Diese heißt der *Spektralkalkül* von Φ.

Analog können wir auch einen Spektralkalkül für normale Matrizen definieren: Ist $A \in \mathbb{C}^{n\times n}$ normal und $\Phi_A : \mathbb{C}^n \to \mathbb{C}^n$, $v \mapsto Av$, so definieren wir $f(A)$ für eine beliebige Funktion $f : \mathrm{spec}_{\mathbb{C}}(A) \to \mathbb{C}$ durch die Gleichung

$$f(A)v = f(\Phi_A)(v) \quad (v \in V).$$

Ist $A = S\mathrm{diag}(\lambda_1,\dots,\lambda_n)S^*$ mit $S \in \mathrm{U}_n(\mathbb{C})$, so ist also

$$f(A) = S\mathrm{diag}(f(\lambda_1),\dots,f(\lambda_n))S^*$$

Beispiel 8.2.20 (Spektralkalkül für Polynome)**.** Es sei $\Phi \in \mathrm{End}(V)$ normal und $f(X) = a_0 + a_1X + \cdots + a_mX^m \in \mathbb{C}[X]$. Wir können dann Φ auf zwei Arten in f einsetzen: In Beispiel 5.4.40 haben wir den Einsetzungshomomorphismus durch

$$f(\Phi) = \mathrm{ev}_\Phi(f) = a_0 + a_1\Phi + \cdots + a_m\Phi^m$$

definiert. In Konstruktion 8.2.19 haben wir hingegen $f(\Phi) = \mathrm{Ev}_\Phi(f)$ via Spektralkalkül definiert. Wir wollen uns nun überlegen, dass diese beiden Definitionen übereinstimmen, dass also der Spektralkalkül für normale Endomorphismen den Einsetzungshomomorphismus von Polynomen auf beliebige Funktionen auf dem Spektrum erweitert.

[3] Dies folgt aus der folgenden Beobachtung (Übung!): Sind π_i und π_j Orthogonalprojektionen mit $\pi_i \circ \pi_j = \pi_j \circ \pi_i = 0$, so stehen die entsprechenden Bilder V_i und V_j senkrecht aufeinander und $\pi_i + \pi_j$ ist die Orthogonalprojektion auf $V_i \oplus V_j$.

Zum Beweis müssen wir uns überlegen, dass

$$\mathrm{ev}_\Phi(f)(v) = \mathrm{Ev}_\Phi(f)(v)$$

für alle $v \in V$ gilt. Da $\mathrm{ev}_\Phi(f)$ und $\mathrm{Ev}_\Phi(f)(v)$ linear sind, genügt es dies für v in einer beliebigen Basis von V zu zeigen; wir dürfen daher annehmen, dass v ein Eigenvektor von Φ ist. Ist λ der zugehörige Eigenwert, so ist aber

$$\mathrm{ev}_\Phi(f)(v) = (a_0 + a_1\Phi + \cdots + a_m\Phi^m)(v) = a_0 v + a_1\lambda v + \cdots + a_m\lambda^m v = f(\lambda)v = \mathrm{Ev}_\Phi(f)(v).$$

Beispiel 8.2.21. Wir betrachten die Funktion $f : \mathbb{R} \to \mathbb{C}$, $\lambda \mapsto 2^{-\lambda}$. Ist $C \in \mathbb{C}^{n\times n}$ eine beliebige hermitesche Matrix, so gilt $\mathrm{spec}_{\mathbb{C}}(C) \subseteq \mathbb{R}$, und daher ist

$$2^{-C} := f(C)$$

wohldefiniert. Für die symmetrische Matrix

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

haben wir in Beispiel 8.2.6 gezeigt, dass

$$A = S\,\mathrm{diag}(0,-1,-1)S^*, \quad \text{wobei} \quad S := \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix},$$

unitär ist. Es gilt daher

$$2^{-A} = S\,\mathrm{diag}(2^{-0}, 2^{-(-1)}, 2^{-(-1)})S^* = S\,\mathrm{diag}(1,2,2)S^* = \frac{1}{2}\cdot\begin{pmatrix} 3 & 0 & -1 \\ 0 & 4 & 0 \\ -1 & 0 & 3 \end{pmatrix}.$$

Wir stellen nun einige Eigenschaften des Spektralkalküls zusammen.

Übung 8.2.22 (Lagrange-Interpolation)**.** Es seien $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ paarweise verschieden und es sei $f : \{\lambda_1, \ldots, \lambda_k\} \to \mathbb{C}$. beliebig. Wir definieren $F \in \mathbb{C}[X]$ durch

$$F(X) = \sum_{j=1}^{k} f(\lambda_j) \prod_{l \neq j} \frac{X - \lambda_l}{\lambda_j - \lambda_l}$$

Zeigen Sie, dass F ein *Interpolationspolynom* für f ist, dass also gilt

$$F(\lambda_j) = f(\lambda_j) \quad (j \in \{1, \ldots, k\}).$$

Proposition 8.2.23 (Abbildungseigenschaften des Spektralkalküls)**.** *Ist* $\Phi \in \mathrm{End}(V)$ *normal und* $f : \mathrm{spec}_{\mathbb{C}}(\Phi) \to \mathbb{C}$ *beliebig, so gilt:*

(i) Es existiert ein $F \in \mathbb{C}[X]$ *mit* $f(\Phi) = F(\Phi)$.

(ii) $f(\Phi)$ *ist normal und vertauscht mit* Φ.

(iii) *Ist* $g : f[\mathrm{spec}(\Phi)] \to \mathbb{C}$ *eine weitere Funktion, so sind* $g(f(\Phi))$ *und* $(g \circ f)(\Phi)$ *definiert, und es gilt.*

$$(g \circ f)(\Phi) = g(f(\Phi)). \tag{8.2.5}$$

(iv) $f(\Phi)$ *ist genau dann invertierbar, wenn* $0 \notin f[\mathrm{spec}_{\mathbb{C}}(\Phi)]$*, und in diesem Fall ist* $f(\Phi)^{-1} = g(\Phi)$*, wobei* $g : \mathrm{spec}_{\mathbb{C}}(\Phi) \to \mathbb{C}$*,* $g(\lambda) := 1/f(\lambda)$*.*

Beweis. (i) folgt sofort aus Übung 8.2.22.

(ii) Dass $f(\Phi)$ normal ist, haben wir bereits in Konstruktion 8.2.19 gesehen. Ist $F \in \mathbb{C}[X]$ wie in (i), so liegen sowohl Φ als auch $f(\Phi) = F(\Phi)$ im Bild des Auswärtungshomomorphismus $\mathrm{ev}_\Phi : \mathbb{C}[X] \to \mathrm{End}(V)$. Da $\mathbb{C}[X]$ eine kommutative Algebra ist, ist auch das Bild kommutativ, also vertauschen Φ und $f(\Phi)$.

(iii) Wohldefiniertheit folgt sofort aus (8.2.4). Ist v ein Eigenvektor zu Φ zum Eigenwert λ, so gilt nach Definition

$$(g \circ f)(\Phi)(v) = (g \circ f)(\lambda)(v) = g(f(\Phi))(v),$$

also gilt (8.2.5) für alle Vektoren in einer Basis von V und daher für alle $v \in V$.

(iv) Die erste Aussage folgt sofort aus $\mathrm{spec}_{\mathbb{C}}(f(\Phi)) = f[\mathrm{spec}_{\mathbb{C}}(\Phi)]$ und dem Injektivitätskriterium. Für die zweite Aussage genügt es zu zeigen, dass $f(\Phi)g(\Phi)v = v$ für jeden Eigenvektor v von V gilt, und ist λ der zugehörige Eigenwert, so gilt

$$f(\Phi)g(\Phi)v = f(\lambda)g(\lambda)v = f(\lambda)f(\lambda)^{-1}v = v. \qquad \square$$

Beispiel 8.2.24 (Quadratwurzeln)**.** Es sei $A \in \mathbb{C}^{n\times n}$ eine positiv-semidefinite hermitesche Matrix, so dass A normal mit $\mathrm{spec}_{\mathbb{C}}(A) \subseteq [0,\infty)$ ist. Ist $f : \mathrm{spec}_{\mathbb{C}}(A) \to \mathbb{C}$ gegeben durch $f(\lambda) := \sqrt{\lambda}$, so definieren wir die *positive normale Quadratwurzel* von A durch $\sqrt{A} := f(A)$. Nach Proposition 8.2.23 ist $\sqrt{A}$ normal und vertauscht mit A, und wenden wir (8.2.5) mit $g(\lambda) = \lambda^2$ an, so erhalten wir

$$\sqrt{A}^2 = A.$$

Eine normale Matrix mit reellem nicht-negativem Spektrum besitzt also eine normale Quadratwurzel mit reellen nicht-negativen Spektrum.

Beispiel 8.2.24 ist Ausdruck eines allgemeinen Prinzips: Kann man Gleichungen auf der Ebene der Spektren lösen (z.B. die Gleichung $\mu^2 = \lambda$), so kann man diese Gleichungen auch auf der Ebene der normalen Matrizen lösen (z.B. $B^2 = A$). Wir illustrieren das anhand eines anderen Beispiels; dazu benötigen wir:

Lemma 8.2.25 (Hermitesche Matrizen)**.** *Für eine normale Matrix* $A \in \mathbb{C}^{n\times n}$ *gilt*

$$\mathrm{spec}_{\mathbb{C}}(A) \subseteq \mathbb{R} \iff A = A^*.$$

Beweis. Ist $\mathrm{spec}_{\mathbb{C}}(A) \subseteq \mathbb{R}$, so existieren nach dem Spektralsatz $S \in \mathrm{U}_n(\mathbb{C})$ und $D \in \mathrm{Diag}_n(\mathbb{R})$ mit $A = SDS^*$. Es gilt dann

$$A^* = (SDS^*)^* = (S^*)^* D^* S^* = SDS^* = A.$$

Die Umkehrung folgt aus Beispiel 8.1.18.(i). $\square$

Bemerkung 8.2.26 (Exponentialfunktion auf hermiteschen Matrizen)**.** Die Exponentialreihe

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

konvergiert (z.B. nach dem Quotientenkriterium) für alle $z \in \mathbb{C}$ absolut und definiert eine glatte Funktion $\exp : \mathbb{C} \to \mathbb{C}^\times$. Schränken wir diese Funktion auf $\mathbb{R}$ ein so erhalten wir eine Funktion $\exp : \mathbb{R} \to (0,\infty)$. Wegen $\exp' = \exp$ ist diese Funktion streng monoton wachsend und wegen $\lim_{x\to-\infty} \exp(x) = 0$ und $\lim_{x\to\infty} \exp(x) = \infty$ ist sie surjektiv, also bijektiv. Wir bezeichnen mit $\log : (0,\infty) \to \mathbb{R}$ die Umkehrfunktion.

Im Folgenden bezeichne $\mathrm{Herm}_n(\mathbb{C}) \subseteq \mathbb{C}^{n\times n}$ den $\mathbb{R}$-Vektorraum der hermiteschen Matrizen und $\mathrm{Pd}_n(\mathbb{C}) \subseteq \mathrm{Herm}_n(\mathbb{C})$ die Teilmenge der positiv definiten Matrizen. Ist $A \in \mathrm{Herm}_n(\mathbb{C})$, so ist A normal, und daher ist $\exp(A)$ definiert. Weiter gilt

$$\mathrm{spec}_{\mathbb{C}}(\exp(A)) = \exp[\mathrm{spec}_{\mathbb{C}}(A)] \subseteq \exp[\mathbb{R}] \subseteq (0,\infty).$$

Nach Lemma 8.2.25 ist daher $\exp(A)$ hermitesch und wegen Korollar 8.3.9 zusätzlich positiv definit. Wir erhalten also eine wohldefinierte Funktion

$$\exp : \mathrm{Herm}_n(\mathbb{C}) \to \mathrm{Pd}_n(\mathbb{C}).$$

Ist andererseits $A \in \mathrm{Pd}_n(\mathbb{C})$, so ist A normal mit $\mathrm{spec}_{\mathbb{C}}(A) \subseteq (0,\infty)$, und daher ist $\log(A)$ wohldefiniert mit $\mathrm{spec}_{\mathbb{C}}(A) \subseteq \mathbb{R}$. Aus Lemma 8.2.25, folgt daher, dass $\log(A) \in \mathrm{Herm}_n(\mathbb{C})$. Mit Proposition 8.2.23.(iii) folgt dann, dass

$$\log : \mathrm{Pd}_n(\mathbb{C}) \to \mathrm{Herm}_n(\mathbb{C})$$

die Umkehrfunktion von exp ist. Insbesondere ist exp bijektiv und es gilt

$$\mathrm{Pd}_n(\mathbb{C}) = \exp[\mathrm{Herm}_n(\mathbb{C})].$$

Zusammenfassung von Abschnitt 8.2.

(1) Eine komplexe Matrix ist genau dann unitär diagonalisierbar, wenn sie normal ist. Folglich besitzten normale Endomorphismen unitärer Vektorräume eine ONB aus Eigenvektoren.

(2) Die Signatur einer hermiteschen Sesquilinearform über $\mathbb{C}$ ist gegeben durch die Anzahl der Eigenwerte einer beliebigen darstellenden Matrix mit dem entsprechenden Vorzeichen (gezählt mit Vielfachheit). Komplexe Skalarprodukte entsprechen daher hermiteschen Matrizen mit positiven reellen Eigenwerten.

(3) Jeder normale Endomorphismus kann in eine beliebige komplexwertige Funktion auf seinem Spektrum eingesetzt werden, indem man in seiner Spektralzerlegung die Eigenwerte in die Funktion einsetzt. Dies führt das Lösen von Gleichungen in normalen Matrizen auf das Lösungen von Gleichungen in $\mathbb{C}$ zurück.

[13.06.24]

8.3 Orthogonale Diagonalisierung und Isometrie-Normalform

Im letzten Abschnitt haben wir gesehen, dass sich komplexe normale Matrizen unitär diagonalisieren lassen. Wie sieht es nun mit reellen normalen Matrixen aus?

Definition 8.3.1. Matrizen $A,B \in \mathbb{R}^{n\times n}$ heißen *orthogonal äquivalent*, falls ein $S \in \mathrm{O}_n(\mathbb{R})$ existiert mit $A = OBO^{-1} = OBO^\top$. Weiter heißt A *orthogonal diagonalisierbar*, wenn A orthogonal äquivalent zu einer reellen Diagonalmatrix ist.

Nach Definition ist jede orthogonale reelle Matrix insbesondere eine unitäre komplexe Matrix, und daher impliziert orthogonale Diagonalisierbarkeit automatisch unitäre Diagonalisierbarkeit. Mit anderen Worten, jede orthogonal diagonalisierbare Matrix A ist normal (d.h. $AA^\top = A^\top A$). Die Umkehrung gilt nicht:

Beispiel 8.3.2 (Normal ist nicht genug)**.** Ist $A \in \mathbb{R}^{n\times n}$ eine orthogonale Matrix, so gilt $AA^\top = \mathrm{Id} = A^\top A$, also ist A normal. Im Allgemeinen ist A aber nicht $\mathbb{R}$-diagonalisierbar und daher erst recht nicht orthogonal diagonalisierbar - bekanntlich ist eine ebene Drehung um den Ursprung genau dann $\mathbb{R}$-diagonalisierbar, wenn der Drehwinkel ein Vielfaches von π ist.

Bemerkung 8.3.3 (Von $\mathbb{C}$ nach $\mathbb{R}$)**.** Es sei $A \in \mathbb{R}^{n\times n}$ normal. Wir bezeichnen mit $\Phi_\mathbb{R} : \mathbb{R}^n \to \mathbb{R}^n$ bzw. $\Phi_\mathbb{C} : \mathbb{C}^n \to \mathbb{C}^n$ die durch Multiplikation mit A definierten normalen Endomorphismen. Da das charakteristische Polynom von A reell (und daher invariant unter der Galois-Involution) sind, sind die komplexen Eigenwerte von A entweder reell oder treten als komplex-konjugierte Paare auf. Im Folgenden bezeichnen $\mu_1, \overline{\mu}_1, \ldots, \mu_k, \overline{\mu}_k$ die komplex-konjugierten Paare nichtreeller Eigenwerte von A und $\lambda_{2k+1}, \ldots, \lambda_n$ die reellen Eigenwerte von A (jeweils aufgezählt mit algebraischen Vielfachheiten). Die zugehörigen Eigenräume in $\mathbb{C}^n$ bilden dann eine orthogonale Zerlegung, d.h.

$$\mathbb{C}^n = \big(V_{\mu_1}(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}_1}(\Phi_\mathbb{C})\big) \oplus \ldots \oplus \big(V_{\mu_k}(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}_k}(\Phi_\mathbb{C})\big) \oplus V_{\lambda_{2k+1}}(\Phi_\mathbb{C}) \oplus \ldots \oplus V_{\lambda_n}(\Phi_\mathbb{C}).$$

Der aus der Theorie der reellen Jordannormalform bekannte Galois-Abstieg liefert dann

$$\mathbb{R}^n = \big(V_{\mu_1}(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}_1}(\Phi_\mathbb{C})\big)^\sigma \oplus \ldots \oplus \big(V_{\mu_k}(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}_k}(\Phi_\mathbb{C})\big)^\sigma \oplus V_{\lambda_{2k+1}}(\Phi_\mathbb{R}) \oplus \ldots \oplus V_{\lambda_n}(\Phi_\mathbb{R}).$$

Hierbei haben wir verwendet, dass zwei Unterräume von $\mathbb{R}^n$ genau dann orthogonal sind, wenn sie als Unterräume von $\mathbb{C}^n$ orthogonal sind. Wie können wir nun in den einzelnen Summanden geschickte Basen finden? Im Fall der rellen Eigenwerte können wir einfach wieder für jeden der Eigenräume eine ONB wählen. Wir betrachten nun den Fall komplexer Eigenwertpaare.

Es sei dazu $\mu \in \{\mu_1, \ldots, \mu_k\}$ fixiert. Da $\Phi_\mathbb{C}$ unitär diagonalisierbar ist, besitzt $V_\mu(\Phi_\mathbb{C})$ eine OGB $(v_1, \ldots, v_l)$, deren Normalisierung beliebig gewählt werden kann. Wir werden später noch sehen, dass es zweckmäßig ist, die Normalisierung

$$\|v_1\| = \cdots = \|v_l\| = \sqrt{2}$$

zu wählen. Aus der rellen Jordantheorie wissen wir, dass $(\overline{v}_1, \ldots, \overline{v}_l)$ eine Basis von $V_{\overline{\mu}}(\Phi_\mathbb{C})$. Wegen $B_0(\overline{v}_i, \overline{v}_j) = \overline{v_i}^\top v_j = \overline{B_0(v_i, v_j)}$ ist diese Basis wieder orthogonal, und es gilt $\|\overline{v}_j\| = \sqrt{2}$.

Eine geordnete Basis von $\left(V_\mu(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}}(\Phi_\mathbb{C})\right)^\sigma$ ist nun gegeben durch

$$\mathscr{B} = (\mathrm{Re}(v_1), \mathrm{Im}(v_1), \ldots, \mathrm{Re}(v_l), \mathrm{Im}(v_l)).$$

Wegen $\langle \mathrm{Re}(v_j), \mathrm{Im}(v_j)\rangle_\mathbb{R} \subseteq \langle v_j, \overline{v}_j\rangle_\mathbb{C}$ und $\langle v_i, \overline{v}_i\rangle_\mathbb{C} \perp \langle v_j, \overline{v}_j\rangle_\mathbb{C}$ für $i \neq j$ gilt also

$$\left(V_{\mu_1}(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}_1}(\Phi_\mathbb{C})\right)^\sigma = \langle \mathrm{Re}(v_1), \mathrm{Im}(v_1)\rangle_\mathbb{R} \oplus \ldots \oplus \langle \mathrm{Re}(v_l), \mathrm{Im}(v_l)\rangle$$

Wir überlegen uns nun, was wir über die Längen und Winkel der Basisvektoren sagen können. Wegen $V_\mu(\Phi) \perp V_{\overline{\mu}}(\Phi)$ gilt für $j \in \{1, \ldots, l\}$, dass

$$\begin{aligned} 0 &= B_0(v_j, \overline{v_j}) = B_0\left(\mathrm{Re}(v_j) + i\mathrm{Im}(v_j), \mathrm{Re}(v_j) - i\mathrm{Im}(v_j)\right) \\ &= \left(\|\mathrm{Re}(v_j)\|^2 - \|\mathrm{Im}(v_j)\|^2\right) + 2i \cdot B_0\left(\mathrm{Re}(v_j), \mathrm{Im}(v_j)\right) \end{aligned}$$

Da sowohl Real- und Imaginärteil verschwinden müssen, folgt $\mathrm{Re}(v_j) \perp \mathrm{Im}(v_j)$ und $\|\mathrm{Re}(v_j)\|^2 = \|\mathrm{Im}(v_j)\|^2$. Wegen Pythagoras gilt dann

$$\|\mathrm{Re}(v_j)\|^2 + \|\mathrm{Im}(v_j)\|^2 = \|v_j\|^2 = \sqrt{2}^2 = 2,$$

also folgt, dass $\|\mathrm{Re}(v_j)\|^2 = \|\mathrm{Im}(v_j)\|^2 = 1$. Dies rechtfertigt unsere Wahl der Normalisierung und zeigt, dass $\mathscr{B}$ eine OGB von $\left(V_{\mu_1}(\Phi_\mathbb{C}) \oplus V_{\overline{\mu}_1}(\Phi_\mathbb{C})\right)^\sigma$ ist. Ist $\mu = a + bi$ mit $a, b \in \mathbb{R}$, so wissen wir aus der reellen Jordantheorie, dass $\Phi_\mathbb{R}$ auf $\langle \mathrm{Re}(v_j), \mathrm{Im}(v_j)\rangle$ bzgl. der Basis $(\mathrm{Re}(v_j), \mathrm{Im}(v_j))$ durch die Matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ dargestellt wird. Damit haben wir den folgenden Satz bewiesen.

Satz 8.3.4 (Normaler Galoisabstieg)**.** *Es sei $A \in \mathbb{R}^{n\times n}$ und es seien $\mu_1 = a_1 + ib_1, \overline{\mu}_1, \ldots, \mu_k = a_k + ib_k, \overline{\mu}_k$ die komplex-konjugierten Paare nicht-reeller Eigenwerte von A und $\lambda_{2k+1}, \ldots, \lambda_n$ die reellen Eigenwerte von A (jeweils aufgezählt mit algebraischen Vielfachheiten). Dann existiert eine OGB $\mathscr{B}$ von $\mathbb{R}^n$ bzgl. der $\Phi_A : \mathbb{R}^n \to \mathbb{R}^n$ durch die Matrix*

$$\begin{pmatrix} a_1 & -b_1 & & & & & & 0 \\ b_1 & a_1 & & & & & & \\ & & \ddots & \ddots & & & & \\ & & & a_k & -b_k & & & \\ & & & b_k & a_k & & & \\ & & & & & \lambda_{2k+1} & & \\ & & & & & & \ddots & \\ 0 & & & & & & & \lambda_n \end{pmatrix} \tag{8.3.1}$$

dargestellt wird. Insbesondere ist A orthogonal ähnlich zu dieser Matrix. □

Konkret können wir die Basis $\mathscr{B}$ bestimmen, in dem wir wie folgt vorgehen:

- Für jedes Paar konjugiert-komplexer nicht-reeller Eigenwerte wählen wir eine OGB eines der beiden zugehörigen komplexen Eigenraums, normalisieren diese auf Länge $\sqrt{2}$ und nehmen dann Real- und Imaginärteil zu unserer Basis hinzu.
- Für jeden rellen Eigenwert wählten wir eine OGB des zugehörigen reellen Eigenraums und fügen diese unserer Basis hinzu.

Ausgehend von Satz 8.3.4 können wir nun orthogonale Diagonalisierbarkeit charakterisieren:

Korollar 8.3.5 (Reeller Spektralsatz, Erste Form)**.** *Für $A \in \mathbb{R}^{n\times n}$ sind äquivalent:*

(i) *A ist orthogonal diagonalisierbar.*

(ii) *A ist symmetrisch, d.h. $A = A^\top$.*

(iii) *A ist normal und $\operatorname{spec}_{\mathbb{C}}(A) \subseteq \mathbb{R}$.*

Beweis. (i)$\Longrightarrow$(ii): Ist $A = SDS^\top$ mit D diagonal und $S \in \mathrm{O}_n(\mathbb{R})$, so gilt $A^\top = (SDS^\top)^\top = SD^\top S^\top = SDS^\top = A$.

(ii)$\Longrightarrow$(iii): Dies folgt sofort aus Beispiel 8.1.18.(i).

(iii)$\Longrightarrow$(i): Wenn A normal ist und nur reelle Eigenwerte besitzt, so ist die Matrix aus (8.3.1) diagonal. □

Wie im komplexen Fall erhält man die folgenden Umformulierungen:

Korollar 8.3.6 (Reeller Spektralsatz, Zweite Form)**.** *Ist (V,B) ein euklidischer Vektorraum und $\Phi \in \operatorname{End}(V)$, so sind äquivalent:*

(i) *V besitzt eine ONB aus Eigenvektoren von V.*

(ii) *Sind $\lambda_1,\dots,\lambda_k$ die verschiedenen Eigenwerte von Φ, so gilt*

$$(V,B) = V_{\lambda_1}(\Phi) \perp\!\!\!\perp \dots \perp\!\!\!\perp V_{\lambda_k}(\Phi).$$

(iii) *Φ ist selbstadjungiert.*

(iv) *Φ ist normal und $\operatorname{spec}_{\mathbb{C}}(\Phi) \subseteq \mathbb{R}$.* □

Korollar 8.3.7 (Reeller Spektralsatz, Dritte Form)**.** *Es sei (V,B) ein orthogonaler Vektorraum und $\Phi \in \operatorname{End}(V)$. Dann ist Φ genau dann orthogonal diagonalisierbar, wenn paarweise verschiedene $\lambda_1,\dots,\lambda_k \in \mathbb{R}$ und Endomorphismen $\pi_1,\dots,\pi_k$ von V mit den folgenden Eigenschaften existieren:*

(U1) *$\pi_j^2 = \pi_j^* = \pi_j$ und $\pi_j \neq 0$ für alle $j \in \{1,\dots,k\}$.*

(U2) *$\pi_i \circ \pi_j = 0$ für alle $i,j \in \{1,\dots,k\}$ mit $i \neq j$.*

(U3) *$\Phi = \sum_{j=1}^k \lambda_j \pi_j$.*

Im diesem Fall sind $\lambda_1,\dots,\lambda_k$ die Eigenwerte von Φ und für $j \in \{1,\dots,n\}$ gilt $\operatorname{Bild}(\pi_j) = V_{\lambda_j}(\Phi)$, insbesondere sind die Paare $(\lambda_1,\pi_1),\dots,(\lambda_k,\pi_k)$ durch Φ bis auf Reihenfolge eindeutig bestimmt. □

Auch die im letzen Abschnitt beschriebenen Korollare des Spektralsatzes übertragen sich. Für symmetrische Bilinearformen erhält man beispielsweise:

Satz 8.3.8 (Reeller Signatursatz)**.** *Ist $B : V \times V \to \mathbb{R}$ eine reelle symmetrische Bilinearform, $\mathscr{B}$ eine Basis von V und $A = D_{\mathscr{B}}(B)$, so sind die Signatur (r_+,r_-,r_0) und der Witt-Index r von B wie folgt gegeben:*

(i) *$r_0 = \operatorname{def}(A)$.*

(ii) *$r_+ = \sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(0,\infty)} \dim V_\lambda(A)$ und $r_- = \sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(-\infty,0)} \dim V_\lambda(A)$.*

(iii) *$r = \min\left\{\sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(0,\infty)} \dim V_\lambda(A), \sum_{\lambda\in\operatorname{spec}_{\mathbb{R}}(A)\cap(-\infty,0)} \dim V_\lambda(A)\right\}$.* □

Korollar 8.3.9 (Reelles Eigenwertkriterium)**.** *Eine symmetrische reelle Matrix A ist genau dann positiv-definit (bzw. positiv-semidefinit), wenn alle Eigenwerte von A positiv (bzw. nicht-negativ) sind.* □

Bemerkung 8.3.10 (Reeller Spektralkalkül)**.** Es sei $A \in \mathbb{C}^{n\times n}$ eine normale Matrix und $f : \operatorname{spec}_{\mathbb{C}}(A) \to \mathbb{R}$ eine *reellwertige* Funktion auf dem Spektrum. nach dem (komplexen) Spektralkalkül können wir dann die Matrix $f(A)$ definieren. Diese ist normal mit reellen Eigenwerten, also nach Lemma 8.2.25 stets hermitesch.

Ist $A \in \mathbb{R}^{n\times n}$ sogar eine reelle symmetrische Matrix, so ist $A = SDS^\top$ für ein $S \in \mathrm{O}_n(\mathbb{R})$ und $D = \operatorname{diag}(\lambda_1,\dots,\lambda_n) \in \operatorname{Diag}_n(\mathbb{R})$. Ist f reellwertig, so ist also $f(A) = S\operatorname{diag}(f(\lambda_1),\dots,f(\lambda_n))S^\top$ reell und es gilt $A^\top = S\operatorname{diag}(\lambda_1,\dots,\lambda_n)S^\top = A$. Einsetzen einer reellen symmetrischen Matrix in eine reellwertige Funktion liefert also wieder eine symmetrische reelle Matrix.

Der reelle Spektralsatz macht nur Ausssagen über symmetrische reelle Matrizen. Man kann aber aus dem komplexen Spektralsatz mittels Galoisabstieg auch Normalformen für andere Klassen von normalen reellen Matrizen herleiten. Von besonderem Interesse ist hier der Fall von reellen orthogonalen Matrizen.

Bemerkung 8.3.11 (Orthogonale Automorphismen)**.** Ist $A \in \mathbb{R}^{n\times n}$ orthogonal, so ist A insbesondere eine unitäre komplexe Matrix, und ihre Eigenwerte haben den Betrag 1. Es gibt nun zwei Möglichkeiten:

- Ist λ ein reeller Eigenwert von A, so ist $\lambda \in \{\pm 1\}$.
- Ist μ ein nicht-reeller Eigenwert, so gilt $\mu = e^{-i\theta} = \cos(\theta) - i\sin(\theta)$ für ein $\theta \in (0,\pi)\cup(\pi,2\pi)$.

Aus Satz 8.3.4 ergibt sich daher der folgende Spezialfall:

Korollar 8.3.12 (Normalform für orthogonale Automorphismen)**.** *Sei (V,B) ein euklidischer Vektorraum und $\Phi \in \mathrm{O}(V,B)$. Dann existiert eine ONB $\mathscr{B} = (w_1,\dots,w_n)$ von V und reelle Zahlen $\theta_1,\dots,\theta_k,\lambda_{2k+1},\dots,\lambda_n$ mit $\theta_1,\dots,\theta_k \in (0,\pi)\cup(\pi,2\pi)$ und $\lambda_{2k+1},\dots,\lambda_n \in \{-1,1\}$ mit*

$$D_{\mathscr{B}}(\Phi) = \begin{pmatrix} \cos(\theta_1) & -\sin(\theta_1) & & & & & & & 0 \\ \sin(\theta_1) & \cos(\theta_1) & & & & & & & \\ & & \ddots & & \ddots & & & & \\ & & & & \cos(\theta_k) & -\sin(\theta_k) & & & \\ & & & & \sin(\theta_k) & \cos(\theta_k) & & & \\ & & & & & & \lambda_{2k+1} & & \\ & & & & & & & \ddots & \\ 0 & & & & & & & & \lambda_n \end{pmatrix}. \qquad \square$$

Bemerkung 8.3.13 (Geometrische Bedeutung)**.** Geometrisch bedeutet Korollar 8.3.12 das Folgende: Man findet zunächst eine Reihe von paarweise orthogonalen Ebenen, auf denen Φ als Drehung operiert. Das orthogonale Komplement dieser Ebenen zerlegt sich dann weiter. Für jedes Paar von Eigenwerten der Form $(1,-1)$ finden wir eine Ebene, in der Φ durch eine Geradenspiegelung wirkt, und auch diese Ebenen sind wieder paarweise orthogonal. Spalten wir auch diese Ebenen ab, so bleibt am Ende nur ein Unterraum übrig, auf dem Φ entweder als die Identität oder als die Punktspiegelung am Ursprung (also $-\mathrm{Id}$) wirkt.

Zusammenfassung von Abschnitt 8.3.

(1) Eine reelle Matrix ist genau dann orthogonal diagonalisierbar, wenn sie symmetrisch ist. Folglich besitzten selbstadjungierte Endomorphismen euklidischer Vektorräume eine ONB aus Eigenvektoren.

(2) Die Signatur einer symmetrischen Bilinearform über $\mathbb{R}$ ist gegeben durch die Anzahl der Eigenwerte einer beliebigen darstellenden Matrix mit dem entsprechenden Vorzeichen (gezählt mit Vielfachheit). Reelle Skalarprodukte entsprechen daher symmetrischen Matrizen mit positiven reellen Eigenwerten.

(3) Setzt man reelle symmetrische Matrizen mittels Spektralkalkül in reellwertige Funktionen ein, so erhält man wieder symmetrische Matrizen.

(4) Orthogonale Automorphismen euklidischer Vektorräume zerlegen sich in Drehungen in paarweise orthogonalen Ebenen und Punktspiegelungen in dazu orthogonalen Geraden.

8.4 Polar- und Singulärwertzerlegung

Beispiel 8.4.1 (Polarzerlegung komplexer Zahlen)**.** Es sei $z = a + bi \in \mathbb{C}^\times$ mit $a, b \in \mathbb{R}$. Setzen wir $t := \log|z|$ und $w := \frac{z}{|z|}$, so gilt

$$z = e^t \cdot w, \quad \text{wobei} \quad t \in \mathbb{R} \text{ und } |w| = 1. \tag{8.4.1}$$

Diese Zerlegung ist eindeutig, denn aus (8.4.1) folgt $|z| = |e^t||w| = e^t$, also $t = \log|z|$, und dann $w = e^{-t}z$. Wir nennen Sie die *Polarzerlegung* von z. Fassen wir z, w und t als komplexe (1×1)-Matrizen auf, so ist $z \in \mathrm{GL}_1(\mathbb{C})$, $w \in \mathrm{U}_n(\mathbb{C})$ und $t \in \mathrm{Herm}_1(\mathbb{C})$. Wir sehen also, dass die Abbildung

$$\mathrm{Herm}_1(\mathbb{C}) \times \mathrm{U}_1(\mathbb{C}) \to \mathrm{GL}_1(\mathbb{C}), \quad (t, w) \mapsto \exp(t)w$$

bijektiv ist. Im Folgenden wollen wir diese Zerlegung mittels Spektralkalkül auf invertierbare Matrizen beliebiger Größe verallgemeinern.

Notation 8.4.2. Ist A eine positiv-semidefinite hermitesche Matrix, so schreiben wir $\sqrt{A}$ für die positive normale Quadratwurzel von A wie in Beispiel 8.2.24. Ist A sogar positiv-definit, so schreiben wir $\log(A)$ für die normale Matrix, die aus A durch Einsetzen in die Funktion $\log : (0, \infty) \to \mathbb{R}$ (also die Umkehrfunktion von $\exp : \mathbb{R} \to (0, \infty)$) mittels Spektralkalkül entsteht. Nach Lemma 8.2.25 sind dann $\sqrt{A}$ und $\log(A)$ hermitesch, und nach Korollar 8.3.9 ist A positiv-semidefinit (und positiv-definit, falls A positiv-definit ist).

Proposition 8.4.3 (Eindeutigkeit der positiv-definiten Quadratwurzel)**.** *Sei $A \in \mathbb{C}^{n \times n}$ hermitesch und positiv-definit. Dann ist $B := \sqrt{A}$ die einzige positiv-semidefinite Matrix mit $B^2 = A$.*

Beweis. Sei $C \in \mathbb{C}^{n \times n}$ eine weitere positiv-semidefinite Matrix mit $C^2 = A$. Dann vertauscht C mit A (denn $AC = C^3 = CA$), und daher mit jedem Polynom in A. Nach Proposition 8.2.23.(i) vertauscht C daher insbesondere mit B, und folglich gilt

$$B^2 = A = C^2 \implies 0 = B^2 - C^2 = B^2 - BC + CB - C^2 = (B + C)(B - C).$$

Ist nun $v \in \mathbb{C}^n$, so gilt

$$v^\top (B+C)\overline{v} = \underbrace{v^\top B\overline{v}}_{>0} + \underbrace{v^\top C\overline{v}}_{\geq 0} > 0,$$

also ist $B+C$ positiv-definit, insbesondere invertierbar. Es folgt dann, dass

$$0 = (B+C)^{-1}0 = (B+C)^{-1}(B+C)(B-C) = B-C,$$

also $B = C$. □

Ist z eine komplexe Zahl, so ist $|z|^2 = \overline{z}z = z\overline{z}$ eine nicht-negative reelle Zahl. Analog kann man aus jeder komplexen Matrix eine positiv-semidefinite hermitesche Matrix produzieren:

Satz 8.4.4 (Konstruktion positiv-definiter Matrizen)**.** *Sei $A \in \mathbb{C}^{n\times n}$.*

(i) A ist positiv semi-definit genau dann, wenn eine Matrix $B \in \mathbb{C}^{n\times n}$ existiert mit $A = B^*B$.

(ii) A ist positiv definit genau dann, wenn eine invertierbare Matrix $B \in \mathrm{GL}_n(\mathbb{C})$ existiert mit $A = B^*B$.

Beweis. (i) Ist A positiv semi-definit, so wählen wir $B := \sqrt{A}$. Da B hermitesch ist, gilt dann $B^*B = B^2 = A$. Sei umgekehrt $B \in \mathbb{C}^{n\times n}$ mit $A = B^*B$. Wegen $A^* = (B^*B)^* = B^*(B^*)^* = B^*B = A$ ist A dann hermitesch. Sei $v \in \mathbb{C}^n$ und $w := \overline{B}v$. Dann gilt

$$v^\top A\overline{v} = v^\top B^*B\overline{v} = w^\top \overline{w} \geq 0,$$

also ist A positiv semi-definit.

(ii) Ist A positiv-definit, so ist $B := \sqrt{A}$ hermitesch und invertierbar, und wie in (i) gilt $B^*B = A$. Ist umgekehrt $A = B^*B$, so ist A positiv semi-definit nach (i), und es gilt $\det(A) = |\det(B)|^2$. Ist B invertierbar, so ist $\det(B) \neq 0$ und daher $\det(A) \neq 0$, also ist 0 kein Eigenwert von A, und daher A sogar positiv definit. □

Positiv-definite Matrizen sind also genau die Matrizen der Form B^*B mit B invertierbar. Statt Matrizen der Form B^*B könnten wir auch Matrizen der Form BB^* verwenden (werden dies aber nicht tun):

Übung 8.4.5. Zeigen Sie ganz analog:

(i) A ist positiv semi-definit genau dann, wenn eine Matrix $B \in \mathbb{C}^{n\times n}$ existiert mit $A = BB^*$.

(ii) A ist positiv definit genau dann, wenn eine invertierbare Matrix $B \in \mathrm{GL}_n(\mathbb{C})$ existiert mit $A = BB^*$.

Weitere Charakterisierungen von positiver Definitheit sind wie folgt:

Proposition 8.4.6 (Positiv definite Matrizen und Quadratwurzeln)**.** *Sei $A \in \mathbb{C}^{n\times n}$ hermitesch. Dann sind die folgenden Aussagen äquivalent:*

(i) A ist positiv definit.

(ii) Es existiert eine (eindeutige) positiv definite hermitesche Matrix B mit $B^2 = A$.

(iii) Es existiert eine invertierbare hermitesche Matrix B mit $B^2 = A$.

Ist A reell und symmetrisch, so kann B in (ii) und (iii) ebenfalls reell gewählt werden.

Beweis. (i) $\Longrightarrow$ (ii) folgt sofort aus 8.4.3 und (ii) $\Longrightarrow$ (iii) ist klar.

(iii) $\Longrightarrow$ (i): Es sei $\Phi_B = \sum_{j=1}^{k} \mu_j \pi_j$ die Spektralzerlegung von B. Da B invertierbar und hermitesch ist, gilt dann $\mu_j \in \mathbb{R}^\times$ für alle $j \in \{1,\dots,k\}$. Es ist dann

$$\Phi_A = \Phi_B \circ \Phi_B = \sum_{i=1}^{k}\sum_{j=1}^{k} \mu_i\mu_j \pi_i \circ \pi_j = \sum_{j=1}^{k} \mu_j^2 \pi_j,$$

und da $\mu_1^2,\dots,\mu_k^2$ strikt positive reelle Zahlen sind, ist A hermitesch und positiv-definit. □

Übung 8.4.7. Zeigen Sie ganz analog zu Proposition 8.4.3:

(i) Eine hermitesche Matrix $A \in \mathbb{C}^{n\times n}$ ist genau dann positiv semi-definit, wenn eine hermitesche Matrix B existiert mit $B^2 = A$.

(ii) Eine hermitesche Matrix $A \in \mathbb{C}^{n\times n}$ ist genauu dann positiv definit, wenn eine hermitesche Matrix B existiert mit $\exp(B) = A$.

(iii) Wie lauten die analogen Aussagen für reelle Matrizen?

Wir können nun die Polarzerlegung komplexer Zahlen auf invertierbare komplexe Matrizen verallgemeinern:

Satz 8.4.8 (Komplexe Polarzerlegung)**.** *Die Abbildung*

$$\mathscr{P}_{\mathbb{C}} : U_n(\mathbb{C}) \times \mathrm{Herm}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C}), \quad (U,A) \mapsto U\exp(A)$$

ist eine Bijektion. Die Umkehrabbildung ist gegeben durch

$$B \mapsto (B\sqrt{B^*B}^{\,-1}, \log(\sqrt{B^*B})). \tag{8.4.2}$$

Beweis. Wir überlegen uns zunächst, dass die Formel (8.4.2) eine wohldefinierte Abbildung $\mathscr{Q} : \mathrm{GL}_n(\mathbb{C}) \to U_n(\mathbb{C}) \times \mathrm{Herm}_n(\mathbb{C})$ liefert: Da B invertierbar ist, ist B^*B wegen Satz 8.4.4 positiv definit. Folglich ist $P := \sqrt{B^*B}$ wohldefiniert und positiv-definit, und daher ist $A := \log(\sqrt{B^*B})$ wohldefiniert und hermitesch. Ist weiter $U := B\sqrt{B^*B}^{\,-1}$, so ist

$$U^*U = (BP^{-1})^*(BP^{-1}) = (P^*)^{-1}B^*BP^{-1} = P^{-1}P^2P^{-1} = \mathbf{1},$$

also ist U unitär. Nach Definition gilt offensichtlich $B = U\exp(A) = \mathscr{P}_{\mathbb{C}}(U,A)$, also ist $\mathscr{P}_{\mathbb{C}}$ surjektiv und $\mathscr{Q}$ eine Rechtsinverse zu $\mathscr{P}_{\mathbb{C}}$.

Es bleibt zu zeigen, dass $\mathscr{P}_{\mathbb{C}}$ injektiv ist: Seien U,U' unitär und A,A' hermitesch mit $B = U\exp(A) = U'\exp(A')$. Setzen wir $P := \exp(A)$ und $P' := \exp(A')$. Es gilt dann

$$P^2 = PU^*UP = (UP)^*UP = B^*B = (U'P')^*(U'P') = P'(U')^*U'P' = (P')^2.$$

Wegen Proposition 8.4.3 ist dann $P = P'$. Dies impliziert, dass $U = BP^{-1} = B(P')^{-1} = U'$ ist und wegen Bemerkung 8.2.26 auch $A = A'$. Folglich ist $\mathscr{P}_{\mathbb{C}}$ injektiv und $\mathscr{Q} = \mathscr{P}_{\mathbb{C}}^{-1}$. □

Bemerkung 8.4.9 (Rechts- vs. Linkspolarzerlegung)**.** Ist $B = U\exp(A)$ mit $U \in U_n(\mathbb{C})$ und $A \in \mathrm{Herm}_n(\mathbb{C})$, so gilt im Allgemeinen *nicht*, dass $B = \exp(A)U$, weil A und U nicht miteinander vertauschen. Es ist aber möglich,k Matrizen $U' \in U_n(\mathbb{C})$ und $A' \in \mathrm{Herm}_n(\mathbb{C})$ mit $B = \exp(A')U'$ zu finden. Es gilt nämlich

$$B = \exp(A')U' \iff B^* = (U')^* \exp((A'))^* = (U')^{-1}\exp(A'),$$

und diese Gleichung besitzt nach Satz 8.4.8 eine eindeutige Lösung $(A', U') \in \mathrm{Herm}_n(\mathbb{C}) \times U_n(\mathbb{C})$. Wir sehen also, dass auch die Abbildung $\mathscr{P}'_{\mathbb{C}} : \mathrm{Herm}_n(\mathbb{C}) \times U_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$, $(A, U) \mapsto \exp(A)U$ surjektiv ist, und man rechnet leicht nach, dass die Umkehrabbildung gegeben ist durch

$$(\mathscr{P}'_{\mathbb{C}})^{-1} : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{Herm}_n(\mathbb{C}) \times U_n(\mathbb{C}), \quad B \mapsto (\log(\sqrt{BB^*}), (\sqrt{BB^*})^{-1}B).$$

Definition 8.4.10. Die Abbildungen $\mathscr{P}_{\mathbb{C}}^{-1}$ und $(\mathscr{P}'_{\mathbb{C}})^{-1}$ heißen *komplexe Polarzerlegungen*.

Bemerkung 8.4.11 (Probleme im singulären Fall)**.** Es gibt gute Gründe dafür, dass wir uns bei der Polarzerlegung auf *invertierbare* komplexe Matrizen beschränkt haben. Bereits im eindimensionalen Fall lässt sich die 0 nicht als Produkt einer positiven reellen Zahl und einer komplexen Zahl vom Betrag 1 schreiben. Lassen wir nicht-negative Zahlen statt positiver Zahlen zu, so besitzt die 0 zwar eine Polarzerlegung, aber diese ist nicht eindeutig. Wir haben also nur eine sehr schwache und uneindeutige Verallgemeinerung der Polarzerlegung. Nach dem folgenden Satz gilt diese auch in höheren Dimensionen.

Satz 8.4.12 (Verallgemeinerte Polarzerlegung)**.** *Ist $B \in \mathbb{C}^{n\times n}$ beliebig, so existiert $U \in \mathrm{U}_n(\mathbb{C})$ und eine positiv-semidefinite hermitesche Matrix P mit*

$$B = UP \quad \text{und} \quad P = \sqrt{B^*B}.$$

Zum Beweis benötigen wir das folgende Hilfsmittel:

Lemma 8.4.13 (Vergleich der Kerne)**.** *Ist $B \in \mathbb{C}^{n\times n}$, so existiert $P = \sqrt{B^*B}$ und es gilt* $\ker(P) = \ker(B)$.

Beweis. Die Existenz von P folgt auf der positiven Semidefinitheit von B^*B. Nach Definition des Spektralkalküls hat P dieselben Eigenräume wie B^*B, nur die Eigenwerte sind gewurzelt. Folglich gilt $\ker(P) = \ker(B^*B)$. Ist $v \in \ker(B)$, so ist $B^*Bv = B^*0 = 0$, also $v \in \ker(B^*B) = \ker(P)$. Sei umgekehrt $v \in \ker(P) = \ker(B^*B)$. Dann gilt

$$0 = B_0(v, B^*Bv) = B_0(Bv, Bv) = \|Bv\|^2.$$

Daher gilt $Bv = 0$ und folglich $v \in \ker(B)$. □

[19.06.24]

Beweis von Satz 8.4.12. Ist B invertierbar, so folgt die Behauptung sofort aus der klassischen Polarzerlegung. Es sei $B \in \mathbb{C}^{n\times n}$ nicht invertierbar. Dann ist auch $P = \sqrt{B^*B}$ nicht invertierbar (denn $\det(P) = \sqrt{|\det(B)|}$). Es seien $\lambda_1,\dots,\lambda_k$ die von 0 verschiedenen Eigenwerte von P und $V_{\lambda_1},\dots,V_{\lambda_k}$ die zugehörigen Eigenräume; da $\ker(P)$ gerade der Eigenraum zum Eigenwert 0 ist, folgt

$$\mathbb{C}^n = \ker(P) \oplus W, \quad \text{wobei } W := V_{\lambda_1} \oplus \dots \oplus V_{\lambda_k}. \tag{8.4.3}$$

Es sei U die eindeutig bestimmte Matrix, so dass

$$Uv = \begin{cases} v, & \text{falls} \quad v \in \ker(P). \\ B\lambda_j^{-1}v, & \text{falls} \quad v \in V_{\lambda_j} \text{ für ein } j \in \{1,\dots,k\}. \end{cases}$$

Wegen $\ker(P) = \ker(B)$ gilt dann für $v \in \ker(P)$ bzw. $v \in V_{\lambda_j}$, dass

$$UPv = \left\{ \begin{array}{ll} 0, & \text{falls} \quad v \in \ker(P). \\ Bv, & \text{falls} \quad v \in V_{\lambda_j} \text{ für ein } j \in \{1,\dots,k\} \end{array} \right\} = Bv,$$

und daher $UP = B$.

Es bleibt noch zu zeigen, dass U unitär ist. Da U die orthogonale Zerlegung (8.4.3) erhält, genügt es dazu zu zeigen, dass $B_0(Uv,Uv) = 0$ ist, wenn entweder $v \in \ker(P)$ oder $v \in V_{\lambda_j}$ für ein $j \in \{1,\dots,k\}$. Ist $v \in \ker(P)$, so ist $Uv = v$, also gilt die Behauptung. Ist dagegen $v \in V_{\lambda_j}$, so ist

$$B_0(Uv,Uv) = B_0(B\lambda_j^{-1}v, B\lambda_j^{-1}v) = B_0(B^*Bv, \lambda_j^{-2}v) = B_0(P^2v, \lambda_j^2 v) = B_0(\lambda_j^2 v, \lambda_j^{-2}v) = B_0(v,v). \quad \square$$

Übung 8.4.14. Formulieren und beweisen Sie Versionen von Satz 8.4.12 mit $P = \sqrt{BB^*}$ ist.

Wir geben nun eine wichtige Anwendung der (verallgemeinerten) Polarzerlegung.

Definition 8.4.15. Ist $B \in \mathbb{C}^{n\times n}$, so heißen die Eigenwerte von $\sqrt{B^*B}$ die *Singulärwerte* von B.

Die Menge der Singulärwerte von B ist also $\{\sqrt{\lambda} \mid \lambda \in \operatorname{spec}_{\mathbb{C}}(B^*B)\} \subseteq [0,\infty)$. Da die Matrix $\sqrt{B^*B}$ normal ist, stimmen die algebraischen und geometrischen Vielfachheiten ihrer Eigenwerte überein. Man nennt diese daher kurz die *Vielfachheiten* der Singulärwerte von B.

Satz 8.4.16 (Singulärwertzerlegung)**.** *Jede Matrix $B \in \mathbb{C}^{n\times n}$ lässt sich schreiben als*

$$B = U\operatorname{diag}(\mu_1,\dots,\mu_n)U',$$

wobei U und U' unitäre Matrizen und $\mu_1,\dots,\mu_n$ die Singulärwerte von B (aufgezählt mit Vielfachheiten) sind.

Beweis. Wir starten von einer verallgemeinerten Polarzerlegung $B = U_1P$ von P mit $U_1 \in \mathrm{U}_n(\mathbb{C})$ und $P = \sqrt{B^*B}$. Da P hermitesch ist, ist P unitär diagonalisierbar, d.h. es existiert ein $U_2 \in \mathrm{U}_n(\mathbb{C})$ mit $P = U_2\operatorname{diag}(\mu_1,\dots,\mu_n)U_2^*$. Es gilt dann

$$B = U_1P = U_1U_2\operatorname{diag}(\mu_1,\dots,\mu_n)U_2^*$$

Wir können daher $U := U_1U_2$ und $U' := U_2^*$ wählen. $\square$

Korollar 8.4.17 (Singulärwerte und Skalierung)**.** *Ist $A \in \mathbb{C}^{n\times n}$ mit maximalem Singulärwert $\mu_{\max}$ und minimalem Singulärwert $\mu_{\min}$, so gilt*

$$\mu_{\min}\|v\| \le \|Av\| \le \mu_{\max}\|v\|, \tag{8.4.4}$$

wobei $\|\cdot\|$ die Norm bzgl. des Standardskalarprodukts B_0 bezeichnet.

Beweis. Es sei $A = U\operatorname{diag}(\mu_1,\dots,\mu_n)U'$ eine Singulärwertzerlegung von A. Wir setzen $w := U'v$, so dass $\|v\| = \|w\|$. Dann gilt

$$\|Av\| = \|U\operatorname{diag}(\mu_1,\dots,\mu_n)U'v\| = \|\operatorname{diag}(\mu_1,\dots,\mu_n)w\| = \sqrt{\mu_1^2|w_1|^2+\cdots+\mu_n^2|w_n|^2}.$$

Nach Definition gilt $\mu_{\max} \ge \mu_j \ge \mu_{\min}$ für alle $j \in \{1,\dots,n\}$ und daher

$$\begin{aligned}\mu_{\max}\|w\| &= \sqrt{\mu_{\max}^2|w_1|^2+\cdots+\mu_{\max}^2|w_n|^2} \ge \sqrt{\mu_1^2|w_1|^2+\cdots+\mu_n^2|w_n|^2}\\ &\ge \sqrt{\mu_{\min}^2|w_1|^2+\cdots+\mu_{\min}^2|w_n|^2} \ge \mu_{\min}\|w\|.\end{aligned}$$

Wir erhalten daher $\mu_{\max}\|w\| \ge \|Av\| \ge \mu_{\min}\|w\|$, und wegen $\|w\| = \|v\|$ folgt die Ungleichung. □

Übung 8.4.18. Zeigen Sie, dass Gleichheit in (8.4.4) genau dann gilt, wenn v ein Eigenvektor von $\sqrt{A^*A}$ zum Eigenwert $\mu_{\min}$ bzw. $\mu_{\max}$ gilt. Insbesondere gilt

$$\mu_{\min} = \max_{v\in\mathbb{C}^n\setminus\{0\}} \frac{\|Av\|}{\|v\|} = \min_{\|v\|=1}\|Av\| \quad\text{und}\quad \mu_{\max} = \max_{v\in\mathbb{C}^n\setminus\{0\}} \frac{\|Av\|}{\|v\|} = \max_{\|v\|=1}\|Av\|.$$

Bemerkung 8.4.19 (Zur Terminologie)**.** Eine weitreichende Verallgemeinerung der Singulärwertzerlegung ist die sogenannte *Cartan-Zerlegung* in der Theorie der Matrizengruppen. In vielen fortgeschrittenen Büchern wird die Singulärwertzerlegung daher auch schlicht „Cartan-Zerlegung“ genannt. In den Ingenieurwissenschaften und der Angewandten Mathematik hat sich dagegen der Name Singulärwertzerlegung (engl. „singular value decomposition“ oder kurz „SVD“) durchgesetzt.

Bemerkung 8.4.20 (Praktisches Berechnen von Singulärwerten)**.** Theoretisch ist der Beweis der Singulärwertzerlegung konstruktiv, der hier gegebene Beweis führt aber nicht auf einen besonders effizienten Algorithmus. In der Vorlesung NUMERISCHE MATHEMIATK 1 werden Sie effizientere Methoden zur Berechung von Singulärwerten (auch für nicht-quadratische Matrizen) und Singulärwertzerlegungen kennenlernen. Das praktische Berechnen einer Singulärwertzerlegung einer Matrix ist ein zentrales Problem der numerischen Linearen Algebra.

Der hier erkärte Algorithmus ist zwar weniger effizient als z.B. iterative Verfahren, aber von großem theoretischen Wert, da er sich auf allgemeinere Matrizengruppen (z.B. alle klassischen Gruppen über $\mathbb{R}$ und $\mathbb{C}$) übertragen lässt. Wir wollen daher kurz zusammenfassen, wie man mit den hier vorgestellten Methoden die Singulärwertzerlegung einer Matrix $B \in \mathbb{C}^{n\times n}$ zumindest im Prinzip bestimmen kann. Wir nehmen der Einfachheit halber an, dass U invertierbar ist.

(1) Zunächst bestimmt man die Matrix $P^2 := B^*B$.

(2) Man wendet nun den folgenden dreischrittigen Algorithmus auf P^2 an:

   (a) Man bestimmt das charakteristische Polynom und die Eigenwerte von P^2. Die Singulärwerte $\mu_1,\dots,\mu_n$ von B sind die Wurzeln dieser Eigenwerte.

(b) Für jeden Eigenwert λ von P^2 bestimmt man eine Basis des zugehörigen Eigenraums.

(c) Man wendet auf die Basis jedes Eigenraums das (beschleunigte) Gram-Schmidt-Verfahren an und erhält so eine ONB. Die Matrix, deren Spalten durch diese ONB gegeben sind, ist die Matrix U_2.

(3) Es gilt nun $P = U_2 \mathrm{diag}(\mu_1, \ldots, \mu_n) U_2^*$.

(4) Die Matrizen U und U' sind gegeben durch $U' := U_2^*$ und

$$U := U_1 U_2 = (BP^{-1}) U_2 = B(U_2 \mathrm{diag}(\mu_1, \ldots, \mu_n) U_2^*)^{-1} U_2 = B U_2 \mathrm{diag}(\mu_1, \ldots, \mu_n)^{-1}.$$

Ist B nicht-invertierbar, so wird das Verfahren noch etwas hässlicher, da man statt der Polarzerlegung die singuläre Polarzerlegung verwenden muss.

Beispiel 8.4.21 (Eine Singulärwertzerlegung)**.** Wir betrachten die Matrix

$$B := \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \text{so dass} \quad P^2 := B^\top B = \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix}.$$

Das charakteristische Polynom dieser Matrix ist gegeben durch

$$\chi_{P^2}(X) = \det \begin{pmatrix} X-5 & -4 \\ -4 & X-5 \end{pmatrix} = (X-5)(X-5) - 16 = X^2 - 10X + 9 = (X-1)(X-9).$$

Der Eigenraum zum Eigenwert $\lambda_1 = 1$ ist der Kern der Matrix

$$V_{\lambda_1} = \ker \begin{pmatrix} -4 & -4 \\ -4 & -4 \end{pmatrix} = \ker \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \mathbb{C} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Der Eigenraum zum Eigenwert $\lambda_2 = 9$ ist

$$V_{\lambda_2} = \ker \begin{pmatrix} 4 & -4 \\ -4 & 4 \end{pmatrix} = \ker \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix} = \mathbb{C} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Beide Vektoren haben Länge $\sqrt{2}$, und wir erhalten

$$P^2 = U_2 \cdot \mathrm{diag}(1,9) \cdot U_2^*, \quad \text{wobei} \quad U_2 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

An dieser Stelle haben wir übrigens die Polarzerlegung von B berechnet: Es gilt

$$P = U_2 \cdot \mathrm{diag}(1,3) \cdot U_2^* = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{und} \quad U_1 := BP^{-1} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \frac{1}{3} \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In der Tat sieht man leicht, dass P positiv definit und U_1 unitär ist, und folglich ist $B = U_1 P$ die Polarzerlegung von B.

Kehren wir nun zur Berechnung der Singulärwertzerlegung zurück: Die Singulärwerte sind die Wurzeln der Eigenwerte von P^2, also $\mu_1 = 1$ und $\mu_2 = 3$. Es ist also

$$U' := U_2^* = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{und} \quad U := B U_2 \mathrm{diag}(1, 1/3) = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$

Eine mögliche Singulärwertzerlegung von B ist daher

$$B = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}\cdot \operatorname{diag}(1,3)\cdot \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}.$$

Für einen beliebigen Vektor $v \in \mathbb{C}^2$ gilt insbesondere

$$\|v\| \le \|Bv\| \le 3\|v\|.$$

Diese Schranken sind scharf, denn es gilt

$$B\begin{pmatrix}-1\\ 1\end{pmatrix} = \begin{pmatrix}1\\ -1\end{pmatrix} \quad \text{und} \quad B\begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}3\\ 3\end{pmatrix}$$

Bemerkung 8.4.22. In Übung 8.4.18 haben wir gesehen, dass für jede Matrix A das Maximum

$$\|A\|_{\mathrm{op}} := \max_{v\in\mathbb{C}^n\setminus\{0\}} \frac{\|Av\|}{\|v\|} = \max_{\|v\|=1} \|Av\| \tag{8.4.5}$$

existiert. Dieses Maximum hat eine Reihe interessanter Eigenschaften. Zunächst einmal gilt nach Definition, dass

$$\|Av\| \le \|A\|_{\mathrm{op}}\|v\| \quad \text{für alle } v \in \mathbb{C}^n. \tag{8.4.6}$$

Weiterhin gilt nach Übung 8.4.18, dass (in der Notation von Korollar 8.4.17)

$$\|A\|_{\mathrm{op}} = \mu_{\max} \tag{8.4.7}$$

der maximale Singulärwert von A ist.

Proposition 8.4.23. *Durch* (8.4.5) *wir eine Norm* $\|-\|_{\mathrm{op}}$ *auf dem Vektorraum* $\mathbb{C}^{n\times n}$ *definiert, und diese Norm ist submultiplikativ, d.h.*

$$\|AB\|_{\mathrm{op}} \le \|A\|_{\mathrm{op}}\|B\|_{\mathrm{op}}.$$

Beweis. Wir rechnen die drei definierende Eigenschaften einer Norm (vgl. Bemerkung 7.1.8) nach. Seien also $A, B \in \mathbb{C}^{n\times n}$ und $\lambda \in \mathbb{C}$.

(N1) Aus $\|A\|_{\mathrm{op}} = 0$ folgt wegen (8.4.6), dass $\|Av\| \le 0\|v\| = 0$ für alle $v \in \mathbb{C}^n$ gilt. Dann ist aber $Av = 0$ für alle $v \in \mathbb{C}^n$ und daher $A = 0$.

(N2) Es gilt

$$\|\lambda A\|_{\mathrm{op}} = \max_{\|v\|=1} \|(\lambda A)v\| = \max_{\|v\|=1} |\lambda|\|Av\| = |\lambda| \max_{\|v\|=1} \|Av\| = |\lambda|\|A\|_{\mathrm{op}}.$$

$$\|\lambda\Phi(v)$$

(N3) Für $v \in \mathbb{C}^n$ mit $\|v\| = 1$ gilt

$$\|(\Phi+\Psi)(v)\| = \|\Phi(v)+\Psi(v)\| \le \|\Phi(v)\| + \|\Psi(v)\| \le \|\Phi\|_{\mathrm{op}} + \|\Psi\|_{\mathrm{op}},$$

also folgt $\|\Phi+\Psi\|_{\mathrm{op}} = \sup_{\|v\|=1} \|(\Phi+\Psi)(v)\| \le \|\Phi\|_{\mathrm{op}} + \|\Psi\|_{\mathrm{op}}$.

Damit ist $\| - \|_{\mathrm{op}}$ eine Norm. Ist $v \in \mathbb{C}^n$ so gilt wegen (8.4.6), dass

$$\|ABv\| \leq \|A\|_{\mathrm{op}}\|Bv\| \leq \|A\|_{\mathrm{op}}\|B\|_{\mathrm{op}}\|v\|,$$

und geht man zum Maximum über alle v mit $\|v\| = 1$ über, so folgt, dass $\|AB\|_{\mathrm{op}} \leq \|A\|_{\mathrm{op}}\|B\|_{\mathrm{op}}$. □

Definition 8.4.24. Die Norm $\| - \|_{\mathrm{op}}$ heißt die *Operatornorm* auf $\mathbb{C}^{n\times n}$.

Bemerkung 8.4.25 (Matrizennormen)**.** Auf dem Vektorraum $\mathbb{C}^{n\times n}$ gibt es viele verschiedene Normen. Beispielsweise können wir $\mathbb{C}^{n\times n}$ mit $\mathbb{C}^{n^2}$ identifizieren und auf letzterem eine der aus der Analysis geläufigen ℓ^p-Normen verwenden. Für die ℓ^2-Norm bzw. ℓ^∞-Norm ergeben sich

$$\|A\|^2 = \left(\sum_{i=1}^{n}\sum_{j=1}^{n}|a_{ij}|^2\right)^{\frac{1}{2}} = \mathrm{tr}(AA^*)^{\frac{1}{2}} = \mathrm{tr}(A^*A)^{\frac{1}{2}} \quad \text{und} \quad \|A\|_\infty = \max|a_{ij}| = \max_{i,j\in\{1,\dots,n\}}|e_i^\top A\overline{e_j}|.$$

In der ANALYSIS 2 zeigt man, dass alle Normen auf $\mathbb{C}^{n\times n}$ (insbesondere auch die Operatornorm) Lipschitz-äquivalent sind: Sind Sind $\|\cdot\|$ und $\|\cdot\|'$ zwei beliebige Normen, so existiert $C > 0$, so dass

$$\frac{1}{C}\cdot\|v\| \leq \|v\|' \leq C\cdot\|v\|.$$

Für Konvergenzfragen spielt es daher keine Rolle, welche Norm wir auf dem Vektorraum der Matrizen verwenden. Aus Sicht der Algebra bietet aber eine submultiplikative Norm zahlreiche Vorteile.

Proposition 8.4.26 (Invarianzeigenschaften der Operatornorm)**.** *Sei $A \in \mathbb{C}^{n\times n}$ und $U \in \mathrm{U}_n(\mathbb{C})$. Dann gilt*

$$\|AU\|_{\mathrm{op}} = \|UA\|_{\mathrm{op}} = \|A\|_{\mathrm{op}}.$$

Insbesondere haben unitär ähnliche Matrizen dieselbe Operatornorm.

Beweis. Die zweite Gleichheit folgt sofort aus $\|UAv\| = \|Av\|$ und Übergang zum Maximum über alle $v \in \mathbb{C}^n$ mit $\|v\| = 1$. Ist $v \in \mathbb{C}^n$, so gilt genau dann $\|v\| = 1$, wenn $\|Uv\| = 1$, und daher

$$\|AU\|_{\mathrm{op}} = \sup_{\|v\|=1}\|AUv\| = \sup_{\|Uv\|=1}\|AUv\| = \sup_{\|w\|=1}\|Aw\| = \|A\|_{\mathrm{op}}.$$ □

Korollar 8.4.27 (Operatornorm normaler Matrizen)**.** *Ist $A \in \mathbb{C}^{n\times n}$ normal, so gilt*

$$\|A\|_{\mathrm{op}} = \rho(A) := \sup\{|\lambda| \mid \lambda \in \mathrm{spec}_{\mathbb{C}}(A)\}.$$

Beweis. Nach dem Spektralsatz ist A unitär ähnlich zu einer Diagonalmatrix $D = \mathrm{diag}(\lambda_1,\dots,\lambda_n)$. Dann besitzen A und D sowohl dieselben Eigenvektoren (da sie ähnlich sind), als auch dieselbe Operatornorm (nach Proposition 8.4.26). Wir dürfen daher annehmen, dass $A = D$ gilt. Die Singulärwerte einer Diagonalmatrix sind aber genau die Absolutbeträge der Eigenwerte, denn

$$DD^* = \mathrm{diag}(|\lambda_1|^2,\dots,|\lambda_2|^2) \implies \sqrt{DD^*} = \mathrm{diag}(|\lambda_1|,\dots,|\lambda_2|).$$

Der größte Singulärwert von D ist daher genau $\rho(D)$. □

Definition 8.4.28. Für $A \in \mathbb{C}^{n\times n}$ heißt $\rho(A) := \sup\{|\lambda| \mid \lambda \in \mathrm{spec}_{\mathbb{C}}(A)\}$ der Spektralradius von A.

Bemerkung 8.4.29 (Operatornorm vs. Spektralradius)**.** Wie hängen der Spektralradius und die Operatornorm einer Matrix $A \in \mathbb{C}^{n\times n}$ zusammen?

Ist v ein Eigenvektor von A mit $\|v\| = 1$ und Eigenwert λ, so gilt $\|Av\| = \|\lambda v\| = |\lambda|\|v\| = |\lambda|$ und daher $|\lambda| \le \|A\|_{\mathrm{op}}$. Zusammen mit (8.4.7) folgt daher, dass

$$\rho(A) \le \|A\|_{\mathrm{op}} = \rho(\sqrt{A^*A}) = \sqrt{\rho(A^*A)}. \tag{8.4.8}$$

Für normale Matrizen gilt nach Korollar 8.4.27 sogar Gleichheit, also gilt insbesondere

$$\|A^*A\|_{\mathrm{op}} = \rho(A^*A) = \|A\|_{\mathrm{op}}^2. \tag{8.4.9}$$

Man könnte vielleicht auf die Idee kommen, dass die Operatornorm immer mit dem Spektralradius übereinstimmt. Das ist auf den ersten Blick gar nicht unplausibel: Die Beträge der Eigenwerte sagen ja, wie stark gewisse Vektoren (die Eigenvektoren) gestreckt oder gestaucht werden. Es ist aber leider falsch:

Ist z.B. A nilpotent, so ist $\mathrm{spec}_{\mathbb{C}}(A) = \{0\}$ und daher $\rho(A) = 0$. Andererseits gilt aber $\|A\|_{\mathrm{op}} = 0$ nur, wenn $A = 0$. Für eine von 0 verschiedene nilpotente Matrix gilt daher $\rho(A) < \|A\|_{\mathrm{op}}$. Man kann dies in konkreten Beispielen nachrechnen: Für alle $R > 0$ gilt

$$A := \begin{pmatrix} 0 & R \\ 0 & 0 \end{pmatrix} \Longrightarrow A^*A = \begin{pmatrix} 0 & 0 \\ 0 & R^2 \end{pmatrix} \Longrightarrow \mathrm{spec}(A^*A) = \{0, R^2\} \Longrightarrow \|A\|_{\mathrm{op}} = \sqrt{R^2} = R > \rho(A) = 0,$$

also lässt sich $\|A\|_{\mathrm{op}}$ nicht durch $\rho(A)$ beschränken. Was passiert hier qualitativ? Der Eigenvektor e_1 wird auf $0 \cdot e_1$ abgebildet, aber der Vektor e_2, der kein Eigenvektor ist, wird auf eine Vektor derselben Länge (nämlich e_1) geschickt. Die Operatornorm sieht das, aber der Spektralradius sieht nur, um welche Faktoren Eigenvektoren gestreckt werden; der Vektor e_2 bleibt daher für ihn unsichtbar.

Konstruktion 8.4.30 (Approximation mittels Singulärwertzerlegung)**.** Es sei $M \in \mathbb{C}^{n\times n}$ eine Matrix. Wir ordnen die Singulärwerte von B so, dass $\mu_1 \ge \mu_2 \ge \cdots \ge \mu_n$. Es sei nun $\varepsilon \in (\mu_1, \mu_n)$ vorgegeben, und es gelte

$$\mu_1 \ge \cdots \ge \mu_k > \varepsilon \ge \mu_{k+1} \ge \cdots \ge \mu_n. \tag{8.4.10}$$

Wir berechnen nun eine Singulärwertzerlegung der Form

$$M = U\,\mathrm{diag}(\mu_1, \ldots, \mu_n)U'$$

mit $U, U' \in U_n(\mathbb{C})$ und definieren

$$M_\varepsilon := U\,\mathrm{diag}(\mu_1, \ldots, \mu_k, 0, \ldots, 0)U'$$

Diese Matrix ist dann von der Form

$$M_\varepsilon = \begin{pmatrix} A & B \\ C & 0 \end{pmatrix} \quad \text{mit } A \in \mathbb{C}^{k\times k}, B \in \mathbb{C}^{k\times(n-k)}, C \in \mathbb{C}^{(n-k)\times k}$$

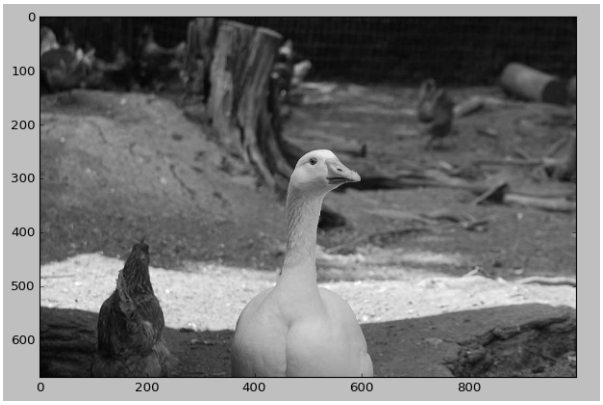
und hat daher k^2 Einträge, die gleich 0 sind. Sie verbraucht daher weniger Speicherplatz als M. Andererseits gilt

$$\|M - M_\varepsilon\|_{\mathrm{op}} = \|U\,\mathrm{diag}(0, \ldots, 0, \mu_{k+1}, \ldots, \mu_n)U'\|_{\mathrm{op}} = \mu_{k+1} \le \varepsilon.$$

Die Matrix M_ε ist daher für kleine Werte von ε eine gute Näherung von M (in der Operatornorm, aber wegen der Äquivalenz der Normen dann auch in der ℓ^∞-Norm, d.h. alle Einträge von M_ε sind nah an den entsprechenden Einträgen von M), die weniger Speicherplatz frisst. Der Gewinn ist besonders dann groß, wenn nur einige wenige wenige Singulärwerte groß und alle anderen sehr klein sind. Man behält dann die großen Singulärwerte, und schmeisst die kleinen weg.

Bemerkung 8.4.31 (Bildkompression)**.** Typische Anwendungsbeispiele der Methode aus Konstruktion 8.4.30 betreffen die Bild- und Tonkompression. Nehmen wir an, sie wollen ein Bild der Auflösung[4] 1024×1024 in ihrem Rechner speichern. Für jeden der über eine Million Pixel müssen Sie dann eine Zahl speichern, die die Farbe des entsprechenden Pixels kodiert. Die entsprechende (1024×1024)-Matrix wird voll besetzt sein. Nun sind aber die Pixel in einem Bild nicht zufällig verteilt, sondern es gibt meist klare Linien, sowie dunklere und hellere Stellen. Es hat sich herausgestellt, dass in solchen Fällen häufig einige wenige Singulärwerte dominant und alle anderen verschwindend klein sind. Dies ist eine rein empirische Beobachtung - man kann künstlich Bilder konstruieren, wo dies nicht der Fall ist, aber in der Realität treten diese anscheinend nicht so häufig auf. Warum genau, ist (mir) unklar.

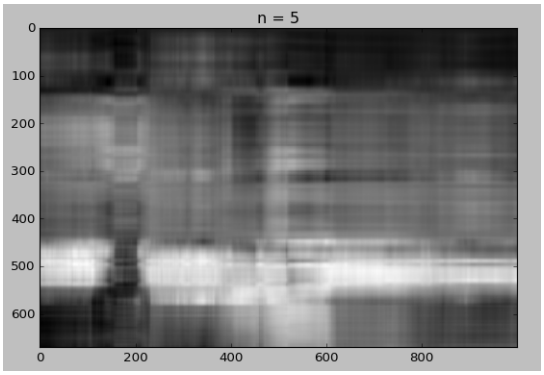
Ein wunderbares Beispiel habe ich auf der folgenden Website gefunden:
`https://hadrienj.github.io/posts/Deep-Learning-Book-Series-2.8-Singular-Value-Decomposition/`

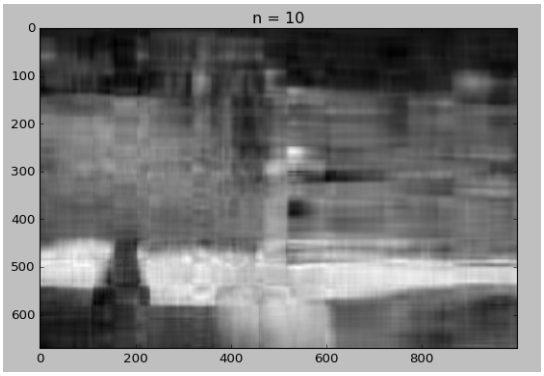


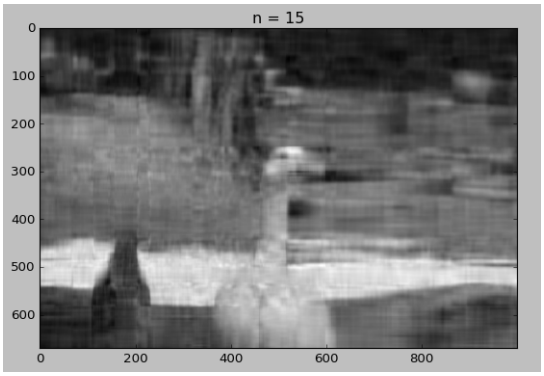
Dort ist das obige Bild von Lucy der Gans[5] mit einer Auflösung von 669×1000 Pixeln gegeben. Eine solche Matrix hat 669 Singulärwerte. Was glauben Sie, wieviele dieser 669 Singulärwerte man für eine Approximation benötigt, in der man Lucy klar erkennen kann? 10? 50? 100? 500? Schätzen Sie, und blättern Sie dann um. Auf der nächsten Seite sehen Sie verschiedene Approximationen. Die Zahl n im jeweiligen Header des Bilds ist die Anzahl der verwendeten Singulärwerte (von 669).

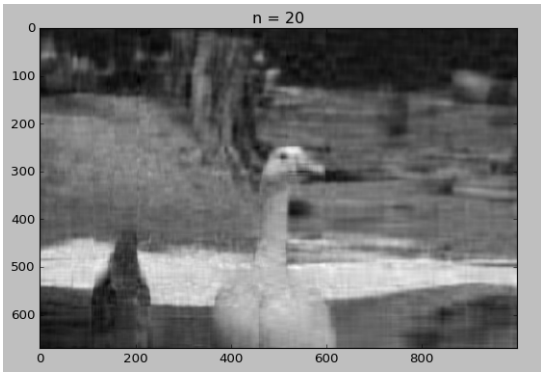
[4] Singulärwertzerlegungen gibt es auch für rechteckige Matrizen, aber um die Präsentation zu vereinfachen, seien alle unsere Bilder quadratisch.

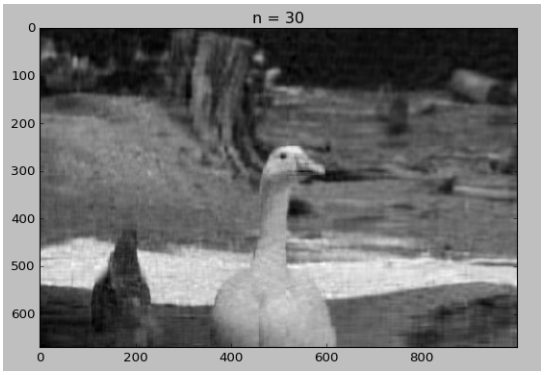
[5] Der Name der Henne ist nicht überliefert...

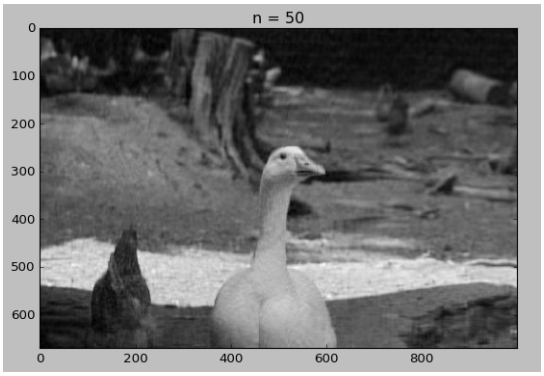

n = 5
0
100
200
300
400
500
600
0
200
400
600
800


n = 10
0
100
200
300
400
500
600
0
200
400
600
800


n = 15
0
100
200
300
400
500
600
0
200
400
600
800


n = 20
0
100
200
300
400
500
600
0
200
400
600
800





Zusammenfassung von Abschnitt 8.4.

(1) Jede komplexe quadratische Matrix zerlegt sich eindeutig als Produkt einer unitären und einer positiv-definiten hermiteschen Matrix (*Polarzerlegung*).

(2) Jede komplexe quadratische Matrix entsteht aus einer bis auf Reihenfolge der Einträge eindeutigen Diagonalmatrix mit nicht-negativen reellen Einträgen durch Multiplikation von links und rechts mit unitären Matrizen. Die Diagonaleinträge heißen die *Singulärwerte* der Matrix.

(3) Die Länge eines Vektors verändert sich nach Multiplikation mit einer Matrix mindestens durch Multiplikation mit dem kleinsten Singulärwert und höchstens durch Multiplikation mit dem größten Singulärwert.

(4) Der größte Singulärwert definiert auf der Algebra der komplexen Matrizen eine submultiplikative Norm, genannt die *Operatornorm*. Für normale Matrizen stimmt diese mit dem Spektralradius überein, im allgemeinen ist die Operatornorm von A durch den Spektralradius von $\sqrt{A^*A}$ gegeben.

(5) Man kann eine Matrix approximieren, indem man eine Singulärwertzerlegung durchführt und kleine Singulärwerte zu 0 setzt. Dies wird u.a. in der Bildkompression eingesetzt, um Speicherplatz zu sparen.

9 Affine Quadriken

[21.06.24]

9.1 Quadriken und Hauptachsentransformation

Quadriken sind Nullstellenmengen von quadratischen Polynomen in mehreren Veränderlichen. Wir überlegen uns zuerst, was das bedeutet.

Bemerkung 9.1.1 (Polynome in mehreren Veränderlichen)**.** Für einen beliebigen Integritätsbereich R haben wir in Proposition 5.4.9 gesehen, dass der Polynomring $R[X]$ über R in einer Unbestimmten wieder ein Integritätsbereich ist. Wir können daher den Polynomring $R[X,Y] := R[X][Y]$ über $R[X]$ in einer weiteren Unbestimmten Y bilden. Elemente von $R[X,Y]$ sind formale Ausdrücke der Form

$$p = \sum_{i=0}^{k} \sum_{j=0}^{l} a_{ij} X^i Y^j \quad \text{mit } a_{ij} \in R \text{ für } i \in \{0,\dots,k\}, j \in \{0,\dots,l\},$$

die wir auch als *(formale) Polynome in zwei Veränderlichen über R* bezeichnen, und zwei solche formalen Polynome stimmen nach Definition genau dann überein, wenn sie dieselben von 0 verschiedenen Koeffiziente a_{ij} besitzen.

Induktiv definieren wir nun den Ring der *(formalen) Polynome in n Veränderlichen* über R als $R[X_1,\dots,X_n] := R[X_1,\dots,X_{n-1}][X_n]$. Seine Elemente sind formale Ausdrücke der Form

$$p = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n} \quad \text{mit } a_{i_1,\dots,i_n} \in R \text{ für } j \in \{1,\dots,n\}, i_j \in \{0,\dots,k_n\}. \tag{9.1.1}$$

Ist $p \in R[X_1,\dots,X_n]$ das formale Polynom, das durch die Formel (9.1.1) gegeben ist, so heißt die Funktion

$$p_R : R^n \to R, \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto p(x) := \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

die zugehörige Polynomfunktion. Bereits im Fall von einer Veränderlichen haben wir gesehen, dass verschiedene Polynome dieselbe Polynomfunktion definieren können. Es ist daher im Allgemeinen wichtig, zwischen Polynomen und Polynomfunktionen zu unterscheiden.

Wir werden im Folgenden nur Polynome in mehreren Veränderlichen über einem Körper $\mathbb{K}$ betrachten.

Bemerkung 9.1.2 (Totaler Grad von Polynomen)**.** Ein Polynom $q \in \mathbb{K}[X_1,\dots,X_n]$ der Form

$$q = X_1^{i_1} \cdots X_n^{i_n} \quad \text{mit } i_1,\dots,i_n \in \mathbb{N}_0$$

heißt ein *Monom* vom *totalen Grad* $i_1 + \cdots + i_n$. Jedes Polynom $p \in \mathbb{K}[X_1, \ldots, X_n] \setminus \{0\}$ ist eine Linearkombination mit Koeffizienten in $\mathbb{K} \setminus \{0\}$ von Monomen. Man nennt dann den maximalen totalen Grad dieser Monome den *totalen Grad* von p, geschrieben $\deg(p)$. Besitzen alle Monome denselben totalen Grad, so nennt man das Polynom *homogen*. Nach Definition ist also ein Polynom vom Grad d eine Summe von homogenen Polynomen von Graden $\leq d$. Beispielsweise ist

$$X_1^2X_2 + X_1X_2 + X_2^2 + 3 = (X_1^2X_2) + (X_1X_2 + X_2^2) + 3$$

ein Polynom vom totalen Grad 3 (nämlich die Summe von 4 Mononmen), geschrieben als die Summe von drei homogenen Polynomen der totalen Grade 3, 2 und 0.

Wie im Fall von einer Variablen setzen wir noch $\deg(0) := -\infty$.

Definition 9.1.3. Ist $p \in \mathbb{K}[X_1, \ldots, X_n]$, so heißt

$$V(p) := \{x \in \mathbb{K}^n \mid p(x) = 0\} \subseteq \mathbb{K}^n$$

die *Nullstellenmenge* von p. Sind $p_1, \ldots, p_k \in \mathbb{K}[X_1, \ldots, X_n]$, so heißt

$$V(p_1, \ldots, p_n) := V(p_1) \cap V(p_2) \cap \cdots \cap V(p_n) \subseteq \mathbb{K}^n$$

eine *affine algebraische Menge*.

Man beachte, dass die Nullstellenmenge eines Polynoms p nur von der Polynomfunktion $p_{\mathbb{K}}$ abhängt. Das Studium affiner algebraischer Mengen ist ein klassisches Teilgebiet der Geometrie, die sogenannte (AFFINE) ALGEBRAISCHE GEOMETRIE.

Bemerkung 9.1.4. Ist $n = 1$, so ist jede Nullstellenmenge eines Polynoms $p \in \mathbb{K}[X]$ – und daher jede affine algebraische Menge $V \subseteq \mathbb{K}^1$ – endlich. Umgekehrt ist jede endliche Menge $V \subseteq \mathbb{K}^1$ mit $|V| = n$ die Nullstellenmenge eines Polynoms vom Grad n. Um interessante Nullstellenmengen zu bekommen, sollte man daher Polynome von mindestens zwei Veränderlichen betrachten.

Beispiel 9.1.5 (Polynome vom Grad ≤ 1 und ihre Nullstellen)**.** (i) Das Nullpolynom ist das einzige Polynom in $\mathbb{K}[X_1, \ldots, X_n]$ vom Grad $-\infty$, und seine Nullstellenmenge ist $V(0) = \mathbb{K}^n$.

(ii) Polynome $p \in \mathbb{K}[X_1, \ldots, X_n]$ vom Grad 0 sind von der Form $p = \lambda$ für ein $\lambda \in \mathbb{K}^\times$, und ihre Nullstellenmenge ist leer.

(iii) Homogene Polynome vom Grad 1 sind von der der Form $p = a_1X_1 + \cdots + a_nX_n$ mit $a_1, \ldots, a_n \in \mathbb{K}$, wobei mindestens ein Koeffizient a_j von 0 verschieden ist. Allgemeine Polynome vom Grad 1 sind daher von der Form $p = a_1X_1 + \cdots + a_nX_n + b$. Affine algebraische Mengen von Familien von Polynomfunktionen vom Grad ≤ 1 sind daher genau die Lösungsmengen linearer Gleichungssysteme, also entweder leer oder affine Unterräume des $\mathbb{K}^n$, und ihr Studium war das zentrale Thema der LINEAREN ALGEBRA I.

In der Linearen Algebra II wollen wir nun den Grad ein wenig erhöhen:

Definition 9.1.6. Eine *affine Quadrik* in $\mathbb{K}^n$ ist die Nullstellenmenge eines Polynoms $p \in \mathbb{K}[X_1, \ldots, X_n]$ vom Grad 2.

Beispiel 9.1.7 (Einige affine Quadriken in $\mathbb{R}^2$)**.** Wir geben einige erste Beispiele für affine Quadriken in $\mathbb{R}^2$:

(i) Die affine Quadrik $\{x \in \mathbb{R}^2 \mid x_1^2 + x_2^2 - 1 = 0\}$ ist der *Einheitskreis*.

(ii) Die affine Quadrik $\{x \in \mathbb{R}^2 \mid (x_1/a_1)^2 + (x_2/a_2)^2 - 1 = 0\}$ ist für beliebige $a_1, a_2 \in \mathbb{R}^\times$ eine *Standardellipse* .

(iii) Die affine Quadrik $\{x \in \mathbb{R}^2 \mid (x_1/a_1)^2 - (x_2/a_2)^2 - 1 = 0\}$ ist für beliebige $a_1, a_2 \in \mathbb{R}^\times$ eine *Standardhyperbel* .

(iv) Die affine Quadrik $\{x \in \mathbb{R}^2 \mid \{(x_1/a_1)^2 - x_2 = 0\}$ ist für beliebiges $a_1 \in \mathbb{R}^\times$ eine *Parabel*.

Beispiel 9.1.8 (Pseudosphären als Quadriken)**.** Ist B eine nicht-ausgeartete symmetrische Bilinearform auf $\mathbb{K}^n$, so ist $(\mathbb{K}^n, B)$ ein orthogonaler Vektorraum, und die zugehörigen Pseuodsphären sind Quadriken, da sie durch die quadratischen Gleichungen $B(x,x) = R$ für ein festes $R \in \mathbb{K}$ definiert sind. Das Studium der Quadriken schließt also insbesondere das Studium der Pseudosphären in orthogonalen Vektorräumen als Spezialfall ein.

Bemerkung 9.1.9 (Nullstellenmenge vs. Polynom)**.** Es ist eine interessante Frage, inwieweit die Nullstellenmenge $V(p)$ eines Polynoms p dieses bereits eindeutig bestimmt. Natürlich gilt stets $V(\lambda p^r) = V(p)$ für alle $\lambda \in \mathbb{K}^\times$ und $r \in \mathbb{N}$, und daher ist p durch $V(p)$ nicht eindeutig bestimmt. Über einem endlichen Körper passieren aber noch viel schlimmere Dinge: Hier definieren ja u.U. völlig verschiedene Polynome dieselbe Polynomfunktion, und haben daher dieselbe Nullstellemenge. Probleme treten aber auch schon über den reellen Zahlen auf: Es gilt ja $V(X_1^2 + 1) = \emptyset = V(X_2^2 + 1)$.

Mit all diesen Probleme beschäftigt sich die algebraische Geometrie. Wir zitieren hier einige Resultate, die sie in der Vorlesung ALGEBRA lernen können. Über einem algebraisch abgeschlossenen Körper (z.B. $\mathbb{K} = \mathbb{C}$) gilt stets $V(p) \subsetneq \mathbb{K}^n$ für jedes $p \in \mathbb{K}[X_1, \ldots, X_n] \setminus \{0\}$. Ist weiter $V(p) = V(q)$ mit p und q von minimal möglichem Grad[1], so gilt $q = \lambda p$ für ein $\lambda \in \mathbb{K}^\times$. Insbesondere folgt aus $\deg(p) > 1$, dass $V(p) \neq \emptyset$. Eine allgemeinere Aussage für mehrere Polynome ist der *Hilbertsche Nullstellensatz*, einer der zentralen Aussagen der kommutativen Algebra.

Über $\mathbb{K} = \mathbb{R}$ gilt des Hilbertsche Nullstellensatz nicht, denn die Polynome $X_1^2 + 1$ und $X_2^2 + 1$ haben dieselben reellen Nullstellenmenge. Sie haben aber verschiedene *komplexe* Nullstellenmengen.

Allgemein gilt: Ist $\mathbb{L}$ eine Körperweiterung von $\mathbb{K}$, so können wir für $p \in \mathbb{K}[X_1, \ldots, X_n]$ die Nullstellenmengen

$$V(p) \subseteq \mathbb{K}^n \quad \text{und} \quad V_{\mathbb{L}}(p) := \{x \in \mathbb{L}^n \mid p(x) = 0\}$$

betrachten. Ist $\mathbb{L}$ algebraisch abgeschlossen und p von minimalem Grad für $V_{\mathbb{L}}(p)$, so legt letztere Menge das Polynom bis auf Vielfache fest. Man beachte, dass

$$V_{\mathbb{L}}(p) = V_{\mathbb{L}}(q) \implies V(p) = V(q).$$

Ab jetzt sei $\mathbb{K}$ ein Körper der Charakteristik $\neq 2$.

Bemerkung 9.1.10 (Beschreibung quadratischer Polynome durch Matrizen)**.** Es sei $p \in \mathbb{K}[X_1, \ldots, X_n]$ homogen vom totalen Grad 2. Dann ist

$$p = \sum_{i=1}^{n} \alpha_i X_i^2 + \sum_{1 \leq i < j \leq n} \beta_{ij} X_i X_j \quad \text{mit } \alpha_i, \beta_{ij} \in \mathbb{K}$$

[1] Diese Annahme schließt den Fall $p = q^r$ mit $r > 1$ aus.

Da die Charakteristik von $\mathbb{K}$ nicht 2 ist, können wir eine symmetrische Matrix $B = (b_{ij}) \in \mathbb{K}^{n\times n}$ definieren durch

$$b_{ij} := \begin{cases} \alpha_i, & \text{falls } i = j \\ \beta_{ij}/2, & \text{falls } i < j \\ \beta_{ji}/2, & \text{falls } i > j \end{cases}$$

Nach Definition gilt dann

$$p(x) = x^\top Bx, \quad x \in \mathbb{K}^n.$$

Ist allgemeiner $p \in \mathbb{K}[X_1,\dots,X_n]$ ein beliebige Polynom vom Grad 2, so können wir p als Summe homogener Polynome vom Grad ≤ 2 schreiben. Es existieren daher $B \in \mathbb{K}^{n\times n}$, $b \in \mathbb{K}^n$ und $c \in \mathbb{K}$ mit

$$p(x) = x^\top Bx + 2b^\top x + c.$$

Mit dem Faktor 2 hat es die folgende Bewandnis: Definieren wir die *erweiterte Matrix* von p durch

$$B' := \begin{pmatrix} B & b \\ b^\top & c \end{pmatrix}, \tag{9.1.2}$$

und definieren für $x \in \mathbb{K}^n$ den *erweiterten Vektor* x' durch $x' := (x_1,\dots,x_n,1)$, so gilt

$$p(x) = (x')^\top B'x'.$$

Bezeichnet $\mathrm{Sym}_n(\mathbb{K}) \subseteq \mathbb{K}^{n\times n}$ die Menge der symmetrischen Matrizen und $\mathbb{K}[X_1,\dots,X_n]_{\le 2}$ die Menge der Polynome vom Grad ≤ 2, so erhalten wir also eine Bijektion

$$p : \mathrm{Sym}_{n+1}(\mathbb{K}) \to \mathbb{K}[X_1,\dots,X_n]_{\le 2}, \quad p(B')(x) = (x')^\top B'x'.$$

Statt $V(p(B'))$ (bzw. $V_{\mathbb{L}}(p(B'))$) schreiben wir im Folgenden auch kurz $Q(B')$ (bzw. $Q_{\mathbb{L}}(B')$) und nennen diese Menge die *Quadrik zur Matrix* B' (über $\mathbb{L}$). Statt $p(B')$ bzw. $Q(B')$ schreiben wir manchmal auch $p(B,b,c)$ bzw. $Q(B,b,c)$.

Beispiel 9.1.11. Ist $p(X) = X_1^2 + X_1X_2 + 3X_2^2 + X_1 + 2X_2 + 3 \in \mathbb{K}[X_1,X_2]$, so ist $p = p(B')$ mit

$$B' := \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 3 & 1 \\ \frac{1}{2} & 1 & 3 \end{pmatrix}$$

Wichtig: Die Koeffizienten außerhalb der Hauptdiagonalen müssen halbiert werden!

Bemerkung 9.1.12 (Verkettung mit affinen Abbildungen)**.** Wir erinnern daran, dass eine *affine Abbildung* von $\mathbb{K}^n$ eine Abbildung der Form

$$\Phi : \mathbb{K}^n \to \mathbb{K}^n, \quad x \mapsto Ax + v \quad \text{mit } A \in \mathbb{K}^{n\times n}, v \in \mathbb{K}^n$$

ist, und dass diese genau dann invertierbar ist, wenn A invertierbar ist. Wir schreiben in Folgenden $\mathrm{Aff}(\mathbb{K}^n)$ für die *Gruppe der affinen Bewegungen*, also die Gruppe der invertierbaren affinen Abbildungen.

Affine Abbildungen lassen sich in erweiterten Koordinaten besonders gut beschreiben: Definieren wir wie zuvor $x' := (x_1,\dots,x_n,1)^\top$, so gilt

$$\Phi(x)' = A'x' \quad \text{mit} \quad A' = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}.$$

Man nennt dann A' auch eine *affine Matrix* mit *Kernmatrix* A und *Verschiebungsvektor* v und schreibt dann auch $\Phi_{A'}$ oder $\Phi_{A,v}$ für Φ.

Es sei nun $p = p(B') \in \mathbb{K}[X_1,\dots,X_n]_{\leq 2}$. Für alle $x \in \mathbb{K}^n$ gilt dann

$$(p(B') \circ \Phi_{A'})(x) = (\Phi_{A'}(x'))^\top B' \Phi_{A'}(x)' = (A'x')^\top B'(A'x') = (x')^\top (A')^\top B' A' x' = p((A')^\top B' A')(x),$$

und daher

$$p(B') \circ \Phi_{A'} = p((A')^\top B' A'). \tag{9.1.3}$$

Schreibt man B' wie in (9.1.2), so kann man dies noch weiter ausschreiben. Es gilt dann

$$(A')^\top B' A' = \begin{pmatrix} A^\top & 0 \\ v^\top & 1 \end{pmatrix} \cdot \begin{pmatrix} B & b \\ b^\top & c \end{pmatrix} \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A^\top BA & A^\top Bv + A^\top b \\ (A^\top Bv + A^\top b)^\top & v^\top Bv + b^\top v + c \end{pmatrix},$$

und daher

$$p(B,b,c) \circ \Phi_{A,v} = p(A^\top BA, A^\top Bv + A^\top b, v^\top Bv + b^\top v + c). \tag{9.1.4}$$

Ist hierbei A zusätzlich orthogonal (wie etwa im Fall einer euklidischen Bewegung), so sind B und $A^\top BA$ orthogonal ähnlich und haben daher dieselben Eigenwerte. Zwei Spezialfälle von (9.1.4) sind besonders interessant: Ist $\Phi_{A'}$ linear (d.h. $v = 0$), so vereinfacht sich (9.1.4) zu

$$p(B,b,c)(Ax) = p(A^\top BA, A^\top b, c)(x) \tag{9.1.5}$$

Ist hingegen $\Phi_{A'} = \tau_v$ eine reine Translation um v (d.h. $A = \mathbf{1}$), so erhalten wir

$$p(B,b,c)(x+v) = p(B, Bv + b, v^\top Bv + b^\top v + c). \tag{9.1.6}$$

Bemerkung 9.1.13 (Geometrische Interpretation)**.** Nach dem Hilbertschen Nullstellensatz ist (9.1.3) für Polynome vom totalen Grad 2 äquivalent zu der Aussage

$$\Phi_{A'}^{-1}[Q_{\mathbb{L}}(B')] = Q_{\mathbb{L}}((A')^\top B' A') \tag{9.1.7}$$

für jede Körperweiterung $\mathbb{L}$ von $\mathbb{K}$, und impliziert insbesondere die (im Allgemeinen schwächere) Aussage

$$\Phi_{A'}^{-1}[Q(B')] = Q((A')^\top B' A') \quad \text{bzw.} \quad \Phi_{A'}[Q(B')] = Q(((A')^{-1})^\top B (A')^{-1}).$$

Dies zeigt u.a., dass Quadriken unter affinen Abbildungen wieder auf Quadriken abgebildet werden. Im Fall $\mathbb{K} = \mathbb{R}$ sieht man insbesondere, dass euklidische Bewegungen reelle Quadriken wieder auf reelle Quadriken abbilden.

Definition 9.1.14. Zwei Polynome $p_1, p_2 \in \mathbb{K}[X_1,\dots,X_n]_{\leq 2}$ heißen *affin äquivalent*, falls $p_1 \circ \Phi = p_2$ für ein $\Phi \in \mathrm{Aff}_n(\mathbb{K})$ gilt.

Zwei affine Quadriken $V_1, V_2 \subseteq \mathbb{K}^n$ heißen *affin äquivalent*, falls es eine affine Bewegung Φ gibt mit $\Phi[V_1] = V_2$.

Ist $\mathbb{K} = \mathbb{R}$, so heißen $p_1, p_2 \in \mathbb{R}[X_1,\dots,X_n]_{\leq 2}$ *euklidisch äquivalent*, falls $p_1 \circ \Phi = p_2$ für eine euklidische Bewegung Φ gilt.

Ist $\mathbb{K} = \mathbb{R}$, so heißen zwei affine Quadriken $V_1, V_2 \subseteq \mathbb{K}^n$ *euklidisch äquivalent*, falls $\Phi[V_1] = V_2$ für eine euklidische Bewegung Φ gilt.

Bemerkung 9.1.15. Sind $p_1, p_2 \in \mathbb{K}[X_1,\dots,X_n]_{\leq 2}$ Polynome vom selben Grad[2], so sind p_1 und p_2 nach dem Hilbertschen Nullstellensatz genau dann affin äquivalent, wenn die Quadriken $V_{\mathbb{L}}(p_1)$ und $V_{\mathbb{L}}(p_2)$ über beliebigen Köpererweiterungen $\mathbb{L}$ von $\mathbb{K}$ affin äquivalent sind. Im Allgemeinen ist diese Aussage stärker als die Aussage, dass $V(p_1)$ und $V(p_2)$ affin äquivalent sind.

[2]Diese Voraussetzung ist notwendig, denn $(X_1-1)(X_2-2)^2$ und $(X_1-1)^2(X_2-2)$ definieren stets dieselben Nullstellenmengen!

Wir halten noch die folgende Konsequenz aus (9.1.3) und (9.1.4) fest:

Lemma 9.1.16. *Sind Polynome $p_1, p_2 \in \mathbb{K}[X_1,\dots,X_n]_{\leq 2}$ affin äquivalent und ist $p_j = p(B'_j) = p(B_j, b_j, c_j)$, so gilt $\operatorname{rk}(B'_1) = \operatorname{rk}(B'_2)$ und $\operatorname{rk}(B_1) = \operatorname{rk}(B_2)$.* □

Damit ist zumindest einmal klar, dass nicht alle Quadriken affin äquivalent zueinander sind. Wir überlegen uns nun, was wir mittels des Spektralsatzes (und quadratischer Ergänzung) über euklidische Äquivalenz von Quadriken sagen können. Die geometrische Bedeutung des Resultats werden wir in den folgenden Abschnitte noch genauer untersuchen.

Konstruktion 9.1.17 (Diagonalisierung quadratischer Polynome)**.** Wir betrachten ein reelles Polynom $p = p(B') = p(B, b, c) \in \mathbb{R}[X_1,\dots,X_n]_{\leq 2}$. Da B symmetrisch ist existiert nach dem rellen Spektralsatz eine orthogonale Matrix $S \in \mathrm{O}_n(\mathbb{R})$ und eine Diagonalmatrix $\operatorname{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$ (mit $\lambda_j \in \mathbb{R}^\times$ und $r = \operatorname{rk}(B)$), so dass $S^T B S = \operatorname{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$. Dabei sind $\lambda_1,\dots,\lambda_r$ genau die von 0 verschiedenen Eigenwerte von B (mit Vielfachheiten). Setzen wir $b' := S^\top b$, so folgt mit (9.1.5), dass

$$p(Sx) = \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2 + 2b'_1 x_1 + \cdots + 2b'_n x_n + c \quad \text{mit} \quad r = \operatorname{rk}(B). \tag{9.1.8}$$

Wir erhalten also ein zu p euklidisch äquivalentes Polynom, dass keine „gemisch-quadratischen Terme“ der Form $x_i x_j$ mit $i \neq j$ mehr enthält. Insbesondere gilt

$$S^{-1}[V(p)] = \{x \in \mathbb{R}^n \mid \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2 + 2b'_1 x_1 + \cdots + 2b'_n x_n + c = 0\}$$

und analog $S^{-1}[V_{\mathbb{C}}(p)] = \{x \in \mathbb{C}^n \mid \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2 + 2b'_1 x_1 + \cdots + 2b'_n x'_n + c = 0\}$. Dabei sind $\lambda_1,\dots,\lambda_r$ genau die von 0 verschiedenen Eigenwerte von B (mit Vielfachheiten).

Wir wollen nun noch die linearen Terme soweit wie möglich vereinfachen.

Konstruktion 9.1.18 (Quadratische Ergänzung)**.** Für $j \in \{1,\dots,r\}$ beobachten wir, dass

$$\lambda_j y_j^2 + b'_j y_j = \lambda_j \left(y_j^2 + 2\frac{b'_j}{\lambda_j} y_j \right) = \lambda_j \left(y_j + \frac{b'_j}{\lambda_j} \right)^2 - \frac{\left(b'_j\right)^2}{\lambda_j}.$$

Wir erhalten daher,

$$p(Sy) = \left(\sum_{j=1}^{r} \lambda_j \left(y_j + \frac{b'_j}{\lambda_j} \right)^2 \right) + \sum_{j=r+1}^{n} b'_j y'_j + \left(c - \sum_{j=1}^{r} \frac{\left(b'_j\right)^2}{\lambda_j} \right).$$

Wir können also die ersten r linearen Terme loswerden, indem wir geeignet verschieben. Setzen wir nämlich

$$v := (b'_1/\lambda_1, \dots, b'_r/\lambda_r, 0, \dots, 0) \quad \text{und} \quad c' := c - \sum_{j=1}^{r} \frac{\left(b'_j\right)^2}{\lambda_j}$$

so erhalten wir

$$p(Sy - Sv) = p(S)(y - v) = \sum_{j=1}^{n} \lambda_j y_j^2 + \sum_{j=r+1}^{n} b'_j y'_j + c'.$$

Setzen wir nun $\Phi := \Phi_{S,-Sv} \in \mathrm{Mot}(\mathbb{R}^n)$, so gilt

$$q := p \circ \Phi = p(B_1') = p(B_1, b'', c') \quad \text{mit} \quad B_1' = \begin{pmatrix} \lambda_1 & & & & & & 0 \\ & \ddots & & & & & \vdots \\ & & \lambda_r & & & & 0 \\ & & & 0 & & & b'_{r+1} \\ & & & & \ddots & & \vdots \\ & & & & & 0 & b'_n \\ 0 & \dots & 0 & b'_{r+1} & \dots & b'_n & c' \end{pmatrix}$$

Dabei sind $\lambda_1, \dots, \lambda_r$ immer noch die von 0 verschiedenen Eigenwerte von B (mit Vielfachheiten).

Konstruktion 9.1.19 (Aufräumen)**.** Wir betrachten nun, welche Möglichkeiten noch bleiben. Wir wissen, dass $\mathrm{rk}(B_1') = \mathrm{rk}(B') \geq \mathrm{rk}(B), \mathrm{rk}(B)+1, \mathrm{rk}(B+2)\} = \{r, r+1, r+2\}$.

FALL I: $\mathrm{rk}(B') = \mathrm{rk}(B)$.

In diesem Fall sind schon $b'_{r+1}, \dots, b'_n = c' = 0$. Es gilt daher (für $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$), dass

$$q(x) = \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 \quad \text{und} \quad \Phi^{-1}[V_{\mathbb{K}}(p)] = \{x \in \mathbb{K}^n \mid \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 = 0\}.$$

FALL II: $\mathrm{rk}(B') = \mathrm{rk}(B) + 1$ und $b'' = 0$.

In diesem Fall ist $c' \neq 0$ und wir setzen $\lambda'_j := -\lambda_j / c'$. Dann gilt

$$q(x) = -c'(\lambda'_1 x_1^2 + \dots + \lambda'_r x_r^2 - 1) \quad \text{und} \quad \Phi^{-1}[V_{\mathbb{K}}(p)] = \{x \in \mathbb{K}^n \mid \lambda'_1 x_1^2 + \dots + \lambda'_r x_r^2 = 1\}.$$

Eventuell haben sich hier die Vorzeichen der λ'_j geändert, aber gegenüber den λ_j höchstens um ein globales Vorzeichen.

[26.06.24]

Bevor wir uns den dritten Fall anschauen (dessen Behandlung zusätzliche Ideen erfordert), schauen wir uns zwei Beispiele in der Ebene an.

Beispiel 9.1.20 (Eine Nichtstandard-Ellipse)**.** Wir betrachten die Quadrik

$$E := \{x \in \mathbb{R}^2 \mid 36x_1^2 + 29x_2^2 + 24x_1x_2 - 180 = 0\} \subseteq \mathbb{R}^2.$$

Es gilt dann

$$E = \{x \in \mathbb{R}^2 \mid x^\top Bx + 2b^\top x + c = 0\} = \{x \in \mathbb{R}^2 \mid (x')^\top B'x' = 0\},$$

wobei (mit derselben Notation wie zuvor)

$$B' := \begin{pmatrix} 36 & 12 & 0 \\ 12 & 29 & 0 \\ 0 & 0 & -180 \end{pmatrix}, B := \begin{pmatrix} 36 & 12 \\ 12 & 29 \end{pmatrix}, b := \begin{pmatrix} 0 \\ 0 \end{pmatrix}, c := -180, x' = \begin{pmatrix} x \\ 1 \end{pmatrix}.$$

Vorsicht: Die Nebendiagonaleinträge der Matrix B sind 12 und nicht etwa 24!

Wir diagonalisieren nun die Matrix B orthogonal: Das charakteristische Polynom ist

$$\chi_B(X) = \det\begin{pmatrix} X-36 & -12 \\ -12 & X-29 \end{pmatrix} = X^2 - 65X + 900 = (X-20)(X-45).$$

Die Eigenräume zu den Eigenwerten 20 und 45 sind gegeben durch

$$V_{20}(B) = \ker\begin{pmatrix} -16 & -12 \\ -12 & -9 \end{pmatrix} = \ker\begin{pmatrix} 4 & 3 \\ 0 & 0 \end{pmatrix} = \mathbb{K}\begin{pmatrix} 3 \\ -4 \end{pmatrix},$$

$$V_{45}(B) = \ker\begin{pmatrix} 9 & -12 \\ -12 & 16 \end{pmatrix} = \ker\begin{pmatrix} 3 & -4 \\ 0 & 0 \end{pmatrix} = \mathbb{K}\begin{pmatrix} 4 \\ 3 \end{pmatrix}.$$

Wir erhalten daher ein ONB aus Eigenvektoren durch die Spalten der Matrix

$$T := \frac{1}{5}\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix},$$

und diese Matrix ist folglich orthogonal. Weiter gilt

$$T^{-1}AT = \operatorname{diag}(20,45) \quad \text{und} \quad T^\top b = 0.$$

Sei nun $f : \mathbb{R}^2 \to \mathbb{R}^2$ gegeben durch $f(x) = T^{-1}x = T^\top x$. Dann gilt

$$y \in f[E] \iff Ty \in E \iff y^\top T^\top ATy + 2(T^\top b)^\top y + c = 0 \iff 20y_1^2 + 45y_2^2 = 180,$$

Wegen 20/180 = 1/9 und 45/180 = 1/4 folgt, dass

$$f(E) = \left\{ y \in \mathbb{R}^2 \mid \left(\frac{y_1}{3}\right)^2 + \left(\frac{y_2}{2}\right)^2 = 1 \right\}.$$

Die Quadrik $f[E]$ ist eine Standardellipse, und E geht aus dieser durch eine euklidische Bewegung hervor. Daher ist E selbst eine Ellipse.

Die Rechnung in Beispiel 9.1.20 war besonders einfach, weil der lineare Term 0 war, und daher keine quadratische Ergänzung nötig war. Wir betrachten nun ein komplizierteres Beispiel.

Beispiel 9.1.21 (Eine Nichtstandard-Hyperbel)**.** Wir betrachten die Quadrik

$$H := \{x \in \mathbb{R}^2 \mid x_1x_2 + \sqrt{2}x_1 + 1 = 0\} = \{x \in \mathbb{R}^2 \mid x^\top Bx + 2b^\top x + c = 0\} = \{x \in \mathbb{R}^2 \mid (x')^\top B'x' = 0\},$$

wobei (in unserer Standardnotation)

$$B' := \begin{pmatrix} 0 & 1/2 & 1/\sqrt{2} \\ 1/2 & 0 & 0 \\ 1/\sqrt{2} & 0 & 1 \end{pmatrix}, B := \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}, b := \begin{pmatrix} 1/\sqrt{2} \\ 0 \end{pmatrix}, c := 1, x' = \begin{pmatrix} x \\ 1 \end{pmatrix}.$$

Vorsicht: Die Nebendiagonaleinträge der Matrix B sind 1/2 und nicht etwa 1!
Wir diagonalisieren nun die Matrix B orthogonal. Das charakteristische Polynom ist

$$\chi_B(X) = \det\begin{pmatrix} X & -1/2 \\ -1/2 & X \end{pmatrix} = X^2 - 1/4 = (X + 1/2)(X - 1/2).$$

Die Eigenräume zu den Eigenwerten $-1/2$ und $1/2$ sind gegeben durch

$$V_{-1/2}(B) = \ker\begin{pmatrix} -1/2 & -1/2 \\ -1/2 & -1/2 \end{pmatrix} = \ker\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \mathbb{K}\begin{pmatrix} -1 \\ 1 \end{pmatrix},$$

$$V_{1/2}(B) = \ker\begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} = \ker\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix} = \mathbb{K}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Wir erhalten daher ein ONB aus Eigenvektoren durch die Spalten der Matrix

$$T := \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$

und diese Matrix ist folglich orthogonal. Weiter gilt

$$T^{-1}AT = \operatorname{diag}(-1/2, 1/2) \quad \text{und} \quad T^\top b = \begin{pmatrix} -1/2 \\ 1/2 \end{pmatrix}.$$

Sei nun $f_1 : \mathbb{R}^2 \to \mathbb{R}^2$ gegeben durch $f_1(x) = T^{-1}x = T^\top x$. Dann gilt

$$y \in f_1[H] \iff Ty \in H \iff y^\top T^\top ATy + 2(T^\top b)^\top y + c = 0 \iff -1/2y_1^2 + 1/2y_2^2 - y_1 + y_2 + 1 = 0.$$

Die Formel wird etwas schöner, wenn wir mit 2 durchmultiplizieren. Wir erhalten dann:

$$f_1[H] = \{y \in \mathbb{R}^2 \mid y_1^2 - y_2^2 + 2y_1 - 2y_2 - 2 = 0\}.$$

Quadratische Ergänzung liefert nun

$$y_1^2 - y_2^2 + 2y_1 - 2y_2 - 2 = (y_1 + 1)^2 - (y_2 + 1)^2 - 2.$$

Setzen wir nun $z := y + \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, so gilt

$$y \in f_1[H] \iff z_1^2 - z_2^2 = 2 \iff \left(\frac{z_1}{\sqrt{2}}\right)^2 - \left(\frac{z_2}{\sqrt{2}}\right)^2 = 1.$$

Definieren wir nun eine euklidische Bewegung $f : \mathbb{R}^2 \to \mathbb{R}^2$, $x \mapsto T^\top x + \begin{pmatrix}1\\1\end{pmatrix}$, so folgt, dass

$$f[H] = \left\{ x \in \mathbb{R}^2 \mid \left(\frac{z_1}{\sqrt{2}}\right)^2 - \left(\frac{z_2}{\sqrt{2}}\right)^2 = 1 \right\}.$$

Dies ist eine Standardhyperbel, und H geht aus dieser durch eine euklidische Bewegung hervor, ist also ebenfalls eine Hyperbel.

In Konstruktion 9.1.19 haben wir einen Fall noch nicht behandelt. Diese Fall ist sehr nervig und kann überhaupt nur auftreten, wenn $\operatorname{rk}(B) = r < n$, wenn also B nicht vollen Rang hat. Der Vollständigkeit halber, wollen wir diesen Fall nun auch noch behandeln.

Konstruktion 9.1.22 (Zu Ende aufräumen)**.** Der in Konstruktion 9.1.19 noch fehlende Fall lautet:

FALL *III*: $\operatorname{rk}(B') = \operatorname{rk}(B) + 2$ und $b'' := (0, \dots, 0, b'_{r+1}, \dots, b'_n)^\top \neq 0$.

Durch orthogonales Diagonalisieren und quadratische Ergänzung wie in den letzten beiden Beispielen können wir uns auf den Fall von Polynomen der Form

$$q(x) = \lambda x_1^2 + \dots + \lambda_r x_r^2 + 2b'_{r+1}x_{r+1} + \dots + 2b'_n x_n + c$$

zurückziehen, wobei es nach Annahme mindestens einen linearen Term gibt. Unser Ziel ist es nun zu zeigen, dass man alle bis auf einen der linearen Terme und den konstanten Term loswerden kann. Wir setzen $w_1 := -\frac{1}{\sqrt{(b'_{r+1})^2 + \dots + (b'_n)^2}}(b'_{r+1}, \dots, b'_n)^\top \in \mathbb{R}^{n-r}$ und ergänzen w_1 zu einer Basis von $\mathbb{R}^{n-r}$. Durch Anwenden von Gram-Schmidt erhalten wir eine ONB $(w_1, \dots, w_{n-r})$ von $\mathbb{R}^{n-r}$, und es gilt dann

$$Q := \begin{pmatrix} e_1 & \cdots & e_r & 0 & \dots & 0 \\ 0 & \dots & 0 & w_1 & \dots & w_{n-r} \end{pmatrix} \in \mathrm{O}_n(\mathbb{R}).$$

Es gilt dann $Qe_1 = e_1, \dots, Qe_r = e_r$ und $Qe_{r+1} = -\|b''\|^{-1}b''$. Speziell gilt dann

$$Q^\top b'' = -\|b''\| Q^{-1}\left(-\|b''\|^{-1}b''\right) = -\|b''\| e_{r+1}.$$

Wir definieren nun $y := Qx$, so dass insbesondere $y_1 = x_1, \dots, y_r = x_r$ gilt. Es gilt dann

$$\begin{aligned} q(y) &= \lambda_1 y_1^2 + \dots + \lambda_r y_r^2 + 2(b'')^\top y + c' \\ &= \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 + 2(b'')^\top Q x + c' \\ &= \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 + 2\left(Q^\top b''\right)^\top x + c' \\ &= \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 - 2\|b''\| e_{r+1}^\top x + c' \\ &= \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 - 2\|b''\| x_{r+1} + c' \\ &= 2\|b''\|\left(\lambda'_1 x_1^2 + \dots + \lambda'_r x_r^2 - x_{r+1} + c'/2\|b''\|\right), \end{aligned}$$

wobei $\lambda'_j := \lambda_j / 2\|b''\|$ dasselbe Vorzeichen wie λ_j hat. Den konstanten Term werden wir nun noch mittels einer Verschiebung los: Wir definieren eine euklidische Bewegung f durch

$$f(x) := Q(x + c'/2\|b''\| e_{r+1}).$$

Ist $z = f(x)$, so folgt, dass

$$q(z) = 2\|b''\|\left(\lambda'_1 x_1^2 + \dots + \lambda'_r x_r^2 - (x_{r+1} + c'/2\|b''\|) + c'/2\|b''\|\right) = \|b''\|\left(\lambda'_1 x_1^2 + \dots + \lambda'_r x_r^2 - x_{r+1}\right),$$

und daher

$$V(q) = f^{-1}\left[\left\{x \in \mathbb{R}^n \mid \|b''\|\lambda'_1 x_1^2 + \dots + \lambda'_r x_r^2 = x_{r+1}\right\}\right]$$

Bemerkung 9.1.23. Wir erkennen nun in allen drei Fällen eine ähnliche Struktur: Wir können die Quadrik in allen Fällen durch Anwenden einer euklidischen Bewegung auf eine Modellquadrik der Form

$$Q = \{x \in \mathbb{R}^n \mid \lambda_1' x_1^2 + \cdots + \lambda_r' x_r^2 = R(x)\}$$

bringen. In Fall I wählen wir $R(x) = 0$, in Fall II ist $R(x) = 1$ und in Fall III ist $R(x) = x_{r+1}$. Zur besseren geometrischen Interpretation der Parameter λ_j' ist es zweckmäßig, diese als $\lambda_j' = \varepsilon_j / a_j^2$ mit $\varepsilon_j \in \{\pm 1\}$ und $a_j \in (0, \infty)$ zu schreiben. Es gilt dann

$$Q = Q(\varepsilon_1, \ldots, \varepsilon_r, a_1, \ldots, a_r, R) = \left\{ x \in \mathbb{R}^n \mid \varepsilon_1 \left(\frac{x_1}{a_1}\right)^2 + \ldots \varepsilon_r \left(\frac{x_r}{a_r}\right)^2 = R(x) \right\}. \tag{9.1.9}$$

Diese Darstellung ist allerdings nicht ganz eindeutig, d.h. es gibt Modellquadriken mit verschiedenen Parametern, die trotzdem euklidisch äquivalent sind:

Durch Anwendung von Transpositionen (die ja geometrisch Spiegelungen entsprechen und daher euklidische Bewegungen sind), kann man die Reihenfolge der Variablen x_n beliebig vertauschen. Ist σ eine Permutation von $\{1, \ldots, r\}$ so sind also

$$Q(\varepsilon_1, \ldots, \varepsilon_r, a_1, \ldots, a_r, R) \quad \text{und} \quad Q(\varepsilon_{\sigma(1)}, \ldots, \varepsilon_{\sigma(r)}, a_{\sigma(1)}, \ldots, a_{\sigma(r)}, R),$$

euklidisch äquivalent.

Im Fall I kann man die definierende Gleichung noch mit einer beliebigen globalen Konstanten multiplizieren. Für $a > 0$ und $\varepsilon \in \{\pm 1\}$ sind also

$$Q(\varepsilon_1, \ldots, \varepsilon_r, a_1, \ldots, a_r, 0) \quad \text{und} \quad Q^I_{\mathbb{K}}(\varepsilon\varepsilon_1, \ldots, \varepsilon\varepsilon_r, aa_r, \ldots, aa_r, 0).$$

euklidisch äquivalent. Im Fall III liefert die Spiegelung an der Hyperebene $\{e_{r+1}\}^\perp$ eine euklidische Äquivalenz zwischen

$$Q^{III}_{\mathbb{K}}(\varepsilon_1, \ldots, \varepsilon_r, a_1, \ldots, a_r) \quad \text{und} \quad Q^{III}_{\mathbb{K}}(-\varepsilon_1, \ldots, -\varepsilon_r, a_1, \ldots, a_r).$$

Bezeichnet nun r_+ die Anzahl der positiven und r_- die Anzahl der negativen Vorzeichen unter den ε_j, so machen wir die folgenden Normalisierungskonventionen:

- Im Fall I wählen wir (durch Umsortieren und ggf. ein globales Vorzeichen) die Vorzeichen so, dass $r_+ \geq r_-$ und $\{\varepsilon_1, \ldots, \varepsilon_{r_+}\} = 1$. Die Parameter a_j wählen wir so, dass $a_1 \geq a_2 \geq \cdots \geq a_{r+}$ und $a_{r_+ + 1} \geq \cdots \geq a_r = 1$.
- Im Fall II können wir die Vorzeichen lediglich umsortieren, d.h. sowohl $r_+ \geq r_-$ als auch $r_- \geq r_+$ können auftauchen. Wir treffen wieder die Konventionen $\{\varepsilon_1, \ldots, \varepsilon_{r_+}\} = 1$ sowie $a_1 \geq a_2 \geq \cdots \geq a_{r+}$ und $a_{r_+ + 1} \geq \cdots \geq a_r$ (wobei wir a_r nicht normieren können).
- Im Fall III wählen wir $r_+ \geq r_-$ und $\{\varepsilon_1, \ldots, \varepsilon_{r_+}\} = 1$ sowie $a_1 \geq a_2 \geq \cdots \geq a_{r+}$ und $a_{r_+ + 1} \geq \cdots \geq a_r$.

Wir machen noch zwei abschließende Beobachtungen: Die ursrpünglichen ε_j waren die Vorzeichen der λ_j', und diese entstanden aus den Eigenwerten von B durch Skalieren. Ist $(\sigma_+, \sigma_-, \sigma_0)$ die Signatur von B, so folgt, dass

$$(r_+, r_-) \in \{(\sigma_+, \sigma_-), (\sigma_-, \sigma_+)\}.$$

Insbesondere gilt $r_+ + r_- = r = \mathrm{rk}(B)$.

Wir fassen zusammen:

Satz 9.1.24 (Satz von der Hauptachsentransformation)**.** *Sei $p = p(B') = p(B,b,c) \in \mathbb{R}[X_1,\dots,X_n]$ ein Polynom vom Grad 2 und $Q = V(p)$ die zugehörige Quadrik. Weiter bezeichnen r' und r den Rang von B' bzw. B und $(\sigma_+,\sigma_-,\sigma_0)$ die Signatur von B. Dann existieren $r_+,r_- \in \mathbb{N}$ mit $\{r_+,r_-\} = \{\sigma_+,\sigma_-\}$ und $a_1,\dots,a_r \in (0,\infty)$ mit $a_1 \geq a_2 \geq \cdots \geq a_{r+}$ und $a_{r_++1} \geq \cdots \geq a_r$, so dass einer der folgenden Fälle eintritt.*

(Fall I) $r' = r$, $r_+ \geq r_-$, $a_r = 1$ *und Q ist euklidisch äquivalent zu*

$$Q^I(r_+,r_-,a_1,\dots,a_r) = \left\{x \in \mathbb{R}^n \mid \left(\left(\frac{x_1}{a_1}\right)^2 + \cdots + \left(\frac{x_{r_+}}{a_{r_+}}\right)^2\right) - \left(\left(\frac{x_{r_++1}}{a_{r_++1}}\right)^2 + \cdots + \left(\frac{x_r}{a_r}\right)^2\right) = 0\right\}$$

(Fall II) $r' = r+1$ *und Q ist euklidisch äquivalent zu*

$$Q^{II}(r_+,r_-,a_1,\dots,a_r) = \left\{x \in \mathbb{R}^n \mid \left(\left(\frac{x_1}{a_1}\right)^2 + \cdots + \left(\frac{x_{r_+}}{a_{r_+}}\right)^2\right) - \left(\left(\frac{x_{r_++1}}{a_{r_++1}}\right)^2 + \cdots + \left(\frac{x_r}{a_r}\right)^2\right) = 1\right\}$$

(Fall III) $r' = r+2 \leq n+1$, $r_+ \geq r_-$ *und Q ist euklidisch äquivalent zu*

$$Q^{III}(r_+,r_-,a_1,\dots,a_r) = \left\{x \in \mathbb{R}^n \mid \left(\left(\frac{x_1}{a_1}\right)^2 + \cdots + \left(\frac{x_{r_+}}{a_{r_+}}\right)^2\right) - \left(\left(\frac{x_{r_++1}}{a_{r_++1}}\right)^2 + \cdots + \left(\frac{x_r}{a_r}\right)^2\right) = x_{r+1}\right\}$$

Man kann zeigen, dass mit den obigen Konventionen die Modellquadrik im Wesentlichen eindeutig ist. Ganz eindeutig ist sie nicht, denn die leere Quadrik hat mehrere mögliche Beschreibungen, die sich aber in den komplexen Punkten unterscheiden. Wir werden uns das in Dimensionen 2 und 3 genauer anschauen, und den allgemeinen Fall hier nicht behandeln. Im Fall I nennt man die Quadrik I eine *Kegelquadrik* mit *Signatur* (r_+,r_-) und *Lägenparametern* $(a_1,\dots,a_r)$. Im Fall II (bzw. Fall III) spricht man von einer *Mittelpunktsquadrik* (bzw. *parabolischen Quadrik*). Die Bedeutung dieser Namen wird sich im Laufe dieses Kapitels klären.

Bemerkung 9.1.25 (Hauptachsen)**.** Die Modellquadriken sind so ausgerichtet, dass die ersten r Achsen des Standardkoordinatensystems Symmetrieachsen sind. Diese sind die sogenannten *Hauptachsen* der jeweiligen Modellquadrik. Im Fall III bezeichnet man auch die Gerade $\mathbb{K}e_{r+1}$ als Hauptachse.

Ist Q eine beliebige Quadrik, so geht sie mittels einer euklidischen Bewegung aus einer Modellquadrik hervor, und die Bilder der ersten r (bzw. $r+1$ Standardkoordinatenachsen unter dieser Bewegung sind dann die sogenannten *Hauptachsen* von Q. Eine wie im Beweis von Satz 9.1.24 konstruierte euklidische Bewegung, die Q auf eine Modellquadrik und die Hauptachsen von Q auf die Standardkoordinatenachsen abbildet, heißt daher auch eine *Hauptachsentransformation* zu Q.

Ist $Q^\alpha(r_+,r_-,a_1,\dots,a_r)$ eine Modellquadrik, so können wir diese durch eine affine Transformation (genauer: durch Multiplikation mit einer invertierbaren Diagonalmatrix) auf die Quadrik

$$Q^\alpha(r_+,r_-) := Q^\alpha(r_+,r_-,1,\dots,1)$$

transformieren. Damit haben wir das folgende Korollar bewiesen:

Korollar 9.1.26 (Affine Modelle)**.** *Sei $p = p(B') = p(B,b,c) \in \mathbb{R}[X_1,\dots,X_n]$ ein Polynom vom Grad 2 und $Q = V(p)$ die zugehörige Quadrik. Weiter bezeichnen r' und r den Rang von B' bzw. B und $(\sigma_+,\sigma_-,\sigma_0)$ die Signatur von B. Dann existieren $r_+,r_- \in \mathbb{N}$ mit $\{r_+,r_-\} = \{\sigma_+,\sigma_-\}$, so dass einer der folgenden Fälle eintritt.*

(Fall I) $r' = r$, $r_+ \geq r_-$ *und Q ist euklidisch äquivalent zu $Q^I(r_+,r_-)$.*

(Fall II) $r' = r+1$ *und Q ist euklidisch äquivalent zu $Q^{II}(r_+,r_-)$.*

(Fall III) $r' = r+2 < n+1$, $r_+ \geq r_-$ *und Q ist euklidisch äquivalent zu $Q^{III}(r_+,r_-)$.*

Insbesondere gibt es in jeder Dimension nur endlich viele Quadriken bis auf affine Ähnlichkeit. □

In kleinen Dimensionen kann man alle affinen Ähnlichkeitsklassen affiner Quadriken explizit auflisten. Das wollen wir im nächsten Abschnitt in Dimension 2 und 3 tun, und zugleich eine bessere geometrische Vorstellung für Quadriken gewinnen.

Zusammenfassung von Abschnitt 9.1.

(1) Quadriken sind Nullstellenmengen quadratischer Polynome in mehreren Veränderlichen.

(2) Mittels Hauptachsentransformation kann man jede Quadrik in eine besonders einfache Modellquadrik überführen,. Dazu verwendet man den reellen Spektralsatz und quadratische Ergänzung.

(3) Modellquadriken werden durch Gleichungen der Form $(x_1^2+\dots+x_r^2)-(y_1^2+\dots+y_s^2) = R$ beschrieben, wobei $R \in \{0,1\}$ oder $R = z$ für eine weitere Variable z gilt.

9.2 Ebene und räumliche Quadriken

9.2.1 Ebene Quadriken

Es sei $p = p(B') = p(B,b,c) \in \mathbb{R}[X_1,X_2]$ ein Polynom vom Grad 2 und $Q = V(p) \subseteq \mathbb{R}^2$ die zugehörige *ebene Quadrik*. Es seien r' und r die Ränge von B' bzw. B und es sei (r_+,r_-) die Signatur von Q. Damit p wirklich Grad 2 hat, muss $r \geq 1$ gelten. Es gilt dann also

$$r = r_+ + r_- \in \{1,2\} \quad \text{und} \quad r' \in \{r, r+1\}.$$

Bis auf euklidische Äquivalenz gibt es die folgenden Möglichkeiten für $Q(B')$:

Beispiel 9.2.1 (Ebene Kegelquadriken)**.** Im Fall I ist $r' = r$ und (nach unserer Konvention) $r_+ \geq r_-$ und die entsprechende Modellquadrik ist entweder der Ursprung, eine Ursprungsgerade oder besteht aus zwei sich schneidenen Ursprungsgerade. Da euklidische Bewegungen affine Unterräume auf affine Unterräume derselben Dimension abbilden, ist dann auch Q selbst entweder eine Punkt, eine affine Gerade oder besteht aus zwei sich schneidenden affinen Geraden. Genauer gilt:

r'	r	(r_+, r_-)	Gleichung der Modellquadrik	Name der Quadrik
2	2	(2,0)	$(x_1/a_1)^2 + (x_2/a_2)^2 = 0$	Punkt
2	2	(1,1)	$(x_1/a_1)^2 - (x_2/a_2)^2 = 0$	zwei sich schneidende affine Geraden
1	1	(1,0)	$(x_1/a_1)^2 = 0$	affine Gerade

Beispiel 9.2.2 (Ebene Mittelpunktsquadriken)**.** Im Fall II ist $r' = r+1$ und die entsprechende Modellquadrik ist entweder leer, eine Modellellipse, eine Modellhyperbel oder besteht aus zwei parallelen affinen Geraden. Im ersten bzw. letzten Fall ist Q selbst leer bzw. besteht aus zwei parallelen affinen Geraden. Im zweiten bzw. dritten Fall nennen wir Q eine *Ellipse* bzw. *Hyperbel*. Genauer gilt:

r'	r	(r_+, r_-)	Gleichung der Modellquadrik	Name der Quadrik
3	2	(2,0)	$(x_1/a_1)^2 + (x_2/a_2)^2 = 1$	Ellipse
3	2	(1,1)	$(x_1/a_1)^2 - (x_2/a_2)^2 = 1$	Hyperbel
3	2	(0,2)	$-(x_1/a_1)^2 - (x_2/a_2)^2 = 1$	leere Menge
2	1	(1,0)	$(x_1/a_1)^2 = 1$	zwei parallele affine Geraden
2	1	(0,1)	$-(x_1/a_1)^2 = 1$	leere Menge

Beispiel 9.2.3 (Ebene parabolische Quadriken)**.** Im Fall III ist $r' = r+1$ und notwendigerweise $r = 1$. In diesem Fall gibt es nur eine Art von Modellquadriken, nämlich Modellparabeln, und daher sind alle solche Quadriken Parabeln. Dies erklärt den Namen „parabolische Quadriken“.

r'	r	(r_+, r_-)	Gleichung der Modellquadrik	Name der Quadrik
3	1	(1,0)	$(x_1/a_1)^2 = x_2$	Parabel

Im Folgenden nennen wir eine Quadrik *ausgeartet*, wenn sie eine endliche Vereinigung von algebraischen Mengen vom Grad ≤ 1 ist. Ausgeartete ebene Quadriken sind also Quadriken, die entweder leer sind oder aus endlich vielen Punkten oder Geraden bestehen. Damit können wir die Klassifikation der ebenen Quadriken wie folgt formulieren:

Satz 9.2.4 (Klassifikation ebener Quadriken)**.** *Jede nicht-ausgeartete ebene Quadrik ist entweder eine Ellipse, Hyperbel oder Parabel. Die ausgearteten ebenen Quadriken sind: Die leere Quadrik, einpunktige Quadriken, affine Gerade, Paare sich schneidender affiner Geraden und Paare paralleler affiner Geraden.* □

Die drei nicht-ausgearteten ebenen Quadriken (Ellipse, Hyperbel und Parabel) spielen in vielen Bereichen der Mathematik[3] eine zentrale Rolle. Wir wollen uns diese drei Arten von Quadriken nun etwas genauer anschauen.

Bemerkung 9.2.5 (Beschreibungen der Modellellipse)**.** Wir diskutieren drei Beschreibungen der Modellellipse

$$E(a_1, a_2) := Q^{II}(2, 0, a_1, a_2) \quad (a_1 > a_2).$$

[3] In der Analysis unterscheidet man elliptische, hyperbolische und parabolische Differentialgleichungen, in der Geometrie unterscheidet man elliptische, hyperbolische und parabolische Isometrien metrischer Räume, in der Theorie der algebraischen Gruppen spricht man von elliptischen, hyperbolischen und parabolischen Elementen usw. usf.

1. BESCHREIBUNG ALS NULLSTELLENMENGE

Nach Definition ist $E(a_1,a_2)$ die Menge aller $x \in \mathbb{R}^2$, die der Gleichung

$$\left(\frac{x_1}{a_1}\right)^2 + \left(\frac{x_2}{a_2}\right)^2 = 1$$

genügen. Aus dieser Gleichung folgt sofort, dass $|x_1| \leq 1$ und $|x_2| \leq 1$ gilt, folglich ist $E(a_1,a_2)$ beschränkt. Da jede Quadrik als Nullstellenmenge einer stetigen Funktion abgeschlossen ist, folgt daraus, dass $E(a_1,a_2) \subseteq \mathbb{R}^2$ kompakt ist. Ist $a_1 = a_2$, so handelt es sich bei $E(a_1,a_2)$ um einen Kreis vom Radius $r = a_1 = a_2$ um den Ursprung, andernfalls nennen wir $E(a_1,a_2)$ eine *echte Ellipse*.

2. PARAMETRISIERUNG

Die Ellipse $E(a_1,a_2)$ wird durch die Abbildung $x \mapsto \operatorname{diag}(a_1,a_2)x$ bijektiv auf den Einheitskreis abgebildete, dessen Punkte durch trigonometrische Funktionen beschrieben werden können. Daher ist die Abbildung

$$\varphi : [0,2\pi) \to E(a_1,a_2), \quad t \mapsto \begin{pmatrix} a_1\cos(t) \\ a_2\sin(t) \end{pmatrix}$$

eine stetige[4] Bijektion.

3. BRENNPUNKTBESCHREIBUNG

Wir definieren $e := \sqrt{a_1^2 - a_2^2}$ und definieren die *Brennpunkte* von $E(a_1,a_2)$ als

$$f_- := \begin{pmatrix} -e \\ 0 \end{pmatrix} \quad \text{und} \quad f_+ := \begin{pmatrix} e \\ 0 \end{pmatrix}.$$

In der Übung werden Sie Nachrechnen, dass ein Punkt $x \in \mathbb{R}^2$ genau dann auf $E(a_1,a_2)$ liegt, wenn er der *Brennpunktgleichung*

$$d(x,f_-) + d(x,f_+) = 2a_1$$

genügt. In Worten: Die Ellipse $E(a_1,a_2)$ ist die Menge aller Punkte, für die die Summe der Abstände zu den Brennpunkten konstant gleich $2a_1$ ist.

Ist $E(a_1,a_2)$ ein Kreis (also $a_1 = a_2$), so gilt $e = 0$ und die Brennpunkte fallen im Ursprung zusammen. In diesem Fall hat E keine bevorzugte Hauptachse (alle Achsen durch den Ursprung sind Symmetrieachsen). Wir nehmen daher jetzt an, dass $E(a_1,a_2)$ eine echte Ellipse ist. Die Gerade $\mathbb{R}e_1$ durch die beiden Brennpunkte heißt dann die *Brennachse* von $E(a_1,a_2)$ und die Mittelsenkrechte $\mathbb{R}e_2$ der Brennpunkte heißt die *Nebenachse*. Beide Hauptachsen schneiden sich im *Mittelpunkt* von f_- und f_+ (dem Koordinatenursprung). Beide Hauptachsen schneiden die Ellipse in je zwei Punkten, und deren Abstände zum Mittelpunkt sind genau a_1 (im Fall der Brennachse) bzw. a_2 (im Fall der Nebenachse).

[4] Die Umkehrfunktion ist nicht stetig, da das Bild der kompakten Menge $E(a_1,a_2)$ unter einer stetigen Funktion kompakt sein muss und daher kein halboffenes Intervall sein kann.

[27.06.24]

Bemerkung 9.2.6 (Beschreibung allgemeiner Ellipsen)**.** Nach Definition ist eine Quadrik E genau dann eine Ellipse, wenn eine Modellellipse $E(a_1,a_2)$ mit $a_1 > a_2 > 0$ und eine euklidische Bewegung $f : \mathbb{R}^2 \to \mathbb{R}^2$ existiert mit $E = f[E(a_1,a_2)]$. Ist $f(x) = Sx + v$ mit $v \in \mathrm{O}_2(\mathbb{R})$ und $v \in \mathbb{R}^2$ so ergeben sich die folgenden drei Beschreibungsmöglichkeiten für E.

1. Beschreibung als Nullstellenmenge

Da E eine Quadrik ist, wird diese durch eine Formel der Bauart

$$x^\top Bx + 2b^\top x + c = 0,$$

beschrieben. Damit eine Ellipse vorliegt, muss B den Rang 2 und die Signatur (2,0) oder (0,2) haben, also positiv oder negativ definit ist. Außerdem muss die erweiterte Matrix B' den Rang 3 haben. Der Klassifikation entnimmt man, dass diese Bedingungen auch schon hinreichen sind, sofern E nicht leer ist.

2. Parametrisierung

Aus der Parametrisierung der Standardellipse ergibt sich für E die Parametrisierung

$$\varphi : [0,2\pi) \to E, \quad t \mapsto S \begin{pmatrix} a_1 \cos(t) \\ a_2 \sin(t) \end{pmatrix} + v.$$

3. Brennpunktbeschreibung

Es seien f_+ und f_- die Bilder der Brennpunkte von $E(a_1,a_2)$ unter f und es sei $a := 2a_1$. Da f Abstände erhält gilt dann

$$E = E_{f_-,f_+,a} = \{x \in \mathbb{R}^2 \mid d(x,f_-) + d(x,f_+) = a\}.$$

Wir nennen dann $f_\pm$ die Brennpunkte von E; fallen diese zusammen, so ist E ein Kreis. Andernfalls nennen wir die Verbindungsgerade bzw. Mittelsenkrechte der Brennpunkte die *Brennachse* bzw. *Nebenachse*. Diese beiden Hauptachsen schneiden sich wieder im Mittelpunkt der Ellipse, und ihre Schnittpunkte mit der Ellipse haben vom Mittelpunkt die Abstände a_1 (im Fall der Brennachse) bzw. a_2 (im Fall der Nebenachse).

Übung 9.2.7. Wir haben gesehen, dass jede Ellipse euklidisch äquivalent zu einer Menge der Form $E_{f_-,f_+,a}$ mit $f_\pm \in \mathbb{R}^2$ und $a > 0$ ist. Zeigen Sie umgekehrt, dass jede solche Menge eine Ellipse ist. Die Ellipsen sind also genau die Kurven, die durch Brennpunktgleichungen beschrieben werden können.

Bemerkung 9.2.8 (Gärtnerkonstruktion)**.** Wie legt ein Gärtner ein elliptisches Blumenbeet an? Er schlägt zunächst zwei Pflöcke in die Brennpunkte seines Blumenbeets. Anschließend bindet er die Enden eines Seils (der Länge $2a_1$) an den beiden Pflöcken fest. Er spannt nun eine Schaufel in das Seil ein und zieht dieses mit der Schaufel stramm. Er zieht nun mit der Schaufel im Boden eine Linie, wobei er darauf achtet, dass das Seil von der Schaufel stets straff gespannt wird. Die sich ergebende Linie ist dann eine Ellipse - warum?

Mittels Hauptachsentransformation kann man leicht die Hauptachsen und Hauptlängen einer Ellipse sowie eine Parametrisierung finden:

Beispiel 9.2.9 (Hauptachsenbestimmung)**.** In Beispiel 9.1.20 haben wir gesehen, dass die Quadrik

$$E := \{x \in \mathbb{R}^2 \mid 36x_1^2 + 29x_2^2 + 24x_1x_2 - 180 = 0\} \subseteq \mathbb{R}^2.$$

euklidisch äquivalent zur Standardellipse $E(3,2)$ ist. Genauer haben wir gesehen, dass die Bewegung

$$f : \mathbb{R}^2 \to \mathbb{R}^2, x \mapsto \frac{1}{5}\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix} x$$

die Standardellipse $E(3,2)$ auf E abbildet.

Wegen $\sqrt{3^2-2^2} = \sqrt{5}$ sind die Brennpunkte von E gegeben durch

$$f_- = f\begin{pmatrix} -\sqrt{5} \\ 0 \end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix} -3 \\ 4 \end{pmatrix} \quad \text{und} \quad f_+ = f\begin{pmatrix} \sqrt{5} \\ 0 \end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix} 3 \\ -4 \end{pmatrix},$$

und ihr Mittelpunkt ist $f(0) = 0$. Die Ellipse E ist also in Brennpunktsform gegeben durch

$$E = \left\{x \in \mathbb{R}^2 \mid d\left(x, \frac{1}{\sqrt{5}}\begin{pmatrix} -3 \\ 4 \end{pmatrix}\right) + d\left(x, \frac{1}{\sqrt{5}}\begin{pmatrix} 3 \\ -4 \end{pmatrix}\right) = 6\right\}.$$

Die Brennachse und Nebenachse sind gegeben durch

$$f[\mathbb{R}e_1] = \left\{\begin{pmatrix} 3x \\ -4x \end{pmatrix} \mid x \in \mathbb{R}\right\} \quad \text{und} \quad f[\mathbb{R}e_2] = \left\{\begin{pmatrix} 4x \\ 3x \end{pmatrix} \mid x \in \mathbb{R}\right\}.$$

Eine Parametrisierung der Ellipse ist gegeben durch

$$\varphi : [0, 2\pi) \to E, \quad t \mapsto \frac{1}{5}\begin{pmatrix} 9\cos(t) + 8\sin(t) \\ -12\cos(t) + 6\sin(t) \end{pmatrix}.$$

Bemerkung 9.2.10 (Beschreibungen der Modellhyperbel)**.** In Analogie mit dem elliptischen Fall diskutieren wir nun drei Beschreibungen der Modellhyperbel

$$H(a_1, a_2) := Q^{II}(1,1,a_1,a_2).$$

1. Beschreibung als Nullstellenmenge

Nach Definition ist $H(a_1,a_2)$ die Menge aller $x \in \mathbb{R}^2$, die der Gleichung

$$\left(\frac{x_1}{a_1}\right)^2 - \left(\frac{x_2}{a_2}\right)^2 = 1$$

genügen. Ist $x \in H(a_1,a_2)$ mit $x_1 > 0$ und $x_2 > 0$, so gilt

$$x_2 = \frac{a_2}{a_1}\sqrt{x_1^2 - a_1^2} \implies \frac{x_2}{a_2/a_1 x_1} = \sqrt{1 - a_1/x_1^2} \xrightarrow{x_1 \to \infty} 1,$$

und daher $x_2 \approx \frac{a_2}{a_1}x_1$. Dieselbe Näherung gilt auch, wenn $x_1 < 0$ und $x_2 < 0$ betragsmäßig groß-sind. Haben x_1 und x_2 hingegen unterschiedliche Vorzeichen und sind betragsmäßig groß, so gilt stattdessen $x_2 \approx -\frac{a_2}{a_1}x_1$. Die Geraden

$$A_\pm(a_1,a_2) := \left\{x \in \mathbb{R}^2 \mid x_2 = \pm\frac{a_2}{a_1}x_1\right\}$$

sind daher *Asymptoten* an $H(a_1,a_2)$.

2. PARAMETRISIERUNG

H ist die disjunkte Vereinigung zweier Äste $H^+(a_1,a_2)$ und $H^-(a_1,a_2)$, die durch

$$\varphi_\pm : \mathbb{R} \to H^\pm, \quad t \mapsto S \begin{pmatrix} \pm a_1 \cosh(t) \\ a_2 \sinh(t) \end{pmatrix} + v$$

parametrisiert werden. Insbesondere ist H unbeschränkt, nicht-kompakt und unzusammenhängend.

3. BRENNPUNKTBESCHREIBUNG

Es sei $e := \sqrt{a_1^2 + a_2^2}$ - man beachte den Vorzeichenunterschied zum elliptischen Fall! Wir definieren die *Brennpunkte* $f_\pm$ durch

$$f_- := \begin{pmatrix} -e \\ 0 \end{pmatrix} \quad \text{und} \quad f_+ := \begin{pmatrix} e \\ 0 \end{pmatrix}.$$

In den Übungen werden Sie zeigen, dass die Punkte auf H^- bzw. H^+ durch die Brennpunktgleichungen

$$d(x,f_-) - d(x,f_+) = -2a_1 \quad \text{bzw.} \quad d(x,f_-) - d(x,f_+) = 2a_1$$

charakterisiert sind, d.h. es gilt

$$H^\pm(a_1,a_2) = \{x \in \mathbb{R}^2 \mid d(x,f_-) - d(x,f_+) = \pm 2a_1\}.$$

Die Gerade $\mathbb{R}e_1$ durch die beiden Brennpunkte heißt wie im elliptischen Fall die *Brennachse* von $H(a_1,a_2)$ und die Mittelsenkrechte $\mathbb{R}e_2$ der Brennpunkte heißt die *Nebenachse*. Diese beiden Hauptachsen sind Symmetrieachsen der Hyperbel, aber anders als im Fall der Ellipse schneidet nur die Brennachse die Hyperbel (je einmal in jedem der beiden Äste), und der Abstand der beiden Schnittpunkte zum *Mittelpunkt* von f_- und f_+ (dem Koordinatenursprung, der auch Schnittpunkt der beiden Hauptachsen ist) ist $2a_1$.

Die Variable a_2 hat keine eigenständige geometrische Bedeutung, aber sie bestimmt mit, wie stark die Hyperbeläste gebogen sind. Die relevantere Größe ist das *Verhältnis* a_2/a_1, denn $\pm a_2/a_1$ sind die Steigungen der Asymptoten. Genau im Fall $a_1 = a_2$ stehen die Asymptoten senkrecht aufeinander.

Bemerkung 9.2.11 (Beschreibung allgemeiner Hyperbeln)**.** Nach Definition ist eine Quadrik H genau dann eine Hyperbel, wenn eine Modellhyperbel $H(a_1,a_2)$ und eine euklidische Bewegung $f : \mathbb{R}^2 \to \mathbb{R}^2$ existiert mit $H = f[H(a_1,a_2)]$. Ist $f(x) = Sx + v$ mit $S \in \mathrm{O}_2(\mathbb{R})$ und $v \in \mathbb{R}^2$ so ergeben sich die folgenden drei Beschreibungsmöglichkeiten für H.

1. BESCHREIBUNG ALS NULLSTELLENMENGE

Da H eine Quadrik ist, wird diese durch eine Formel der Bauart

$$x^\top B x + 2b^\top x + c = 0,$$

beschrieben. Damit eine Hyperbel vorliegt, muss B den Rang 2 und die Signatur (1,1) haben, also invertierbar und indefinit ist. Außerdem muss die erweiterte Matrix B' den Rang 3 haben. Der Klassifikation entnimmt man, dass diese Bedingungen auch schon hinreichend sind. Die Asymptoten von H ergeben sich als die Bilder der Asymptoten von $H(a_1,a_2)$ unter f. Diese besitzen die Steigungen $\pm a_2/a_1$.

2. PARAMETRISIERUNG

Aus der Parametrisierung der Standardhyperbel ergeben sich für die Äste H^+ und H^- von H die Parametrisierungen

$$\varphi_\pm : \mathbb{R} \to H^\pm, \quad t \mapsto S \begin{pmatrix} \pm a_1 \cosh(t) \\ a_2 \sinh(t) \end{pmatrix} + v$$

3. BRENNPUNKTBESCHREIBUNG

Es seien f_+ und f_- die Bilder der Brennpunkte von $H(a_1, a_2)$ unter f und es sei $a := 2a_1$. Da f Abstände erhält gilt dann

$$H^\pm = H^\pm_{f_-, f_+, a} = \{x \in \mathbb{R}^2 \mid d(x, f_-) - d(x, f_+) = \pm a\}.$$

Umgekehrt definiert jede solche Brennpunktgleichung eine Hyperbel (vgl. die Übungen). Wir nennen $f_\pm$ die Brennpunkte von H und die Verbindungsgerade bzw. Mittelsenkrechte der Brennpunkte die *Brennachse* bzw. *Nebenachse*. Diese beiden Hauptachsen schneiden sich wieder im Mittelpunkt der Hyperbel. Die Brennachse schneidet die Hyperbeläste in je einem Punkt mit Abstand a vom Mittelpunkt, die Nebenachse schneidet die Hyperbel nicht.

Beispiel 9.2.12 (Hauptachsen einer Hyperbel)**.** In Beispiel 9.1.21 haben wir gesehen, dass die Quadrik

$$H := \{x \in \mathbb{R}^2 \mid x_1 x_2 + \sqrt{2} x_1 + 1 = 0\}$$

eine Hyperbel ist. Weiter haben wir gesehen, dass

$$H = f[H(\sqrt{2}, \sqrt{2})], \quad \text{wobei} \quad f(x) = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} x - \begin{pmatrix} 0 \\ \sqrt{2} \end{pmatrix}.$$

Wegen $\sqrt{\sqrt{2}^2 + \sqrt{2}^2} = 2$ sind die Brennpunkte von H gegeben durch

$$f_- = f\begin{pmatrix} -2 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{2} \\ -2\sqrt{2} \end{pmatrix} \quad \text{und} \quad f_+ = f\begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -\sqrt{2} \\ 0 \end{pmatrix},$$

und ihr Mittelpunkt ist $f(0) = \begin{pmatrix} 0 \\ \sqrt{2} \end{pmatrix}$. Die beiden Äste der Hyperbel sind also gegeben durch

$$H^\pm := \left\{ x \in \mathbb{R}^2 \mid d\left(x, \begin{pmatrix} \sqrt{2} \\ -2\sqrt{2} \end{pmatrix}\right) - d\left(x, \begin{pmatrix} -\sqrt{2} \\ 0 \end{pmatrix}\right) = \pm 2\sqrt{2} \right\}.$$

Die Brennachse ist

$$f[\mathbb{R}e_1] = \left\{ \begin{pmatrix} -x \\ x - \sqrt{2} \end{pmatrix} \mid x \in \mathbb{R} \right\},$$

und die Nebenachse ist

$$f[\mathbb{R}e_2] = \left\{ \begin{pmatrix} x \\ x - \sqrt{2} \end{pmatrix} \mid x \in \mathbb{R} \right\}.$$

Parametrisierungen der beiden Hyperbeläste sind gegeben durch

$$\varphi_\pm : \mathbb{R} \to H^\pm, \quad t \mapsto \begin{pmatrix} \mp \cosh(t) + \sinh(t) \\ \pm \cosh(t) + \sinh(t) - \sqrt{2} \end{pmatrix}.$$

□

Bemerkung 9.2.13 (Beschreibungen der Modellparabel)**.** Wir betrachten drei Beschreibungen der *Modellparabel* $P(a_1) := Q^{III}(1,0,a_1)$.

1. Beschreibung als Nullstellenmenge

Nach Definition ist $P(a_1)$ die Menge aller $x \in \mathbb{R}^2$, die der Gleichung

$$\left(\frac{x_1}{a_1}\right)^2 - x_2 = 0 \quad (a_1 > 0)$$

genügen. Die Parabel besitzt die *Symmetrieachse* $\mathbb{R}e_2$, die die Parabel im *Scheitelpunkt* (dem Koordinatenursprung) schneidet. Die Tangente an die Parabel im Scheitelpunkt ist die *Tangentialachse* $\mathbb{R}e_1$.

2. Parametrisierung

Anders als im Fall von Hyperbel und Ellipse ist diese Quadrik ein Funktionsgraph, nämlich der Graph der Funktion[5]

$$f_{a_1} : \mathbb{R} \to \mathbb{R}, \quad f_{a_1}(x_1) = \left(\frac{x_1}{a_1}\right)^2.$$

Daraus folgt insbesondere, dass eine Parametrisierung durch die Formel

$$\varphi : \mathbb{R} \to P(a_1), \quad t \mapsto \begin{pmatrix} t \\ (t/a_1)^2 \end{pmatrix}$$

gegeben ist.

3. Brennpunktbeschreibung

Anders als im hyperbolischen und elliptischen Fall, lässt sich die Parabel nicht Mittels zweier Brennpunkte, sondern mittels eines Brennpunkts und einer sogenannten Leitgerade beschreiben. Wir setzen $e := a_1^2/4$ und definieren den *Brennpunkt* f_+ von $P(a_1)$ durch

$$f_+ := \begin{pmatrix} 0 \\ e \end{pmatrix}$$

und die zugehörige *Leitgerade* ℓ_- durch

$$\ell_- := \left\{ \begin{pmatrix} t \\ -e \end{pmatrix} \mid t \in b\mathbb{R} \right\}$$

Wir behaupten, dass dann die Punkte von $P(a_1)$ gerade durch die Gleichung

$$d(x, f_+) = \operatorname{dist}(x, \ell_-) := \inf\{d(x,y) \mid y \in \ell_-\} \tag{9.2.1}$$

charakterisiert werden. Zum Beweis erinnern wir uns daran, dass der Abstand eines Punktes von einer Ursrpungsgerade durch den Abstand des Punktes von der Orthogonalprojektion auf diese Gerade realisiert wird. Da sich Abstände unter Translationen nicht ändern, gilt die analoge Aussage auch für affine Geraden. Die Orthogonalprojektion von x auf ℓ_- ist nun gerade durch $\pi(x) = \begin{pmatrix} x_1 \\ -e \end{pmatrix}$ gegeben. Wir erhalten daher

$$\operatorname{dist}(x, \ell_-) = d\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} x_1 \\ -e \end{pmatrix}\right) = \sqrt{0^2 + (x_2 + e)^2} = x_2 + e.$$

[5] Da es sich um eine quadratische Funktion handelt, sollte man eigentlich genauer von einer *quadratischen* Parabel sprechen.

Folglich gelten die Äquivalenzen:

$$\begin{aligned} d(x,f_+) = \operatorname{dist}(x,\ell_-) &\iff d\left(\begin{pmatrix}x_1\\x_2\end{pmatrix},\begin{pmatrix}0\\e\end{pmatrix}\right) = x_2+e \\ &\iff \sqrt{x_1^2+(x_2-e)^2} = x_2+e \iff x_1^2+x_2^2-2ex_2+e^2 = x_2^2+2ex_2+e^2 \\ &\iff x_1^2 = 4ex_2 = a_1^2x_2 \iff (x_1/a_1)^2 = x_2 \iff x\in P(a_1). \end{aligned}$$

Bemerkung 9.2.14 (Beschreibung allgemeiner Parabeln)**.** Nach Definition ist eine Quadrik P genau dann eine Hyperbel, wenn eine Modellhyperbel $P(a_1)$ und eine euklidische Bewegung $f:\mathbb{R}^2\to\mathbb{R}^2$ existiert mit $P = f[P(a_1)]$. Ist $f(x) = Sx+v$ mit $S\in \mathrm{O}_2(\mathbb{R})$ und $v\in\mathbb{R}^2$ so ergeben sich die folgenden drei Beschreibungsmöglichkeiten für H.

1. Beschreibung als Nullstellenmenge

Da P eine Quadrik ist, wird diese durch eine Formel der Bauart

$$x^\top Bx + 2b^\top x + c = 0,$$

beschrieben. Damit eine Hyperbel vorliegt, muss B den Rang 1 haben, also singulär und nicht 0 sein. Außerdem muss die erweiterte Matrix B' den Rang 2 haben. Diese Bedingungen sind allerdings noch nicht hinreichend, denn sie gelten auch für zwei parallele affine Geraden. Man benötigt daher eine Zusatzbedingung, z.B. dass P zusammenhängend ist. *Symmetrieachse*, *Scheitelpunkt* und *Tangentialachse* von P ergeben sich als Bilder von Symmetrieachse, Scheitelpunkt und Tangentialachse der entsprechenden Modellparabel unter f.

2. Parametrisierung

Aus der Parametrisierung der Standardparabel ergibt sich für P die Parametrisierung

$$\varphi:\mathbb{R}\to P,\quad t\mapsto S\begin{pmatrix}t\\(t/a_1)^2\end{pmatrix}+v$$

3. Brennpunktbeschreibung

Es seien f_+ und ℓ_- die Bilder des Brennpunkts bzw. der Leitgerade von $P(a_1)$ unter f. Wir nennen diese wieder den *Brennpunkt* bzw. die *Leitgerade* von P. Da f Abstände erhält gilt dann

$$P = P_{\ell_-,f_+} = \{x\in\mathbb{R}^2 \mid d(x,f_+) = \operatorname{dist}(x,\ell_-)\}.$$

Ist umgekehrt ℓ_- eine Gerade und f_+ ein Punkt außerhalb von ℓ_-, so ist P_{ℓ_-,f_+} eine Parabel: Durch eine Drehung kann man erreichen, dass die Gerade parallel zur e_1-Achse liegt, und durch eine Verschiebung kann man zusätzlich erreichen, dass der Brennpunkt auf der e_2-Achse liegt und vom Ursprung denselben Abstand e hat wie die Gerade. Dann sind wir aber genau im Fall der Standardparabel - der Abstand vom Punkt zur Geraden ist dann genau $2e = a_1^2/2$.

Bemerkung 9.2.15 (Analogie zwischen Ellipsen, Hyperbeln und Parabeln)**.** Auch wenn wir Ellipsen, Hyperbeln und Parabeln als Quadriken definiert haben, so lassen sie sich doch auch direkter geometrisch beschreiben:

- Eine Ellipse ist die Menge aller Punkte der Ebene, für die die Summe der Abstände zu zwei gegebenen Punkten (den Brennpunkten) durch eine gewisse Konstante gegeben ist.

- Eine Hyperbel ist die Menge aller Punkte der Ebene, für die die Differenz der Abstände zu zwei gegebenen Punkten (den Brennpunkten) durch eine gewisse Konstante gegeben ist.
- Eine (quadratische) Parabel ist die Menge aller Punkte der Ebene, die von einem gegebenen Punkt (dem Brennpunkt) und einer gegebenen Geraden (der Leitgeraden) denselben Abstand haben.

In Analogie zur Gärtnerkonstruktion der Ellipse gibt es auch für die Hyperbel und Parabel sogenannte Fadenkonstruktionen, die es erlauben eine Hyperbel bzw. Parabel mittels einer Schnur und einem Lineal (bzw. einem Geodreieck) zu zeichnen. Mehr dazu in den Übungen.

9.2.2 Räumliche Quadriken

Wir haben gesehen, dass es in der Ebene bis auf affine Äquivalenz nur drei nicht-ausgeartete Quadriken gibt. In höheren Dimensionen gibt es deutlich mehr Beispiele, selbst in Dimension 3 gibt es bereits 9 solche Beispiele. Um nicht den Überblick zu verlieren, sortieren wir zunächst diejenigen Quadriken aus, die aus Quadriken niedriger Dimension durch Produktbildung mit einem affinen Unterraum entstehen:

Bemerkung 9.2.16 (Zylinderquadriken)**.** Wir betrachten eine allgemeine Modellquadrik $Q = Q^{\alpha}(r_+, r_-, a_1, \ldots, a_r)$ im $\mathbb{R}^n$. Falls $\alpha \in \{I, II\}$, so setzen wir $k := r$, falls $\alpha = III$, so setzen wir $k := r+1$. Wir nehmen nun an, dass $k < n$ gilt. Das bedeutet, dass die Variablen $x_{k+1}, \ldots, x_n$ in der definierenden Formel für Q gar nicht autauchen. Definieren wir Q_o als die Quadrik in $\mathbb{R}^k$, die durch dieselbe Gleichung wie Q definiert wird, so ist daher die Abbildung

$$Q_o \times \mathbb{R}^{n-k} \to Q, \quad (x, y) \mapsto (x_1, \ldots, x_k, y_1, \ldots, y_{n-k})^\top$$

eine Bijektion. Wir nennen dan Q eine *Zylinderquadrik* und genauer gesagt einen *Zylinder* über Q_o. Nach unserer Konvention ist auch die leere Quadrik eine Zylinderquadrik, nämlich ein Zylinder über der leeren Quadrik. Man beachte, dass eine Zylinderquadrik über einer ausgearteten Quadrik wieder ausgeartet ist, da ein Produkt affiner Unterräume wieder ein affiner Unterraum ist.

Beispiel 9.2.17 (Zylinderquadriken in Dimensionen 2 und 3)**.** In Dimension 1 gibt es nur drei affine Äquivalenzklassen von Quadriken, nämlich die leere Quadrik, die einpunktige Quadrik und die zweipunktige Quadrik. Daher gibt es in Dimension 2 genau drei Zylinderquadriken, die leere Quadrik, die affine Gerade und zwei parallele Geraden. Alle ebenen Zylinderquadriken sind ausgeartet.

In Dimension 2 gibt es 3 nicht-ausgeartete und 6 ausgeartete Quadriken, also gibt es in Dimension 2 genau 9 Zylinderquadriken. Die drei nicht-ausgearteten Zylinderquadriken sind der *elliptische, der hyperbolische und der parabolische Zylinder*.

Wir betrachten nun die räumlichen Quadriken $Q \subseteq \mathbb{R}^3$, die keine Zylinderquadriken sind.

Notation 9.2.18. Es sei also $p = p(B') = p(B, b, c) \in \mathbb{R}[X_1, X_2, X_3]$ ein Polynom vom Grad 2, so dass die zugehörige *räumliche Quadrik* $Q = V(p) \subseteq \mathbb{R}^3$ keine Zylinderquadrik ist. Es seien r' und r die Ränge von B' bzw. B und es sei (r_+, r_-) die Signatur von Q. Die Annahme, dass Q keine Zylinderquadrik ist bedeutet gerade, dass r maximal ist (also $r = 3$ im Typ I und II und $r = 2$ im Typ III). Es gilt dann also

$$r = r_+ + r_- \in \{2, 3\} \quad \text{und} \quad r' \in \{r, r+1, r+2\}.$$

Bis auf euklidische Äquivalenz gibt es die folgenden Möglichkeiten für Q:

Beispiel 9.2.19 (Räumliche Kegelquadriken)**.** Im Fall I muss $r' = r = 3$ und (nach unserer Konvention) $r_+ \geq r_-$. Wir erhalten die folgenden Fälle:

r'	r	(r_+, r_-)	Gleichung der Modellquadrik	Name der Quadrik
3	3	(3,0)	$(x_1/a_1)^2 + (x_2/a_2)^2 + (x_3/a_3)^2 = 0$	Punkt
3	3	(2,1)	$(x_1/a_1)^2 + (x_2/a_2)^2 - (x_3/a_3)^2 = 0$	Doppelkegel

Hier finden wir nun endlich das für diese Klasse von Quadriken namensgebende Beispiel. (Man beachte, dass es sich beim Doppelkegel um die kleinste *nicht-ausgeartete* Kegelquadrik handelt.)

Beispiel 9.2.20 (Ebene Mittelpunktsquadriken)**.** Im Fall II ist $r' = r + 1 = 4$. Wir erhalten die folgenden Fälle

r'	r	(r_+, r_-)	Gleichung der Modellquadrik	Name der Quadrik
4	3	(3,0)	$(x_1/a_1)^2 + (x_2/a_2)^2 + (x_3/a_3)^2 = 1$	Ellipsoid
4	3	(3,1)	$(x_1/a_1)^2 + (x_2/a_2)^2 - (x_3/a_3)^2 = 1$	einschaliges Hyperboloid
4	3	(1,2)	$(x_1/a_1)^2 - (x_2/a_2)^2 - (x_3/a_3)^2 = 1$	zweischaliges Hyperboloid
4	3	(0,3)	$-(x_1/a_1)^2 - (x_2/a_2)^2 - (x_3/a_3)^2 = 1$	leere Menge

Beispiel 9.2.21 (Ebene parabolische Quadriken)**.** Im Fall III ist $r' = r + 2 = 4$. Wir erhalten die folgenden Fälle:

r'	r	(r_+, r_-)	Gleichung der Modellquadrik	Name der Quadrik
4	2	(2,0)	$(x_1/a_1)^2 + (x_2/a_2)^2 = x_3$	elliptisches Paraboloid
4	2	(1,1)	$(x_1/a_1)^2 - (x_2/a_2)^2 = x_3$	hyperbolisches Paraboloid

Damit haben wir insgesamt gezeigt:

Satz 9.2.22 (Klassifikation räumlicher Quadriken)**.** *Es gibt* 15 *affine Äquivalenzklassen von räumlichen Quadriken, davon* 9 *nicht-ausgeartete (Doppelkegel, Ellipsoid, einschaliges Hyperboloid, zweischaliges Hyperboloid, elliptisches Paraboloid, hyperbolisches Paraboloid, elliptisches Zylinder, hyperbolischer Zylinder, parabolischer Zylinder) und* 6 *ausgeartete (leere Quadrik, einpunktige Quadrik, affine Gerade, affine Ebene, Paar sich schneidender affiner Ebenen, Paar paralleler affiner Ebenen).* □

Beispiel 9.2.23. Wir betrachten die Quadrik $K \subseteq \mathbb{R}^3$ gegeben durch

$$K = \{x \in \mathbb{R}^3 \mid x_1^2 - 2x_1x_2 - 2x_1x_3 + x_2^2 - 2x_2x_3 + x_3^2 + 2x_1 + 2x_2 + 2x_3 - 3 = 0\}.$$

Es gilt $K = Q(B, b, c)$ mit

$$B := \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}, \quad b := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad c := -3.$$

Wir wollen den Typ der Quadrik K bestimmen sowie eine euklidische Bewegung finden, die K auf die entsprechende Modellquadrik abbildet.

Zunächst diagonalisieren wir die Matrix B orthogonal: Das charakteristische Polynom von B ist

$$\chi_B(X) = \det\begin{pmatrix} X-1 & 1 & 1 \\ 1 & X-1 & 1 \\ 1 & 1 & X-1 \end{pmatrix} = (X-1)^3 + 1 + 1 - (X-1) - (X-1) - (X-1)$$

Eine kurze Rechnung zeigt, dass

$$\chi_B(X) = X^3 - 3X^2 + 3X - 1 + 2 - 3X + 3 = X^3 - 3X^2 + 4 = (X-2)^2(X+1),$$

und folglich $\operatorname{spec}(B) = \{2, -1\}$. Die entsprechenden Eigenräume V_2 und V_{-1} sind gegeben durch

$$V_2 = \ker\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \ker\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix} \right\rangle$$

$$V_{-1} = \ker\begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix} = \ker\begin{pmatrix} 1 & 1 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle.$$

Die Basisvektoren sind bereits orthogonal und müssen nur noch normalisiert werden. Es gilt daher

$$B = S \cdot \operatorname{diag}(2,2,-1) \cdot S^\top, \quad \text{wobei } S = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{pmatrix} \text{ und } S^\top b = \begin{pmatrix} 0 \\ 0 \\ \sqrt{3} \end{pmatrix}.$$

Ist also $f_1 := f_{S,0}$, so gilt

$$f_1^{-1}[K] = \{x \in \mathbb{R}^3 \mid 2x_1^2 + 2x_2^2 - x_3^2 + 2\sqrt{3}x_3 - 3 = 0\}.$$

Nun ist aber $-x_3^2 + 2\sqrt{3}x_3 - 3 = -(x_3 - \sqrt{3})^2$. Ist also $v := (0,0,-\sqrt{3})^\top$ und f_2 die Verschiebung um v, so gilt

$$f_2[f_1^{-1}[K]] = \left\{ z \in \mathbb{R}^3 \mid \left(\frac{z_1}{\sqrt{2}^{-1}}\right)^2 + \left(\frac{z_2}{\sqrt{2}^{-1}}\right)^2 - z_3^2 = 0 \right\} = Q^I(2,1,\sqrt{2}^{-1},\sqrt{2}^{-1},1)$$

Es handelt sich bei der Quadrik K also um einen Doppelkegel. Die euklidische Bewegung $f := f_2 \circ f_1^{-1}$ transformiert diesen Doppelkegel auf Normalform, und umgekehrt gilt

$$K = f^{-1}\left[Q^I(2,1,\sqrt{2}^{-1},\sqrt{2}^{-1},1)\right], \quad \text{wobei } f^{-1}(x) = Sx - Sv = Sx + (1,1,1)^\top.$$

Die Spitze des Kegels K ist also der Punkt $(1,1,1)^\top$.

Zusammenfassung von Abschnitt 9.2.

(1) Die nicht-ausgearteten ebenen Quadriken sind Ellipsen, Hyperbeln und Parabeln.

(2) Nicht-ausgeartete ebene Quadriken lassen sich mit Hilfe ihrer Brennpunktgleichungen beschreiben.

(3) Spezielle Punkte und Achsen (z.B. Brennpunkte, Symmetrieachsen, Tangenten, Asymptoten) sowie Parametrisierungen der nicht-ausgearteten ebenen Quadriken lassen sich bestimmen, indem man die Quadrik mittels Hauptachsentransformation auf eine Modellquadrik zurückführt.

(4) Die nicht-ausgearteten Quadriken im dreidimensionalen Raum sind der Doppelkegel, das Ellipsoid, das einschalige und das zweischalige Hyperboloid, das elliptische und das hyperbolische Paraboloid, sowie der elliptische, hyperbolische und parabolischer Zylinder.

[03.07.24]

9.3 Ebene Schnitte räumlicher Quadriken

Eine Möglichkeit sich höherdimensionalen Quadriken zu nähern ist mittels Schnitten mit affinen Unterräumen kleinerer Dimension.

Definition 9.3.1. Es sei $A \subseteq \mathbb{R}^n$ ein affiner Unterraum und $Q \subseteq \mathbb{R}^n$ eine Quadrik. Die Teilmenge $A \cap Q \subseteq A$ heißt dann ein *affiner Schnitt* von Q.

Wir wollen uns nun klarmachen, in welchen Sinne affine Schnitte von Quadriken selbst wieder Quadriken (von niedrigerer Dimension) sind. Dazu überlegen wir uns zunächst, wie wir affine Unterräume euklidisch mit dem Standardraum der entsprechenden Dimension identifizieren können.

Definition 9.3.2. Es sei $A \subseteq \mathbb{R}^n$ ein affiner Unterraum der Dimension k. Eine bijektive Abbildung $\varphi : A \to \mathbb{R}^k$ heißt eine *euklidische Karte* von A, falls eine euklidische Bewegung Φ von $\mathbb{R}^n$ existiert mit

$$\Phi(v) = \begin{pmatrix} \varphi(v) \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{für alle } v \in A.$$

Messen wir Längen und Winkel in A bzw. $\mathbb{R}^k$ bzgl. der Standardskalarprodukte, so sind euklidische Karten nach Definition längen- und winkeltreu.

Proposition 9.3.3 (Euklidische Karten)**.** *Es sei $A \subseteq \mathbb{R}^n$ ein affiner Unterraum der Dimension k.*

(i) Es existiert eine euklidische Karte $\varphi : A \to \mathbb{R}^k$.

(ii) Sind $\varphi_1, \varphi_2 : A \to \mathbb{R}^k$ euklidische Karten, so ist $\varphi_1 \circ \varphi_2^{-1}$ eine euklidische Bewegung von $\mathbb{R}^k$.

Beweis. (i) Wir wählen $v \in A$, so dass $A = v + U$ mit $U := A - A$. Nun wählen wie eine ONB $(v_1, \dots, v_k)$ eine ONB von U und ergänzen diese (mittels Basisergänzungssatz und Gram-Schmidt) zu einer ONB $(v_1, \dots, v_n)$ von $\mathbb{R}^n$. Die Matrix A, deren Spalten durch $v_1, \dots, v_n$ gegeben sind, ist dann orthogonal und es gilt $Ae_j = v_j$ für $j = 1, \dots, n$. Es sei nun Ψ die euklidische Bewegung, die durch $\Psi(x) := Ax + v$ gegeben ist. Es gilt dann

$$\Psi[\langle e_1, \dots, e_k \rangle] = v + \langle Ae_1, \dots, Ae_k \rangle = v + \langle v_1, \dots, v_k \rangle = v + U = A.$$

Definieren wir nun $\Phi := \Psi^{-1}$, so gilt $\Phi[A] = \langle e_1, \dots, e_k \rangle$, und daher definiert Φ eine euklidische Karte φ.

(ii) Entstehen φ_1 und φ_2 als Einschränkungen euklidischer Bewegungen Φ_1 und Φ_2, so ist $\Phi := \Phi_1 \circ \Phi_2^{-1}$ eine euklidische Bewegung, die den Unterraum $\langle e_1, \dots, e_k \rangle$ auf sich selbst abbildet, und daher eine eukldische Bewegung $\varphi = \varphi_1 \circ \varphi_2^{-1}$ von $\mathbb{R}^k$ induziert. □

Proposition 9.3.4 (Affine Schnitte als Quadriken)**.** *Sei $Q \subseteq \mathbb{R}^n$ eine Quadrik, $A \subseteq \mathbb{R}^n$ ein k-dimensionaler affiner Unterraum, der nicht vollständig in Q enthalten ist.*

(i) Ist $\varphi : A \to \mathbb{R}^k$ eine euklidische Karte, so ist $\varphi[A \cap Q] \subseteq \mathbb{R}^k$ eine Quadrik.

(ii) Sind $\varphi_1, \varphi_2 : A \to \mathbb{R}^k$ zwei euklidische Karten, so sind die Quadriken $\varphi_1[A \cap Q]$ und $\varphi_2[A \cap Q]$ euklidisch äquivalent.

Beweis. (i) Es sei φ die Einschränkung der euklidischen Bewegung Φ mit $\Phi[A] = \langle e_1, \ldots, e_k \rangle$. Da Q eine Quadrik ist, ist auch $Q' := \Phi[Q]$ eine Quadrik; es existiert also ein Polynom $p \in \mathbb{R}[X_1, \ldots, X_n]$ mit $Q' = V(p)$. Da Φ bijektiv ist, gilt dann

$$\Phi[A \cap Q] = \Phi[Q] \cap \langle e_1, \ldots, e_k \rangle = \{x \in \mathbb{R}^n \mid p(x) = 0 \text{ und } x_{k+1} = \cdots = x_n = 0\}.$$

Ist nun $p_0 \in \mathbb{R}[X_1, \ldots, X_k]$ das Polynom, das aus p entsteht, in dem man für $X_{k+1}, \ldots, X_n$ jeweils 0 einsetzt, so ist also

$$\varphi[Q \cap A] = \{x \in \mathbb{R}^k \mid p_0(x) = 0\} = V(p_0).$$

Da A nicht in Q enthalten ist, ist p_0 nicht das Nullpolynom, also gilt $0 \leq \deg(p_0) \leq \deg(p) = 2$, also $\deg(p_0) \in \{0,1,2\}$. Ist $\deg(p_0) = 2$, so setzen wir $p_1 := p_0$, ist $\deg(p_0) = 1$, so setzen wir $p_1 := p_0^2$ und ist $\deg(p_0) = 0$, so setzen wir $p_1 := X_1^2 + 1$. Dann ist $\deg(p_1) = 2$ und

$$\varphi[Q \cap A] = V(p_0) = V(p_1).$$

(ii) Wegen $\varphi_1[Q \cap A] = (\varphi_1 \circ \varphi_2^{-1})[\varphi_2[Q \cap A]]$ folgt dies sofort aus Proposition 9.3.3.(ii). □

Aufgrund der Proposition können wir affine Schnitte von Quadriken selbst wieder als Quadriken niedrigerer Dimension (definiert bis auf euklidische Äquivalenz) auffassen, sofern der entsprechende Unterraum nicht in der Quadrik enthalten ist. Im Folgenden interessiert uns speziell der Fall $(k,n) = (2,3)$. Wir sprechen dann von *ebenen Schnitten räumlicher Quadriken*.

Bemerkung 9.3.5 (Parametrisierung affiner Ebenen in $\mathbb{R}^3$)**.** Nach dem Wittschen Fortsetzungssatz existiert für je zwei Unterebenen $U_1, U_2 < \mathbb{R}^3$ eine orthogonale Abbildung Φ des $\mathbb{R}^3$ mit $\Phi[U_1] = U_2$. In dem wir diese Abbildung wenn nötig mit einer Spiegelung an U_2 verketten, können wir sicherstellen, dass $\det(\Phi) = 1$ gilt. Es folgt dann aus dem Satz von der Isometrie-Normalform, dass Φ eine Drehung (möglicherweise die Identität) ist. Folglich können wir jede affine Unterebene im $\mathbb{R}^3$ durch eine orientierungserhaltende euklidische Bewegung auf jede andere affine Unterebene bewegen.

Nehmen wir als Ausgangspunkt die affine Ebene $E_0 = \mathbb{R}^2 \times \{0\} \subseteq \mathbb{R}^3$. Dann erhalten wir jede affine Ebene aus $E_c := E_0 + ce_3$ durch Anwenden einer Drehung. Drehungen in der e_1-e_2-Ebene haben dabei keinen Effekt, da sie E_c als Menge festhalten. Eine interessante Familie von Ebenen in $\mathbb{R}^3$ ist z.B. gegeben durch Drehung in der e_1-e_3-Ebene, also

$$E_{c,\theta} = \left\{ \begin{pmatrix} \cos(\theta) & 0 & -\sin(\theta) \\ 0 & 1 & 0 \\ \sin(\theta) & 0 & \cos(\theta) \end{pmatrix} \left(\begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ c \end{pmatrix} \right) \mid x \in \mathbb{R}^2 \right\} = \left\{ \begin{pmatrix} \cos(\theta)x_1 - \sin(\theta)c \\ x_2 \\ \sin(\theta)x_1 + \cos(\theta)c \end{pmatrix} \mid x \in \mathbb{R}^2 \right\},$$

wobei wir annehmen dürfen, dass $\theta \in [0, \pi)$ gilt. Wir erhalten eine eukldiische Karte $\varphi_{c,\theta}$ für $E_{c,\theta}$ als Umkehrabbildung von

$$\varphi_{c,\theta}^{-1} : \mathbb{R}^2 \to A(c,\theta), \quad x \mapsto \begin{pmatrix} \cos(\theta)x_1 - \sin(\theta)c \\ x_2 \\ \sin(\theta)x_1 + \cos(\theta)c \end{pmatrix}.$$

Beispiel 9.3.6 (Kegelschnitte)**.** Wir betrachen den Kreiskegel

$$K = Q^I(2,1,1,1,1) = \{x \in \mathbb{R}^3 \mid x_1^2 + x_2^2 - x_3^2 = 0\}$$

Ebene Quadriken, die als ebene Schnitte von K realisiert werden können, bezeichnet man als *Kegelschnitte*. Wir betrachten hier speziell die Kegelschnitte, die sich aus den affinen Ebenen $E_{c,\theta}$ mit $c \geq 0$ und $\theta \in [0,\pi)$ ergeben. Es gilt

$$\begin{aligned}
& x \in \varphi_{c,\theta}[K \cap E_{c,\theta}] \quad \iff \quad \varphi_{c,\theta}^{-1}(x) \in K \\
\iff \quad & (\cos(\theta)x_1 - \sin(\theta)c)^2 + x_2^2 - (\sin(\theta)x_1 + \cos(\theta)c)^2 = 0 \\
\iff \quad & \cos^2(\theta)x_1^2 - 2\cos(\theta)\sin(\theta)cx_1 + \sin^2(\theta)c^2 + x_2^2 - \sin^2(\theta)x_1^2 - 2\cos(\theta)\sin(\theta)cx_1 - \cos(\theta)^2c^2 \\
\iff \quad & (\cos^2(\theta) - \sin^2(\theta))x_1^2 - 4cx_1\cos(\theta)\sin(\theta) + x_2^2 = (\cos^2(\theta) - \sin^2(\theta))c^2.
\end{aligned}$$

Wegen $\cos^2(\theta) - \sin^2(\theta) = \cos(2\theta)$ und $2\cos(\theta)\sin(\theta) = \sin(2\theta)$ erhalten wir daher

$$Q_{c,\theta} := \varphi_{c,\theta}[K \cap E_{c,\theta}] = \left\{x \in \mathbb{R}^2 \mid \cos(2\theta)x_1^2 - 2c\sin(2\theta)x_1 + x_2^2 = \cos(2\theta)c^2\right\} \tag{9.3.1}$$

Wir unterscheiden nun verschiedene Fälle:

FALL 1: $c \neq 0$.

Hier drehen wir eine Ebene, die nicht durch die Kegelspitze verläuft („generischer Fall“). Da die Funktion $\cos(2\theta)$ im Intervall $[0,\pi)$ genau die Nullstellen $\pi/4$ und $3\pi/4$ besitzt, empfiehlt es sich, die folgenden Unterfälle zu unterscheiden:

FALL 1A: $c \neq 0$ UND $0 \leq \theta < \pi/4$

In diesem Fall sind sowohl $\cos(2\theta)$ strikt positiv. Wir können daher durch $\cos(2\theta)$ teilen. Definieren wir $x_1' := x_1 - c\tan(2\theta)$, so erhalten wir mittels quadratischer Ergänzung, dass

$$\begin{aligned}
x \in Q_{c,\theta} \quad & \iff \quad x_1^2 - 2c\tan(2\theta)x_1 + \cos(2\theta)^{-1}x_2^2 = c^2 \\
& \iff \quad (x_1 - c\tan(2\theta))^2 - c^2\tan^2(2\theta) + \cos(2\theta)^{-1}x_2^2 = c^2 \\
& \iff \quad (x_1')^2 + \frac{x_2^2}{\cos(2\theta)} = (1 + \tan^2(2\theta))c^2 = \frac{(\cos^2(2\theta) + \sin^2(2\theta))c^2}{\cos^2(2\theta)} = \frac{c^2}{\cos^2(2\theta)} \\
& \iff \quad \left(\frac{x_1'}{a_1}\right)^2 + \left(\frac{x_2}{a_2}\right)^2 = 1, \quad \text{wobei} \quad a_1 := \frac{c}{\cos(2\theta)},\ a_2 := \frac{c}{\sqrt{\cos(2\theta)}}.
\end{aligned}$$

Der Kegelschnitt $K \cap A(c,\theta)$ ist also in diesem Fall eine Ellipse. Beachte, dass

$$\lim_{\theta \to \pi/4} a_1 = \lim_{\theta \to \pi/4} a_2 = \infty.$$

FALL 1B: $c \neq 0$ UND $\theta = \pi/4$

In diesem Grenzfalls gilt wegen $\cos(2\theta) = 0$ und $\sin(2\theta) = 1$, dass

$$x \in Q_{c,\theta} \quad \iff \quad -2cx_1 + x_2^2 = 0.$$

Dies beschreibt eine Parabel.

FALL 1C: $c \neq 0$ UND $\pi/4 < \theta < 3\pi/4$

In diesem Fall ist $\cos(2\theta)$ strikt negativ. Dieselbe Rechnung wie im Fall 1a führt dann auf

$$x \in Q_{c,\theta} \quad \Longleftrightarrow \quad (x_1')^2 + \frac{x_2^2}{\cos(2\theta)} = \frac{c^2}{\cos^2(2\theta)},$$

wobei wiederum $x_1' := x_1 - c\tan(2\theta)$, aber wegen $\cos(2\theta) < 0$ erhalten wir diesmal

$$x \in \varphi_{c,\theta}(K \cap A(c,\theta)) \quad \Longleftrightarrow \quad \left(\frac{x_1}{a_1}\right)^2 - \left(\frac{x_2}{a_2}\right)^2 = 1, \quad \text{wobei} \quad a_1 := \frac{c}{|\cos(2\theta)|},\ a_2 := \frac{c}{\sqrt{|\cos(2\theta)|}}.$$

Der Kegelschnitt $K \cap A(c,\theta)$ ist also in diesem Fall eine Hyperbel. Für $\theta \to 3\pi/4$ gilt wieder $a_1, a_2 \to \infty$.

FALL 1D: $c \neq 0$ UND $\theta = 3\pi/4$

Hier ist nun $\cos(2\theta) = 0$ und $\sin(2\theta) = -1$ und daher gilt

$$x \in Q_{c,\theta} \quad \Longleftrightarrow \quad 2x_1 + x_2^2 = 0.$$

Dies ist wieder eine Parabel (diesmal in die andere Richtung geöffnet).

FALL 1E: $c \neq 0$ UND $3\pi/4 \leq \theta < \pi$

Hier ist nun $\cos(2\theta)$ wieder positiv, und wir erhalten wie im FALL 1A ein Ellipse.

Wir fassen nun FALL1 so zusammen: Verschieben wir die e_1-e_2-Ebene nicht-trivial in e_3-Richtung, so ist der Schnitt mit dem Kegel K zunächst eine Ellipse. Drehen wir die Ebene in der e_1-e_3-Ebene um einen Winkel, der echt kleiner als $\pi/4$ ist, so bleibt der Schnitt eine Ellipse. Drehen wir genau um den Winkel $\pi/4$, so erhalten wir eine Parabel, und drehen wir dann weiter, so erhalten wir eine Hyperbel. Wir sehen also eine geometrische Transition

$$\text{Ellipse} \longrightarrow \text{Parabel} \longrightarrow \text{Hyperbel},$$

wobei die Parabel instabil ist, und nur genau im Übergang von der Ellipse zur Hyperbel auftaucht. Drehen wir nun weiter, so erhalten wir die umgekehrte geometrische Transition

$$\text{Hyperbel} \longrightarrow \text{Parabel} \longrightarrow \text{Ellipse},$$

wobei die Parabel wieder nur genau im Grenzfall $\theta = 3\pi/4$ auftaucht. Für $c \neq 0$ erhalten wir also genau die drei nicht-ausgearteten ebenen Quadriken als Kegelschnitte.

FALL 2: C = 0.

In diesem (degenerierten) Fall vereinfacht sich die definierende Formel für $Q_{c,\theta}$ zu

$$\cos(2\theta)x_1^2 + x_2^2 = 0.$$

Wir unterscheiden nun dieselben Fälle wir zuvor:

FALL 2A: $c = 0$ UND $0 \leq \theta < \pi/4$

Wegen $\cos(2\theta) > 0$ erhalten wir

$$x \in Q_{c,\theta} \quad \Longleftrightarrow \quad x_1^2 + \left(\frac{x_2}{\sqrt{\cos(2\theta)}}\right)^2 = 0,$$

Der Kegelschnitt $K \cap A(c,\theta)$ ist daher einpunktig.

FALL 2B: $c = 0$ UND $\theta = \pi/4$

Wegen $\cos(2\theta) = 0$ erhalten wir den Grenzfall einen einpunktigen Kegelschnitt.

$$x \in Q_{c,\theta} \quad \Longleftrightarrow \quad x_2^2 = 0 \quad \Longleftrightarrow \quad x_2 = 0.$$

$Q_{c,\theta}$ ist also eine Gerade.

FALL 2C: $c = 0$ UND $\pi/4 < \theta < 3\pi/4$:

In diesem Fall gilt $\cos(2\theta) < 0$ und daher

$$x \in Q_{c,\theta} \quad \Longleftrightarrow \quad x_1^2 - \left(\frac{x_2}{\sqrt{|\cos(2\theta)|}}\right)^2 = 0.$$

Der Kegelschnitt $K \cap A(c,\theta)$ ist also ein Paar sich schneidender Geraden.

FALL 2D: $c = 0$ UND $\theta = 3\pi/4$

Wegen $\cos(2\theta) = 0$ erhalten wir wieder

$$x \in Q_{c,\theta} \quad \Longleftrightarrow \quad x_2^2 = 0 \quad \Longleftrightarrow \quad x_2 = 0.$$

$Q_{c,\theta}$ ist also eine Gerade.

FALL 2E: $c = 0$ UND $3\pi/4 < \theta < \pi$

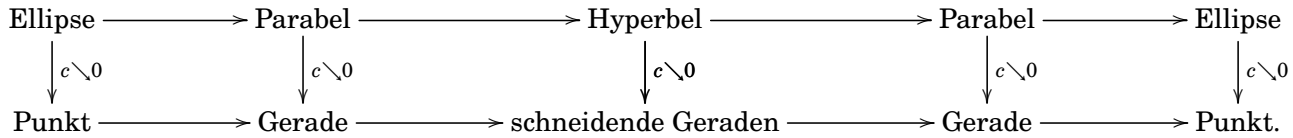
Hier ist $\cos(2\pi)$ wieder positiv, also erhalten wir wie im FALL 2A einen einpunktigen Kegelschnitt.

Wir erhalten insgesamt also in Fall 2 auf dem „Hinweg“eine geometrische Transition der Form

$$\text{Punkt} \longrightarrow \text{Gerade} \longrightarrow \text{Paar schneidender Geraden},$$

und auf dem Rückweg eine geometrische Transition in die umgekehrte Richtung. Wir können also für unsere spezielle Wahl von affinen Hyperebenen nur drei der fünf ausgearteten ebenen Quadriken als Kegelschnitte realisieren; man kann sich überlegen, dass die anderen beiden Typen (die leere Quadrik bzw. Paare paralleler Geraden) sich auch bei anderer Wahl der affinen Hyperebenen nicht realisieren lassen. (Diese beiden Type erhält man allerdings als ebene Schnitte des Kreiszylinders, den man sich als Grenzwert eines Kegels vorstellen kann, wenn die Kegelspitze ins Unendliche wandert.)

Man beachte noch, was passiert, wenn man mit einem positiven c beginnt, und dann c gegen 0 laufen lässt. Man erhält dann eine doppelte Transition



Können Sie alle diese Übergänge vor Ihrem inneren Auge sehen?

Beispiel 9.3.7 (Ellipsoide und Hyperboloide)**.** Schneidet man ein Ellipsoid in $\mathbb{R}^3$ mit einer affinen Ebene, so erhält man entweder die leere Quadrik, einen einzelnen Punkt oder eine Ellipse (die zu einem Kreis ausarten kann). Anders als im Fall von Kegeln wird also nur eine nichtausgeartete Quadrik als affiner Schnitt realisiert.

Im Fall von ein- oder zweischaligen Hyperboloiden erhält man hingegen mitnichten immer eine Hyperbel: Bereits die Schnitte mit den Standard-Koordinatenebenen liefern (je nach Wahl der Koordinatenebene) entweder Ellipsen oder Hyperbeln, und der Grenzfall ist wieder eine Parabel. Statt mit Kegeln könnte man also auch mit Hyperboloiden alle nicht-ausgearteten Kegelschnitte erzeugen. Ein Hyperboloid ist allerdings komplizierter zu beschreiben als ein Kegel.

Die Tatsache, dass sich am Kegel alle drei nicht-ausgearteten ebenen Quadriken realisieren lassen, ist seit der Antike bekannt. Das Studium von Kegelschnitten ist daher ein klassisches Thema der Geometrie, dass bis in die 1980er Jahre an deutschen Gymnasien immer mal wieder zum Abiturstoff gehörte, weswegen man umfangreiche Betrachtungen zu Kegelschnitten z.T. noch in älteren Schulbüchern findet. Der folgende faszinierende Satz über Kegelschnitte wurde von Dandelin[6] im Jahr 1822 entdeckt, und hat zu einer Renaissance der Theorie der Kegelschnitte geführt:

Satz 9.3.8 (Dandelinsche Kugeln)**.** *Es sei K ein Kegel im $\mathbb{R}^3$ und E eine affine Ebene im $\mathbb{R}^3$, die nicht die Spitze von K enthält. Dann ist $E \cap K$ eine Ellipse, Hyperbel oder Parabel, und es gibt es genau zwei Kugeln, die im Innern des Kegels enthalten sind und sowohl E als auch den Kegelmantel tangential berühren. Die Berührpunkte diese Kugeln mit der Ebene sind genau die Brennpunkte der Quadrik $E \cap K$.*

Momentan sind Kegelschnitte etwas aus der Mode geraten, aber gerade angehenden Mathematik-Lehrern sei das Thema nachdrücklich zur Vertiefung empfohlen.

Zusammenfassung von Abschnitt 9.3.

(1) Schnitte von Quadriken mit affinen Unterräumen entsprechen unter euklidischen Karten wieder Quadriken (von entsprechend kleinerer Dimension).

(2) Alle nicht-ausgearteten ebenen Quadriken lassen sich als Kegelschnitte realisieren, wobei die Parabel als Durchgang von der Ellipse zur Hyperbel und umgekehrt auftaucht.

9.4 Affine Quadriken über allgemeinen Körpern

Wir haben bereits gesehen, dass sich affine Quadriken über beliebigen Körpern definieren lassen. Im reellen Fall waren wir besonders daran interessiert, solche Quadriken bis auf euklidische Bewegungen zu klassifizieren - diese Fragestellung ergibt natürlich über allgemeinen Körpern keinen Sinn mehr. Es macht aber sehr wohl Sinn, Quadriken bis auf affine Äquivalenz zu untersuchen (vgl. Definition 9.1.14). Im reellen Fall hatten wir Quadriken zunächst bis auf euklidische Äquivalenz klassifiziert und dann aus dieser Klassifikation die affine Klassifikation abgeleitet. Über allgemeinen Körpern funktioniert das so nicht mehr. Wir wollen uns daher hier noch kurz überlegen, wie man prinizpiell im Fall eines allgemeinen Körpers der Charakteristik $\neq 2$ vorgehen kann.

Notation 9.4.1. Es sei $\mathbb{K}$ ein Körper der Charakteristik $\neq 2$. Ist $B \in \mathbb{K}^{n\times n}$ eine symmetrische Matrix und sind $b \in \mathbb{K}^n$ und $c \in \mathbb{K}$, so schreiben wir $p = p(B,b,c)$ für das Polynom vom Grad ≤ 2

[6] GERMINAL PIERRE DANDELIN (1794-1847), frz. Mathematiker

gegeben durch

$$p(x) = x^\top Bx + 2b^\top x + c.$$

Die zugehörige *erweiterte Matrix* ist wieder

$$B' = \begin{pmatrix} B & b \\ b^\top & c \end{pmatrix} \in \mathbb{K}^{n\times n},$$

und p hat Grad 2 genau dann, wenn $B \neq 0$ gilt. Dies liefert wie im rellen Fall eine Parametrisierung von quadratischen Polynomen durch Matrizen. Wir schreiben dann

$$Q(B') = Q(B,b,c) = V(p)$$

für die zugehörige Quadrik.

Anders als im reellen Fall steht uns über allgemeinen Körpern der Spektralsatz nicht mehr zur Verfügung. Dennoch können wir den folgenen Satz beweisen:

Satz 9.4.2 (Affine Hauptachsentransformation)**.** *Es sei $Q = Q(B,b,c)$ eine Quadrik und es sei $r = \mathrm{rk}(B)$. Dann existieren $\lambda_1,\dots,\lambda_r \in \mathbb{K}^\times$, so dass Q affin äquivalent zu einer der folgenden Modellquadriken ist:*

(Typ I) $Q^I(\lambda_1,\dots,\lambda_r) = \{x \in \mathbb{K}^n \mid \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 = 0\}$.

(Typ II) $Q^{II}(\lambda_1,\dots,\lambda_r) = \{x \in \mathbb{K}^n \mid \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 = 1\}$.

(Typ III) $Q^{III}(\lambda_1,\dots,\lambda_r) = \{x \in \mathbb{K}^n \mid \lambda_1 x_1^2 + \dots + \lambda_r x_r^2 = x_{r+1}\}$.

Beweis. Wir wollen ähnlich wie im euklidischen Fall vorgehen und zunächst den homogenen Teil $p_0(x) = x^\top Bx$ von $p(B,b,c)$ vereinfachen. Die Matrix B definiert auf $V := \mathbb{K}^n$ eine Bilinearform B_V (durch $B_V(x,y) = x^\top By$), und bezeichnet $V^\perp$ das Radikal dieser Bilinearform und W ein beliebiges Komplement von $V^\perp$ in V, so erhalten wir eine orthogonale Zerlegung

$$(V,B_V) = (W,B_W) \perp\!\!\!\perp (V^\perp,0),$$

wobei B_W die Einschränkung von B_V auf $W\times W$ bezeichnet. Da B_W nicht-ausgeartet ist, existiert nach Korollar 7.2.22 eine OGB $\mathscr{B}_W$ von (W,B_W), die wir durch eine beliebige Basis von $V^\perp$ zu einer einer OGB $\mathscr{B}$ von (V,B_V) ergänzen können. (Wir können diese z.B. mittels symmetrischen Gaußbestimmen!)

Ist S die Matrix, deren Spalten durch die Elemente von $\mathscr{B}$ gegeben sind, so folgt, dass $S^\top BS = \mathrm{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$ für gewisse $\lambda_1,\dots,\lambda_r \in \mathbb{K}^\times$, wobei r der Rang von B ist.

Es sei nun $\Phi : \mathbb{K}^n \to \mathbb{K}^n$ die affine (sogar lineare!) Abbildung gegeben durch $\Phi(x) := S^{-1}x$. Es gilt dann

$$z \in \Phi[Q] \iff x := Sz \in Q \iff z^\top S^\top ASz + 2b^\top Sz + c = 0,$$

und daher

$$\Phi[Q] = \{z \in \mathbb{K}^n \mid \lambda_1 z_1^2 + \dots + \lambda_r z_r^2 + 2(S^\top b)^\top z + c = 0\}.$$

Der Rest des Arguments funktioniert nun genau wie im euklidischen Fall: Mittels quadratischer Ergänzung (die über einem beliebigen Körper der Charakteristik $\neq 2$ funktioniert) können wir uns auf den Fall

$$\Phi[Q] = \{z \in \mathbb{K}^n \mid \lambda_1 z_1^2 + \dots + \lambda_r z_r^2 + b_{r+1}z_{r+1} + \dots b_{z_n} + c = 0\}$$

reduzieren. Eine passende affine Bewegung, die nur die Variablen $z_{r+1},\dots,z_n$ betrifft, führt dann auf einen der drei genannten Fälle. □

Wie im reellen Fall reden wir wieder von *Kegelquadriken*, *Mittelpunksquadriken* und *parabolischen Quadriken*. Wir schreiben dann $Q^{\alpha}(\lambda_1,\ldots,\lambda_r)$ für die Modellquadrik vom Typ α mit $\lambda_1,\ldots,\lambda_r$ wie in Satz 9.4.2. Mit Satz 9.4.2 haben wir einen ersten Schritt zur Klassifikation affiner Quadriken vorgenommen. Wir sind aber an dieser Stelle keineswegs fertig, da zunächst unklar ist, welche Modellquadriken affin äquivalent sind.

[05.07.24]

Beispiel 9.4.3 (Ein altbekanntes Problem)**.** Die Gleichungen $-x_1^2 = 1$, $-x_1^2 - x_2^2 = 1$, …, $-x_1^2 - \cdots - x_n^2 = 1$ beschreiben über $\mathbb{K} = \mathbb{R}$ allesamt dieselbe reelle Quadrik (nämlich die leere Quadrik). Daher ist nicht einmal der Rang einer Quadrik wohldefiniert. Das Problem in diesem Beispiel ist, dass zwar die Quadriken affin äquivalent sind, nicht aber die zugehörigen Polynome. Dies ist über $\mathbb{R}$ möglich, da verschiedene Polynome dieselben Nullstellen besitzen können. Über algebraische abgeschlossenen Körpern tritt zumindest dieses Problem (wegen des Hilbertschen Nullstellensatzes) nicht auf.

Es ist zweckmäßig, dieses Problem zunächst zu ignorieren bzw. „wegzudefinieren“: Statt affine Äquivalenzklassen reeller Quadriken zu klassifizieren sollte man daher besser Äquivalenzklassen reell-quadratischer Polynome klassifizieren. Äquivalent dazu kann man auch einen neuen Äquivalenzbegriff für Quadriken definieren, der verlangt, dass eine (reelle) affine Bewegung sowohl die zugehörigen rellen Quadriken als auch die zugehörigen komplexen Quadriken ineinander überführt. Analog sollte man auch über anderen Körpern die Quadriken über Erweiterungskörpern mit einbeziehen. Wir werden das im Folgenden stillschweigend tun, und treffen daher die folgende Konvention.

Notation 9.4.4. Sind p_1 und p_2 zwei Polynome vom Grad 2 in $\mathbb{K}[X_1, \ldots, X_n]$, so schreiben wir $V_\bullet(p_1) \sim V_\bullet(p_2)$, wenn für jeden Erweiterungskörper $\mathbb{L}$ von $\mathbb{K}$ die Teilmengen $V_{\mathbb{L}}(p_1)$ und $V_{\mathbb{L}}(p_2)$ von $\mathbb{L}^n$ affin äquivalent zu.

Bemerkung 9.4.5. Im Allgemeinen ist die Aussage $V_\bullet(p_1) \sim V_\bullet(p_2)$ stärker als die affine Äquivalenz von $V(p_1)$ und $V(p_2)$. Für $\mathbb{K} = \mathbb{R}$ gilt beispielsweise, dass

$$V(-x_1^2) = V(-x_1^2 - x_2^2), \quad \text{aber} \quad V_\bullet(-x_1^2) \not\sim V_\bullet(-x_1^2 - x_2^2),$$

da sich die komplexen Punkte (wie wir noch sehen werden) unterscheiden.

Ist $\mathbb{K}$ *algebraisch abgeschlossen* (und p_1 und p_2 beide vom Grad 2), so folgt aus den erwähnten Prinzipien der fortgeschrittenen Algebra (Hilbertscher Nullstellensatz), dass die folgenden Aussagen äquivalent sind:

(i) $V_\bullet(p_1) \sim V_\bullet(p_2)$.

(ii) $V(p_1)$ und $V(p_2)$ sind affin äquivalent.

(iii) p_1 ist affin äquivalent zu λp_2 für ein $\lambda \in \mathbb{K}^\times$.

Die Äquivalenz von (i) und (iii) (nicht aber von (i) und (ii)) gilt auch über beliebigen Körpern.

Der Beweis von Satz 9.4.2 beweist die folgende stärkere Aussage:

Satz 9.4.6 (Affine Hauptachsentransformation)**.** *Es sei $Q = Q(B, b, c)$ eine Quadrik und es sei $r = \operatorname{rk}(B)$. Dann existieren $\lambda_1, \ldots, \lambda_r \in \mathbb{K}^\times$, so dass $Q_{\mathbb{L}}$ für jede Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$ affin äquivalent zu einer der folgenden Modellquadriken ist:*

(Typ I) $Q_{\mathbb{L}}^I(\lambda_1, \ldots, \lambda_r) = \{x \in \mathbb{L}^n \mid \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2 = 0\}$.

(Typ II) $Q_{\mathbb{L}}^{II}(\lambda_1, \ldots, \lambda_r) = \{x \in \mathbb{L}^n \mid \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2 = 1\}$.

(Typ III) $Q_{\mathbb{L}}^{III}(\lambda_1, \ldots, \lambda_r) = \{x \in \mathbb{L}^n \mid \lambda_1 x_1^2 + \cdots + \lambda_r x_r^2 = x_{r+1}\}$.

Mit anderen Worten, es gilt $Q_\bullet \sim Q^\alpha_\bullet(\lambda_1,\dots,\lambda_r)$ für ein $\alpha \in \{I, II, III\}$. □

Bemerkung 9.4.7 (Rang und erweiterter Rang)**.** Aus (9.1.3) und (9.1.4) folgt wegen Bemerkung 9.4.5 sofort: Falls

$$Q_\bullet(B_1') = Q_\bullet(B_1, b_1, c_1) \sim Q_\bullet(B_2, b_2, c_2) = Q_\bullet(B_2'),$$

so ist $\mathrm{rk}(B_1) = \mathrm{rk}(B_2)$ und $\mathrm{rk}(B_1') = \mathrm{rk}(B_2')$. Für $Q = Q(B') = Q(B, b, c)$ können wir daher den *Rang* bzw. *erweiterten Rang* von $Q_\bullet$ definieren durch

$$r(Q_\bullet) := \mathrm{rk}(B) \quad \text{und} \quad r'(Q_\bullet) = \mathrm{rk}(B').$$

Dies gibt uns zwei erste wichtige affine Invarianten von Quadriken. Nun gilt:

(i) $r(Q^I_\bullet(\lambda_1,\dots,\lambda_r)) = r'(Q^I_\bullet(\lambda_1,\dots,\lambda_r)) = r$.

(ii) $r(Q^{II}_\bullet(\lambda_1,\dots,\lambda_r)) = r'(Q^{II}_\bullet(\lambda_1,\dots,\lambda_r)) - 1 = r$.

(iii) $r(Q^{III}_\bullet(\lambda_1,\dots,\lambda_r)) = r'(Q^{II}_\bullet(\lambda_1,\dots,\lambda_r)) - 2 = r$.

Der Typ $\alpha := r'(Q_\bullet) - r(Q_\bullet) + 1 \in \{1,2,3\}$ ist also eine affine Invariante im folgenden Sinne:

Korollar 9.4.8 (Wohldefiniertheit des Typs)**.** *Gilt $Q_\bullet \sim Q'_\bullet$, so sind Q und Q' entweder beide Kegelquadriken oder beide Mittelpunktsquadriken oder beide parabolische Quadriken (jeweils vom selben Rang).* □

Um eine vollständige Klassifikation zu erreichen, bleibt nun noch innerhalb eines festen Typs $\alpha \in \{I, II, III\}$ zu entscheiden, ob zwei Modellquadriken $Q^\alpha(\lambda_1,\dots,\lambda_r)$ und $Q^\alpha(\mu_1,\dots,\mu_r)$ vom selben Typ affin äquivalent sind.

Beispiel 9.4.9 (Komplexe Hypipsen/Ellerbeln)**.** Über $\mathbb{K} = \mathbb{C}$ sind die „Ellipse“ $E \subseteq \mathbb{C}^2$ gegeben durch die Gleichung $x_1^2 + x_2^2 = 1$ und die „Hyperbel“ $H \subseteq \mathbb{C}^2$ gegeben durch die Gleichung $x_1^2 - x_2^2 = 1$ affin äquivalent. Eine explizite affine Äquivalenz ist z.B. die Abbildung

$$x \mapsto \begin{pmatrix} x_1 \\ ix_2 \end{pmatrix}.$$

Dieses Beispiel lässt sich wie folgt verallgemeinern:

Bemerkung 9.4.10 (Quadratklassen)**.** Sind $\lambda_1,\dots,\lambda_r \in \mathbb{K}^\times$ und $\mu_1,\dots,\mu_1 \in \mathbb{K}^\times$, so sind

$$Q^\alpha(\lambda_1,\dots,\lambda_r) \quad \text{und} \quad Q^\alpha(\lambda_1\mu_1^2,\dots,\lambda_r\mu_r^2)$$

affin äquivalent, und zwar vermittels der invertierbaren linearen Abbildung

$$\Phi(x) = \mathrm{diag}(\mu_1,\dots,\mu_r,1,\dots,1).$$

Notation 9.4.11. Wir nennen zwei Elemente $\lambda, \lambda' \in \mathbb{K}^\times$ *quadratisch äquivalent*, wenn sie sich nur durch Multiplikation mit dem Quadrat eines Elements von $\mathbb{K}^\times$ unterscheiden. Die entsprechenden Äquivalenzklassen heißen die *Quadratklassen* von $\mathbb{K}^\times$. Es ist nun zweckmäßig, für jede Quadratklasse in $\mathbb{K}^\times$ einen Repräsentanten zu wählen. Es bezeichne also $\mathscr{R}_\mathbb{K}$ ein Repräsentantensystem der Quadratklassen von $\mathbb{K}^\times$.

Korollar 9.4.12. *Ist Q eine Quadrik vom Rang r über $\mathbb{K}$, so existiert ein eindeutiges $\alpha \in \{I, II, III\}$ und Elemente $\lambda_1,\dots,\lambda_r \in \mathscr{R}_\mathbb{K}$, so dass $Q_\bullet \sim Q^\alpha_\bullet(\lambda_1,\dots,\lambda_r)$.* □

Korollar 9.4.13 (Endlichkeitssatz)**.** *Besitzt $\mathbb{K}^\times$ endlich viele Quadratklassen, so existieren in $\mathbb{K}^n$ nur endlich viele Quadriken bis auf affine Äquivalenz.* □

Über algebraisch abgeschlossenen Körpern erhalten wir eine vollständige Klassifikation:

Beispiel 9.4.14 (Quadratklassen algebraisch abgeschlossener Körper)**.** Ist $\mathbb{K} = \mathbb{C}$ oder allgemeiner $\mathbb{K}$ ein algebraisch abgeschlossener Körper, so ist jedes Element von $\mathbb{K}^\times$ ein Quadrat (da das Polynom $X^2 - \lambda$ für jedes $\lambda \in \mathbb{K}^\times$ eine Nullstelle besitzt), und daher ist $\mathscr{R}_\mathbb{K} := \{1\}$ ein Repräsentantensystem der Quadratklassen.

Beachten wir noch, dass über einem algebraisch abgeschlossenen Körper $\mathbb{K}$ die Bedingungen (i) und (ii) aus 9.4.5 äquivalent sind, so folgt mit Korollar 9.4.12 die folgende Klassifikation.

Korollar 9.4.15 (Klassifikation über algebraisch abgeschlossenen Körpern)**.** *Es sei $\mathbb{K}$ algebraisch abgeschlossen und $Q = Q(B') = Q(B, b, c) \subseteq \mathbb{K}^n$ mit $r = \mathrm{rk}(B)$. Ist $r \in \{1, \dots, n-1\}$, so ist Q über $\mathbb{K}$ affin äquivalent zu genau einer der drei folgenden Quadriken:*

(Typ I) $Q^I[r] = \{x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_r^2 = 0\}$.

(Typ II) $Q^{II}[r] = \{x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_r^2 = 1\}$.

(Typ III) $Q^{III}[r] = \{x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_r^2 = x_{r+1}\}$.

Ist $r = n$, so ist Q affin äquivalent zu $Q^I[r]$ oder $Q^{II}[r]$. Insbesondere gibt es in $\mathbb{K}^n$ genau $3n-1$ affine Äquivalenzklassen affiner Quadriken, und diese werden repräsentiert durch

$$Q^I[1], \dots, Q^I[n], Q^{II}[1], \dots, Q^{II}[n], Q^{III}[1], \dots, Q^{III}[n-1].$$ □

Bemerkung 9.4.16 (Jenseits algebraisch abgeschlossener Körper)**.** Es ist naheliegend zu versuchen, Korollar 9.4.15 auf nicht-algebraisch abgeschlossene Körper zu erweitern. Das führt aber sehr schnell auf (für uns) unüberwindbare Schwierigkeiten. Naiv könnte man hoffen, dass für jede Quadrik Q die Äquivalenz $Q_\bullet \sim Q^\alpha_\bullet(\lambda_1, \dots, \lambda_r)$ für eindeutig bestimmte $\alpha \in \{I, II, III\}$, $r \in \{1, \dots, n\}$ (bzw. $r \in \{1, \dots, n\}$ falls $\alpha = III$) und bis auf Reihenfolge eindeutig bestimmte $\lambda_1, \dots, \lambda_r \in \mathscr{R}_\mathbb{K}$ ist. Das ist aber *nicht* der Fall, und es ist wichtig zu verstehen, dass $\lambda_1, \dots, \lambda_r \in \mathscr{R}_\mathbb{K}$ im Allgemeinen *nicht* bis auf Reihenfolge eindeutig bestimmt sind.

Bereits im Fall $\mathbb{K} = \mathbb{R}$ gilt $\mathscr{R}_\mathbb{R} = \{-1, 1\}$, aber $Q^I(\lambda_1, \dots, \lambda_k) = Q^I(-\lambda_1, \dots, -\lambda_k)$. Diese Vorzeichenprobleme lassen sich mit etwas Arbeit in den Griff bekommen - das ist aber nur die Spitze des Eisbergs! Für die Zahlentheorie von großem Interesse ist der Fall $\mathbb{K} = \mathbb{Q}$, z.B. das Studium rationaler Punkte auf Kegelschnitten. Hier treten nun ganz neue Schwierigkeiten auf, die wir kurz skizzieren wollen:

Da $\sqrt{2}$ irrational ist, repräsentieren 1 und 2 bzw. -1 und -2 verschiedene Quadratklassen. Die orthogonalen Geometrien $[1, -1]$ und $[2, -2]$ über $\mathbb{Q}$ sind aber äquivalent (es handelt sich ja um isotrope Standardebenen!), und daher sind die Quadriken zu den zugehörigen quadratischen Form $x_1^2 - x_2^2$ und $2x_1^2 - 2x_2^2$ (jeweils vom gleichen Typ) affin äquivalent. Allgemeiner gilt:

$$\begin{gathered}\textit{Existiert eine Matrix } S \in \mathrm{GL}_r(\mathbb{Q}) \textit{ mit } S^\top \mathrm{diag}(\lambda_1, \dots, \lambda_r) S = \mathrm{diag}(\mu_1, \dots, \mu_r)\textit{, so gilt} \\ Q^\alpha_\bullet(\lambda_1, \dots, \lambda_k) \sim Q^\alpha_\bullet(\mu_1, \dots, \mu_k).\end{gathered}$$

Die Existenz einer solchen Matrix S bedeutet gerade, dass die entsprechenden orthogonalen $\mathbb{K}$-Vektorräume isomorph sind. Über $\mathbb{K} = \mathbb{Q}$ führt dies auf Hasse-Minkowski-Theorie, über allgemeinen Körpern – wie bereits im Kontext der orthogonalen Geometrien erwähnt – auf sehr schwierige Probleme (Bestimmung der Witt-Gruppe).

In einem ersten Schritt sollte man auf jeden Fall die Witt-Zerlegung der Bilinearform zur quadratischen Form $\mathrm{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$ durchführen. Man erhält dann eine äquivalente Matrix der Form $\mathrm{diag}(1,-1,1,-1,\dots,1,-1,\mu_{2k+1},\dots\mu_r,0,\dots,0)$, wobei k der Witt-Index und die Bilinearform zu $\mathrm{diag}(\mu_{2k+1},\dots\mu_r)$ total anisotrop über $\mathbb{K}$ ist. Das eigentliche Problem liegt dann wieder im Studium der total anisotropen orthogonalen Vektorräume über $\mathbb{K}$.

Zum Abschluss dieses Kapitels wollen wir uns noch überlegen, warum Quadriken vom Typ II auch „Mittelpunktsquadriken“ genannt werden.

Definition 9.4.17. Ein Punkt $m \in \mathbb{K}^n$ heißt ein *Mittelpunkt* einer Quadrik $Q \subseteq \mathbb{K}^n$, falls für alle $t \in \mathbb{K}$ und $v \in \mathbb{K}^n$ gilt:

$$m + tv \in Q \quad \Longrightarrow \quad m - tv \in Q.$$

Nach Definition ist also ein Punkt m genau dann ein Mittelpunkt von Q, wenn die affine Punktspiegelung an m die Quadrik wieder in sich selbst überführt. Ist Q leer, so ist nach Definition jeder Punkt von $\mathbb{K}^n$ ein Mittelpunkt.

Proposition 9.4.18 (Mittelpunktsgleichung)**.** *Es sei $Q = Q(B,b,c) \subseteq \mathbb{K}^n$.*

(i) Ist $Bm + b = 0$, so ist m ein Mittelpunkt von Q.

(ii) Ist $\mathbb{K}$ algebraisch abgeschlossen, so gilt auch die Umkehrung.

Beweis. Ist $p = p(B,b,c)$, so gilt für alle $t \in \mathbb{K}$ und $v \in \mathbb{K}^n$, dass (wegen $b^\top v = v^\top b$)

$$\begin{aligned} p(m+tv) &= (m+tv)^\top B(m+tv) + 2b^\top(m+tv) + c \\ &= m^\top Bm + 2tv^\top Bm + t^2 v^\top v + 2b^\top m + 2tb^\top v + c \\ &= (m^\top Bm + t^2 v^\top v + c) + 2tv^\top(Bm+b). \end{aligned}$$

und analog

$$p(m-tv) = (m^\top Bm + t^2 v^\top v + c) - 2tv^\top(Bm+b).$$

Daraus folgt nun leicht die Behauptung:

(i) Ist $Bm + b = 0$, so gilt für alle $t \in \mathbb{K}$ und $v \in \mathbb{K}^n$, dass

$$m + tv \in Q \implies p(m+tv) = 0 \implies m^\top Bm + t^2 v^\top v + c = 0 \implies p(m-tv) = 0 \implies m - tv \in Q.$$

(ii) Ist m ein Mittelpunkt, so besitzen die Polynome $v \mapsto p(m+tv)$ und $v \mapsto p(m-tv)$ für jedes $t \in \mathbb{K}$ dieselbe Nullstellenmenge. Ist $\mathbb{K}$ algebraisch abgeschlossen, so folgt, dass diese bis auf eine multiplikative Konstante gleich sind, und Vergleich der konstanten Terme liefert dann, dass die sogar gleich sind. Es gilt dann also

$$0 = p(m+tv) - p(m-tv) = 4tv^\top(Bm+b).$$

für alle $t \in \mathbb{K}$ und $v \in \mathbb{K}^n$ und daher $Bm + b = 0$. □

Ist $\mathbb{K}$ nicht algebraisch abgeschlossen, so gibt es u.U. mehr Mittelpunkte als Lösungen der Gleichungen $Bm + b$ wie der Fall von $V(-x_1^2) = \emptyset$ über $\mathbb{R}$ zeigt (in dem jeder Punkt ein Mittelpunkt ist).

Korollar 9.4.19. *Gilt $Q_\bullet(B,b,c) \sim Q_\bullet(B',b',c')$, so sind die Lösungsmengen der LGS $Bx = b$ und $B'x = b'$ entweder beide leer oder beide affine Räume derselben Dimension.*

Beweis. Es sei $\mathbb{L}$ ein algebraisch abgeschlossener Erweiterungskörper von $\mathbb{K}$. (Das ein solcher Körper immer existiert, lernen Sie in der Vorlesung ALGEBRA). Nach Annahme sind $Q_{\mathbb{L}}(B,b,c)$ und $Q_{\mathbb{L}}(B',b',c')$ affin äquivalent, und daher sind insbesondere ihre Mittelpunktsmengen affin äquivalent. Mit Proposition 9.4.18 folgt die Behauptung. □

Beispiel 9.4.20 (Mittelpunkte der Modellquadriken)**.** Über einem algebraisch abgeschlossenen Körper $\mathbb{K}$ bestimmen wir die Mittelpunkte der Modellquadriken $Q^{\alpha}(\lambda_1,\dots,\lambda_r)$ mit $\alpha \in \{I,II,III\}$ und $\lambda_1,\dots,\lambda_r \in \mathbb{K}^{\times}$.

(i) Ist $Q = Q^{I}(\lambda_1,\dots,\lambda_r)$, so ist $B = \operatorname{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$ und $b = 0$ und daher ist $m \in \mathbb{K}^n$ genau dann ein Mittelpunkt, wenn $m_1 = \cdots = m_r = 0$ gilt. Falls $r = n$ so ist der Ursrpung also der eindeutige Mittelpunkt, andernfalls bilden die Mittelpunkte einen affinen Unterraum der Dimension $n - r$.

(ii) Ist $Q = Q^{II}(\lambda_1,\dots,\lambda_r)$, so ist $B = \operatorname{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$ und $b = 0$ und daher ist $m \in \mathbb{K}^n$ genau dann ein Mittelpunkt, wenn $m_1 = \cdots = m_r = 0$ gilt. Falls $r = n$ so ist der Ursrpung also der eindeutige Mittelpunkt, andernfalls bilden die Mittelpunkte einen affinen Unterraum der Dimension $n - r$.

(iii) Ist $Q = Q^{III}(\lambda_1,\dots,\lambda_r)$, so ist $B = \operatorname{diag}(\lambda_1,\dots,\lambda_r,0,\dots,0)$ und $b = -1/2e_{r+1}$. Daher hat das LGS $Bm = -b$ keine Lösung, d.h. es gibt keinen Mittelpunkt.

Ist $\mathbb{K}$ nicht algebraisch abgeschlossen, so kann es zusätzliche Mittelpunkte geben, etwa im Fall einer leeren Quadrik. Über algebraisch abgeschlossenen Körpern sind also die parabolischen Quadriken genau die Quadriken ohne Mittelpunkte.

Zusammenfassung von Abschnitt 9.4.

(1) Jede Quadrik über einem Körper der Charakteristik $\neq 2$ ist affin äquivalent zu einer Modellquadrik.

(2) Betrachtet man Quadriken bis auf affine Äquivalenz über Erweiterungskörpern, so sind der Rang und der Typ einer Quadrik zwei wichtige affine Invarianten.

(3) Quadriken über algebraisch abgeschlossenen Körpern sind durch ihren Rang und ihren Typ bis auf affine Äquivalenz eindeutig bestimmt. Über allgemeineren Körpern ist dies nicht der Fall.

(4) Im Falle eines algebraisch abgeschlossenen Körpers ist die Menge der Mittelpunkte einer Quadrik entweder leer (genau im parabolischen Fall) oder ein echter affiner Unterraum.

10 Tensorprodukte und Tensoralgebra

10.1 Tensorprodukte endlichdimensionaler Vektorräume

Es sei stets $\mathbb{K}$ ein Körper und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum mit Dualraum V^*.

Beispiel 10.1.1 (Kontravariante 2-Tensoren)**.** In Definition 4.2.6 haben wir den Vektorraum

$$(V^*)^{\otimes k} := \{D : V^k \to \mathbb{K} \mid D \text{ } k\text{-linear}\}$$

der *kontravarianten k-Tensoren* auf V definiert. Diesen wollen wir nun etwas genauer verstehen. Der Einfachheit halber konzentrieren wir uns vorläufig auf den Raum

$$V^* \otimes V^* := (V^*)^{\otimes 2} = \{D : V \times V \to \mathbb{K} \mid D \text{ bilinear}\} = \mathrm{Bil}(V)$$

der *kontravarianten* 2*-Tensoren*, also Bilinearformen. Weiter definieren wir eine Abbildung

$$\iota : V^* \times V^* \to V^* \otimes V^*, \quad (\alpha, \beta) \to \alpha \otimes \beta.$$

Hierbei ist $\alpha \otimes \beta$ der elementare Tensor gegeben durch

$$(\alpha \otimes \beta)(v, w) := \alpha(v)\beta(w) \quad (v, w \in V).$$

Wie beobachten, dass die Abbildung ι bilinear ist, und zwar in dem Sinne, dass die beiden Abbildungen $V^* \to V^* \otimes V^*$ gegeben durch

$$\alpha \mapsto \alpha \otimes \beta \quad \text{bzw.} \quad \beta \mapsto \alpha \otimes \beta$$

beide linear sind. Man beachte, dass die Abbildung ι *nicht* injektiv ist, denn ist $\lambda \in \mathbb{K} \setminus \{1\}$ und $\alpha, \beta \neq 0$, so gilt $(\lambda\alpha, \beta) \neq (\alpha, \lambda\beta)$, aber $(\lambda\alpha) \otimes \beta = \alpha \otimes (\lambda\beta)$. Wir behaupten, dass das Bild von ι schon $V^* \otimes V^*$ aufspannt. Genauer zeigen wir:

Ist $(\lambda_1, \ldots, \lambda_n)$ *eine Basis von* V^**, so ist* $\{\lambda_i \otimes \lambda_j \mid i, j \in \{1, \ldots, n\}\}$ *eine Basis von* $V^* \otimes V^*$.

Zum Beweis sei $B \in V^* \otimes V^*$. Für fixes $w \in V$ ist die Abbildung $v \mapsto B(v, w)$ ein Element der Dualraums V^*. Da $(\lambda_1, \ldots, \lambda_n)$ eine Basis von V^* ist, existieren also von w abhängige eindeutige Koeffzienten $\mu_i(w) \in \mathbb{K}$ mit

$$B(v, w) = \sum_{i=1}^{n} \mu_i(w)\lambda_i(v).$$

Die Abbildungen $w \mapsto \mu_i(w)$ sind nun aber (aufgrund der Eindeutigkeit und der Linearität von B in der zweiten Variablen) linear, also existieren $\alpha_{ij} \in \mathbb{K}$ mit

$$\mu_i(w) = \sum_{j=1}^{n} \alpha_{ij}\lambda_j(w) \quad \Longrightarrow \quad B(v, w) = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij}\lambda_i(v)\lambda_j(w) = \left(\sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij}(\lambda_i \otimes \lambda_j)\right)(v, w)$$

$$\Longrightarrow \quad B = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij}(\lambda_i \otimes \lambda_j).$$

Dies zeigt, dass die Menge $\{\lambda_i \otimes \lambda_j \mid i, j \in \{1, \ldots, n\}\}$ ein Erzeugendensystem von $V^* \otimes V^*$ ist. Dieses besteht aus höchstens $n^2 = \dim \mathrm{Bil}(V)$ Elementen. Aus Dimensionsgründen ist sie daher sogar eine Basis.

Als Anwendung überlegen wir uns, dass die Abbildung ι im Allgemeinen *nicht* surjektiv ist. Ist z.B. $\dim V = 2$ und $\{\lambda_1, \lambda_2\}$ eine Basis von V^*, so ist

$$\text{Bild}(\iota) = \iota(\{(\alpha_1\lambda_1 + \alpha_2\lambda_2, \beta_1\lambda_1 + \beta_2\lambda_2) \mid \alpha_i, \beta_i \in \mathbb{K}\}) = \left\{ \sum_{i,j=1}^{2} \alpha_i\beta_j(\lambda_i \otimes \lambda_j) \mid \alpha_i, \beta_i \in \mathbb{K} \right\}.$$

Die vier Koeffizienten eines elementaren Tensors bzgl. der Basisvektoren $\lambda_i \otimes \lambda_j$ sind also von der Form $\alpha_1\beta_1$, $\alpha_1\beta_2$, $\alpha_2\beta_1$ und $\alpha_2\beta_2$. Ist nun z.B. der erste Koeffizient $\alpha_1\beta_1$ von 0 verschieden und der Koeffizient $\alpha_1\beta_2$ gleich 0, so ist notwendig auch der Koeffizient $\alpha_2\beta_2$ gleich 0. Daher ist die Abbildung ι in diesem Fall nicht surjektiv (obwohl ihr Bild ganz $V^* \otimes V^*$ aufspannt).

Bemerkung 10.1.2 (Lineare Fortsetzung)**.** Ist $\widetilde{f} : V^* \otimes V^* \to W$ eine beliebige lineare Abbildung in einen Vektorraum W, so ist $f := \widetilde{f} \circ \iota$ bilinear (weil ι bilinear ist), und das Diagramm

$$\begin{array}{ccc} V^* \times V^* & \xrightarrow{f} & W \\ {\scriptstyle \iota}\downarrow & \nearrow_{\widetilde{f}} & \\ V^* \otimes V^* & & \end{array}$$

kommutiert. Aus der **linearen** Abbildung $\widetilde{f}$ wird durch Verketten mit ι also eine **bilineare** Abbildung f. Wir nennen dann $\widetilde{f}$ eine *lineare Fortsetzung* der bilinearen Abbildung f.

Satz 10.1.3 (Universelle Eigenschaft)**.** *Jede beliebige bilineare Abbildung $f : V^* \times V^* \to W$ besitzt eine eindeutig lineare Fortsetzung $\widetilde{f} : V^* \otimes V^* \to W$. Die Abbildung $f \mapsto \widetilde{f}$ liefert daher eine Bijektion zwischen bilineare Abbildung $f : V^* \times V^* \to W$ und linearen Abbildung $\widetilde{f} : V^* \otimes V^* \to W$.*

Beweis. Wir wählen eine geordnete Basis $(\lambda_1, \ldots, \lambda_n)$ von V^*, so dass die $\lambda_i \otimes \lambda_j$ eine Basis von $V^* \otimes V^*$ bilden. Es existiert dann eine eindeutige lineare Abbildung $\widetilde{f} : V^* \otimes V^* \to W$ mit

$$\widetilde{f}(\lambda_i \otimes \lambda_j) := f(\lambda_i, \lambda_j) \quad (i, j \in \{1, \ldots, n\}),$$

und wir behaupten, dass diese eine lineare Fortsetzung von f ist. Zum Beweis seien $\lambda, \mu \in V^*$; wir entwickeln

$$\lambda = \sum_{i=1}^{n} \alpha_i\lambda_i \quad \text{und} \quad \sum_{j=1}^{n} \beta_j\lambda_j \quad (\alpha_i, \beta_j \in \mathbb{K}).$$

Es gilt dann

$$f(\lambda, \mu) = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i\beta_j f(\lambda_i, \lambda_j) = \sum_{i,j\in I} \alpha_i\beta_j \widetilde{f}(\lambda_i \otimes \lambda_j) = \widetilde{f}\left(\left(\sum_{i\in I} \alpha_i\lambda_i\right) \otimes \left(\sum_{j\in I} \beta_j\lambda_j\right)\right) = \widetilde{f}(\lambda \otimes \mu),$$

also $f = \widetilde{f} \circ \iota$. Auf den ersten Blick sieht es so aus, als hänge unsere Fortsetzung von der Wahl einer Basis ab. Das ist aber nicht der Fall: Weil das Bild von ι schon $V^* \otimes V^*$ erzeugt, ist die lineare Fortsetzung $\widetilde{f}$ durch ihre Einschänkung auf diese Bild (also f) eindeutig bestimmt. □

$V^* \otimes V^*$ ist also eine Maschine, die es uns erlaubt, gewisse bilineare Abbildungen in lineare Abbildungen zu übersetzen.

Konstruktion 10.1.4 (Doppeldualtrick)**.** Wir haben das „Produkt“ $\otimes$ bisher nur für Dualräume von endlichdimensionalen Vektorräumen definiert. Das ist aber kein echtes Hindernis: Für

jeden endlichdimensionalen Vektorraum V definieren wir eine Abbildung von V in den Doppeldualraum $V^{**} := (V^*)^*$ durch

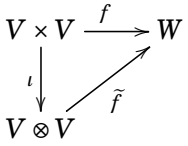
$$\kappa_V : V \to V^{**}, \quad \kappa_V(v)(\lambda) := \lambda(v).$$

Diese Abbildung ist linear (Übung) und ist $v \in \ker(\kappa_V)$, so gilt $\lambda(v) = 0$ für alle $v \in V^*$. Wäre $v \neq 0$, so könnten wir v zu einer Basis $(v = v_1, \ldots, v_n)$ von V ergänzen, und bzgl. der dualen Basis wäre dann $v_1^*(v_1) = 1 \neq 0$. Dieser Widerspruch zeigt, dass $\ker(\kappa_V) = \{0\}$, dass also κ_V injektiv ist. Aus Dimensiongründen ist κ_V dann sogar ein Isomorphismus, der es uns erlaubt V mit $(V^*)^*$ zu identifizieren.

Wir bezeichnen nun mit $V \otimes V$ den Raum der Bilinearformen auf V^* und definieren

$$\iota : V \times V \to V \otimes V, \quad \iota(v, w) = \kappa_V(v) \otimes \kappa_V(w).$$

Zu jeder linearen bilinearen Abbildung $f : V \times V \to W$ existiert dann wieder eine lineare Abbildung $\widetilde{f} : V \otimes V \to W$, so dass das Diagramm



kommutiert.

Wir haben also eine Art „Produkt“ eines endlichdimensionalen Vektorraums V mit sich selbst definiert, das bilineare Abbildungen in lineare Abbildungen übersetzt. Können wir auch Produkte beliebiger endlichdimensionaler Vektorräume mit analogen Eigenschaften definieren?

[10.06.24]

Definition 10.1.5. Es seien $V_1,\dots,V_k$ endlichdimensionale $\mathbb{K}$-Vektorräume. Ein *Tensorprodukt* von $V_1,\dots V_k$ ist ein Paar $(V_1\otimes\cdots\otimes V_k,\iota)$ bestehend aus einem $\mathbb{K}$-Vektorraum $V_1\otimes\cdots\otimes V_k$ und einer k-linearen Abbildung $\iota: V_1\times\cdots\times V_n\to V_1\otimes\cdots\otimes V_n$, so dass es für jede n-lineare Abbildung $f: V_1\times\cdots\times V_n\to W$ in einen $\mathbb{K}$-Vektorraum W eine eindeutig bestimmte lineare Abbildung $\widetilde{f}: V_1\otimes\cdots\otimes V_n\to W$ gibt, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} V_1\times\cdots\times V_n & \xrightarrow{f} & W \\ {\scriptstyle\iota}\downarrow & \nearrow_{\widetilde{f}} & \\ V_1\otimes\cdots\otimes V_n & & \end{array}$$

Mit dieser Terminologie haben wir gezeigt, dass $(\mathrm{Bil}(V^*),\iota)$ (bzw. $(\mathrm{Bil}(V),\iota)$) ein Tensorprodukt von V mit V (bzw. von V^* mit V^*) ist.

Übung 10.1.6. Zeigen Sie analog: Ist $k\geq 2$ und $\iota: V^*\times\cdots\times V^*\to (V^*)^{\otimes k}$ die k-lineare Abbildung gegeben durch $(v_1,\dots,v_k)\mapsto v_1\otimes\cdots\otimes v_k$, so ist $((V^*)^{\otimes k},\iota)$ ein Tensorprodukt von V^*, …, V^*. Finden Sie analog ein Tensorprodukt von V, …, V.

Satz 10.1.7 (Existenz von Tensorprodukten)**.** *Sind $V_1,\dots,V_k$ endlichdimensionale $\mathbb{K}$-Vektorräume mit $d_i:=\dim V_i$, so existiert stets ein Tensorprodukt $(V_1\otimes\cdots\otimes V_k,\iota)$ mit $\dim V_1\otimes\cdots\otimes V_k = d_1d_2\cdots d_k$.*

Beweis. Für $i\in\{1,\dots,k\}$ sei $(v_1^{(i)},\dots,v_K^{(i)})$ eine geordnete Basis von V_i. Wir würden uns wünschen, dass wie im obigen Beispiel gewisse Vektoren der Form $v_{j_1}^{(1)}\otimes\cdots\otimes v_{j_n}^{(n)}$ eine Basis des Tensorprodukts bilden. Nun, nichts leichter als das: Wir definieren das Tensorprodukt einfach so, dass das der Fall ist!

Formal: Wir setzen $d:=d_1\cdots d_k$ und wählen eine Bijektion

$$b:\{1,\dots,d_1\}\times\cdots\times\{1,\dots,d_k\}\to\{1,\dots,d\}$$

Wir setzen dann $V_1\otimes\cdots\otimes V_k:=\mathbb{K}^d$ und definieren

$$v_{j_1}^{(1)}\otimes\cdots\otimes v_{j_k}^{(k)}:=e_{b(j_1,\dots,j_k)}\in V_1\otimes\cdots\otimes V_k=\mathbb{K}^d.$$

Da b eine Bijektion ist, ist dann

$$\mathscr{B}:=\left\{v_{j_1}^{(1)}\otimes\cdots\otimes v_{j_k}^{(k)}\mid j_1\in\{1,\dots,d_1\},\dots,j_k\in\{1,\dots,d_k\}\right\}$$

eine Basis (nämlich die Standardbasis) von V_k. Motiviert durch unsere Beispiele setzen wir nun

$$\iota\left(\sum_{j_1=1}^{d_1}\alpha_{j_1}v_{j_1}^{(1)},\dots,\sum_{j_k=1}^{d_k}\alpha_{j_n}v_{j_n}^{(n)}\right):=\sum_{j_1\in I_1}\cdots\sum_{j_n\in I_n}\alpha_{j_1}\cdots\alpha_{j_n}v_{j_1}^{(1)}\otimes\cdots\otimes v_{j_n}^{(n)}.$$

Diese Abbildung ist offensichtlich n-linear. Ist nun $f: V_1\times\cdots\times V_n\to W$ eine n-lineare Abbildung in einen beliebigen $\mathbb{K}$-Vektorraum W, so definieren wir $\widetilde{f}: V_1\otimes\cdots\otimes V_k\to W$ als die eindeutige lineare Fortsetzung der Abbildung

$$\mathscr{B}\to W,\quad v_{j_1}^{(1)}\otimes\cdots\otimes v_{j_n}^{(n)}\mapsto f(v_{j_1}^{(1)},\dots,v_{j_n}^{(n)}).$$

Nach Konstruktion gilt dann für alle Indizes, dass

$$\widetilde{f} \circ \iota(v_{j_1}^{(1)}, \dots, v_{j_n}^{(n)}) = f(v_{j_1}^{(1)}, \dots, v_{j_n}^{(n)}),$$

und da beide Seiten n-linear sind folgt darauf schon $f = \iota \circ \widetilde{f}$. Dies beweist die Existenz der Fortsetzung von f, und da das Bild von ι bereits den gesamten $\mathbb{K}^d$ erzeugt, ist die Fortsetzung auch eindeutig. □

Der hier präsentierte Beweis ist sehr unbefriedigend, weil die Konstruktion des Tensorprodukts scheinbar von sehr willkürlichen Wahlen abhängt. Wir werden später noch einen abstrakteren Beweis sehen, der keine solche Wahlen erfordert und sich besser verallgemeinern lässt. Zunächst wollen wir uns aber überlegen, in welchem Sinne Tensorprodukte eindeutig sind. Wir schauen uns zunächst ein einfacheres Eindeutigkeitsproblem an:

Bemerkung 10.1.8 (Eindeutigkeit initialer Vektorräume)**.** Ein $\mathbb{K}$-Vektorraum V_0 heiße *initial*, wenn es für jeden $\mathbb{K}$-Vektorraum W eine eindeutige lineare Abbildung $f : V_0 \to W$ gibt. Offensichtlich ist jeder einelementige[1] $\mathbb{K}$-Vektorraum initial. Es seien nun V_0 und W_0 zwei initiale $\mathbb{K}$-Vektorräume. Wir finden dann eindeutige lineare Abbildungen $f : V_0 \to W_0$ (aus der universellen Eigenschaft von V_0) und $g : W_0 \to V_0$ (aus der universellen Eigenschaft von W_0):

$$V_0 \overset{\exists! f}{\dashrightarrow} W_0 \overset{\exists! g}{\dashrightarrow} V_0 \overset{\exists! f}{\dashrightarrow} W_0.$$
$$\qquad\qquad\quad g\circ f \qquad\quad f\circ g$$

Wir haben nun zwei Morphismen $g \circ f : V_0 \to V_0$ und $\mathrm{Id}_{V_0} : V_0 \to V_0$, aber nach der universellen Eigenschaft von V_0 kann es nur einen solchen Morphismus[2] geben. Es gilt also $g \circ f = \mathrm{Id}_{V_0}$. Analog folgt aus der universellen Eigenschaft von W_0, dass $f \circ g = 1_{W_0}$. Das bedeutet aber gerade, dass f und g zueinander inverse Isomorphismen sind, und daher ist $V_0 \cong W_0$. Es gilt sogar noch mehr: Zwischen je zwei initialen Vektorräumen gibt es einen *eindeutigen* Isomorphismus. „Der“ Nullvektorraum ist daher der *bis auf eindeutige Isomorphie eindeutige* initiale $\mathbb{K}$-Vektorraum.

Das Highlander-Argument lässt sich auch auf Tensorprodukte anwenden. Wir erhalten:

Proposition 10.1.9 (Eindeutigkeit des Tensorprodukts)**.** *Sind (T_1, ι_1) und (T_2, ι_2) zwei Tensorprodukte von $V_1, \dots, V_k$, so existiert ein eindeutiger Vektorraumisomorphismus $\iota_{12} : T_1 \to T_2$, so dass das Diagramm*

$$\begin{array}{ccc} & V_1 \times \cdots \times V_k & \\ {\scriptstyle \iota_1}\swarrow & & \searrow{\scriptstyle \iota_2} \\ T_1 & \xrightarrow{\quad \iota_{12} \quad} & T_2 \end{array}$$

kommutiert. Insbesondere gilt $\dim T_1 = \dim T_2 = \dim V_1 \cdots \dim V_k$.

Beweis. Wir können wie bilineare Abbildung ι_2 zu einer linearen Abbildung auf T_1 fortsetzten und umgekehrt. Dies liefert kommutative Diagramme

$$\begin{array}{ccc} & V_1 \times \cdots \times V_k & \\ {\scriptstyle \iota_1}\swarrow & & \searrow{\scriptstyle \iota_2} \\ T_1 & \xrightarrow{\quad \iota_{12} \quad} & T_2 \end{array} \qquad \text{und} \qquad \begin{array}{ccc} & V_1 \times \cdots \times V_k & \\ {\scriptstyle \iota_2}\swarrow & & \searrow{\scriptstyle \iota_1} \\ T_2 & \xrightarrow{\quad \iota_{21} \quad} & T_1 \end{array}$$

[1] Wir haben einen solchen Vektorraum immer als Nullvektorraum bezeichnet. Beachte aber, dass es viele Nullvektorräume gibt, z.B. $\{0\}$ oder $\{0\}$.

[2] Man nennt dieses Argument auch das *Highlander-Argument* (nach dem gleichnamigen Hollywood-Film).

Nach dem Highlander-Argument sind ι_{12} und ι_{21} zueinander inverse Isomorphismen. □

In diesem Sinne kann man von „dem“ Tensorprodukt von (endlichdimensionalen[3]) Vektorräumen sprechen (genauso wie man von „dem“ Nullvektorraum spricht). Die Produktformel für die Dimension rechtfertigt den Namen Tensor*produkt*.

Notation 10.1.10 (Elementare Tensoren)**.** Ist $(V_1 \otimes \cdots \otimes V_k, \iota)$ „das“ Tensorprodukt der Vektorräume $V_1, \ldots, V_k$ so nennen wir Elemente von $V_1 \otimes \cdots \otimes V_k$ *Tensoren*. Weiter schreiben wir (in Übereinstimmung mit unserer bisherigen Notation)

$$v_{i_1} \otimes \cdots \otimes v_{i_k} := \iota(v_{i_1}, \ldots, v_{i_k})$$

und nennen den Vektor $v_{i_1} \otimes \cdots \otimes v_{i_k}$ das *Tensorprodukt* der Vektoren $v_{i_1}, \ldots, v_{i_k}$. Wir haben bereits im Fall $k = 2$ gesehen, dass sich nicht jeder Tensor als ein Tensorprodukt schreiben lässt. Tensoren, die sich als Tensorprodukte schreiben lassen, bezeichnen wir im Folgenden als *elementare Tensoren*.

Wie rechnet man nun konkret in Tensorprodukten endlichdimensionaler Vektorräume?

Bemerkung 10.1.11 (Rechenregeln)**.** Aufgrund der Bilinearität von ι gelten die folgenden Rechenregeln für elementare Tensoren in $V_1 \otimes V_2$; hierbei sind $v_1, w_1 \in V_1$, $v_2, w_2 \in V_2$ und $\lambda \in \mathbb{K}$:

(i) $\lambda(v_1 \otimes v_2) = (\lambda v_1) \otimes v_2 = v_1 \otimes (\lambda v_2)$.

(ii) $(v_1 + w_1) \otimes v_2 = (v_1 \otimes v_2) + (w_1 \otimes v_2)$ und $v_1 \otimes (v_2 + w_2) = (v_1 \otimes v_2) + (v_1 \otimes w_2)$.

Bei mehr als zwei Faktoren gelten entsprechend die Regeln, die sich aus der Multilinearität von ι ergeben.

Beispiel 10.1.12 (Rechnen mit Tensoren)**.** Wir betrachten das Tensorprodukt von $\mathbb{Q}^3$ und $\mathbb{Q}^2$ über $\mathbb{K} = \mathbb{Q}$. Es sei (e_1, e_2, e_3) die Standardbasis von $\mathbb{Q}^3$ und (der besseren Unterscheidbarkeit halber) (f_1, f_2) die Standardbasis von $\mathbb{Q}^2$. Es ist dann

$$\mathscr{B} := (e_1 \otimes f_1, e_1 \otimes f_2, e_2 \otimes f_1, e_2 \otimes f_2, e_3 \otimes f_1, e_3 \otimes f_2)$$

eine geordnete Basis von $\mathbb{Q}^3 \otimes \mathbb{Q}^2$. Wie lassen sich nun allgemeine Tensoren in dieser Basis darstellen?

Da jeder Tensor eine Linearkombination elementarer Tensoren ist, genügt es zu verstehen, wie sich elementare Tensoren darstellen lassen. Hierzu verwenden wir die o.g. Rechenregeln. Z.B. gilt

$$\begin{aligned} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 5 \end{pmatrix} &= (e_1 + 2e_2 + 3e_3) \otimes (4f_1 + 5f_2) \\ &= 4 \cdot e_1 \otimes f_1 + 8 \cdot e_2 \otimes f_1 + 12 \cdot e_3 \otimes f_1 + 5 \cdot e_1 \otimes f_2 + 10 \cdot e_2 \otimes f_2 + 15 \cdot e_3 \otimes f_2. \end{aligned}$$

Wir haben implizit schon sehr viele Beispiele für Tensoren gesehen, nur nicht in dieser abstrakten Notation. Das wollen wir uns nun genauer überlegen.

[3] Wir werden diese Einschränkung im nächsten Abschnitt loswerden.

Definition 10.1.13. Ist V ein $\mathbb{K}$-Vektorraum, so heißt ein Element von

$$V^{\otimes k} \otimes (V^*)^{\otimes l} := \underbrace{V \otimes \cdots \otimes V}_{k} \otimes \underbrace{V^* \otimes \cdots \otimes V^*}_{l}$$

ein *Tensor vom Typ (k,l)* und *totalem Grad* $k+l$ über V. Ein Tensor vom Typ $(0,l)$ ist also ein *kontravarianter l-Tensor* im Sinne von Definition 4.2.6, und analog heißt ein Tensor vom Typ $(k,0)$ ein *kovarianter k-Tensor*. (Auf die Bedeutung der Begriffe kovariant und kontravariant werden wir später noch genauer eingehen.)

Beispiel 10.1.14 (Bilinearformen und Determinantenformen als Tensoren)**.** Kontravariante Tensoren sind uns schon früher begegnet: Kontravariante 2-Tensoren (also Tensoren vom Typ (0,2)) sind Bilinearformen, und von 0 verschiedene alternierende kontravariante n-Tensoren auf einem n-dimensionalen Vektorraum sind Determinantenformen.

Wofür aber sind kovariante Tensoren oder gar Tensoren vom gemischten Typ gut?

Beispiel 10.1.15 (Tensoren vo Typ (1,1)**.** Betrachten wir zunächst einen Tensors $A \in V \otimes V^*$ vom Typ (1,1): Im allereinfachsten Fall ist A ein elementarer Tensor der Form $v \otimes \lambda$ mit $v \in V$ und $\lambda \in V^*$. Das Funktional λ kann einen Vektor „fressen“ und eine Zahl „ausspucken“. Der elementare Tensor $v \otimes \lambda$ hat also gewissermaßen einen Eingang für Vektoren aus V. Wird er gefüttert, so spuckt die erste Komponente λ einen Skalar aus, der dann mit der zweiten Komponente v zu einem Vektor aus V weiterverarbeitet werden kann. Der Tensor $v \otimes \lambda$ kann also einen Vektor fressen, und spuckt dann wieder einen Vektor aus - kommt uns das nicht bekannt vor?

Proposition 10.1.16 ((1,1)-Tensoren als Endomorphismen)**.** *Ist V endlichdimensional, so existiert ein eindeutiger Vektorraumisomorphismus*

$$i : V \otimes V^* \to \mathrm{End}_{\mathbb{K}}(V), \quad \textit{so dass} \quad \imath(v \otimes \lambda)(w) = \lambda(w)v \quad (\lambda \in V^*, v, w \in V). \tag{10.1.1}$$

Unter diesem Isomorphismus entspricht die Verkettung von Endomorphismen der Operation

$$(v_1 \otimes \lambda_1) \circ (v_2 \otimes \lambda_2) = \lambda_1(v_2) \cdot (v_1 \otimes \lambda_2).$$

auf elementaren Tensoren.

Beweis. Die Abbildung $i_0 : V^* \times V \to \mathrm{End}_{\mathbb{K}}(V)$, gegeben durch $i_0(v,\lambda)(w) := \lambda(w)v$, ist bilinear und setzt sich daher eindeutig zu einer linearen Abbildung i fort, die durch die Formel (10.1.1) auf elementaren Tensoren eindeutig bestimmt ist. Um zu sehen, dass i bijektiv ist, sei $(v_1, \ldots, v_n)$ eine geordnete Basis von V und $(v_1^*, \ldots, v_n^*)$ die duale Basis von V^*. Es gilt dann

$$i\left(\sum_{i=1}^n \sum_{j=1}^n \alpha_{ij}(v_i \otimes v_j^*)\right)(w) = \sum_{i=1}^n \left(\sum_{j=1}^n \alpha_{ij} v_j^*(w)\right) v_i.$$

Ist dieser Ausdruck gleich 0 für alle $w \in V$, so folgt aus der linearen Unabhängigkeit der v_i, dass

$$\sum_{j=1}^n \alpha_{ij} v_j^*(w) = 0$$

für alle $w \in V$. Wählt man nun speziell $w := v_i$ so erhält man $\alpha_{ij} = 0$. Diese zeigt, dass i injektiv ist, und aus Dimensionsgründen ist i dann auch surjektiv. Schließlich gilt

$$\begin{aligned}(i(v_1 \otimes \lambda_1) \circ i(v_2 \otimes \lambda_2))(w) &= \lambda_1(\lambda_2(w)v_2)v_1 = \lambda_1(v_2) \cdot \lambda_2(w)v \\ &= \imath(\lambda_1(v_2) \cdot v_1 \otimes \lambda_2)(w).\end{aligned}$$

Damit ist alles gezeigt. □

Bemerkung 10.1.17 ((1,1)-Tensoren in Koordinaten)**.** Betrachtet man $V := \mathbb{K}^n$ mit der Standardbasis $(e_1, \ldots, e_n)$ und der zugehörigen dualen Basis $(e_1^*, \ldots, e_n^*)$, so ist der obige Isomorphismus gegeben durch

$$i(e_i \otimes e_j^*) = E_{ij},$$

wobei E_{ij} durch die Matrix mit Eintrag 1 an der Stelle (i,j) und allen anderen Einträgen 0 ist. Ist nun $\lambda \in V^*$, so existiert ein $w \in V$ mit $\lambda(v) = w^\top v$. Die darstellende Matrix von $i(v \otimes \lambda)$ bzgl. der Standardbasis ist dann gegeben durch die Matrix

$$v \cdot w^\top \in \mathbb{K}^{n \times n}.$$

Eine solche Matrix hat stets Rang ≤ 1. *Elementare Tensoren entsprechen also Matrizen vom Rang* ≤ 1. Nur die wenigsten (1,1)-Tensoren (=Matrizen) sind also elementar, aber jeder Tensor (bzw. jede Matrix) lässt sich als Linearkombination von elementaren Tensoren (bzw. Matrizen vom Rang ≤ 1) schreiben.

Übung 10.1.18. Die Abbildung $V \times V^* \to \mathbb{K}$, $(v, \lambda) \mapsto \lambda(v)$ ist bilinear, induziert also eine lineare Abbildung

$$\mathrm{End}_{\mathbb{K}}(V) \cong V \otimes V^* \to \mathbb{K}.$$

Unter welchem Namen ist Ihnen diese lineare Abbildung bekannt?

Als Warnung - insbesondere für Studierende mit Nebenfach Physik - wollen wir noch das Folgende ansprechen:

Bemerkung 10.1.19 („Erhöhen und Absenken von Indizes“)**.** Ist $B : V \times V \to \mathbb{K}$ eine nichtausgeartete Bilinearform, so liefert B einen Isomorphismus $\iota_B : V \to V^*$. Die bilinearen Abbildung

$$V \times V \xrightarrow{\mathrm{Id} \times \iota_B} V \times V^* \xrightarrow{\iota_B \times \mathrm{Id}} V^* \times V^*$$

induzieren dann Isomorphismen

$$V \otimes V \cong V \otimes V^* \cong V^* \otimes V^*.$$

Nach Wahl einer solchen Bilinearform kann man also (2,0)-Tensoren, (1,1)-Tensoren und (0,2)-Tensoren identifizieren und diese wiederum mit Endomorphismen bzw. Bilinearformen. In der Physik und der Differentialgeometrie ist es üblich, solche Identifikationen stillschweigend durchzuführen (und gelegentlich noch die Bilinearform zu verschweigen). Wählt man jeweils die Standardbasen im $\mathbb{K}^n$ und die Standardbilinearform, dann führt das in lokalen Koordinaten zu keinerlei Schwierigkeiten, aber wenn die Bilinearform komplizierter ist, sollte man sich in Ruhe überlegen, wie genau diese Identifikationen funktionieren.

Bemerkung 10.1.20 (Höhere Tensoren)**.** Fast unsere gesamte Lineare Algebra hat von Tensoren vom totalen Grad 2 gehandelt - Endomorphismen und Bilinearformen. Bei den Determinanten haben wir ausnahmsweise auch Tensoren vom Typ $(0,n)$ verwendet. Wie stellt man sich nun Tensoren von beliebigem Typ vor? Ein Tensor vom Typ (1,2) hat z.B. 2 Eingänge und einen Ausgang: Wenn man zwei Vektoren ‘reinsteckt, kommt ein Vektor ‘raus. Die zugehörige Matrix ist dann kein Quadrat mehr, sondern ein drei-dimensionaler Quader - man muss ja nun $(\dim V)^3$ statt $(\dim V)^2$ Zahlen abspeichern.

In natürlicher Weise tauchen höhere Tensoren vor allem in der Differentialgeometrie auf. So ist die Krümmung einer Riemannschen Mannigfaltigkeit in jedem Punkt ein (0,4)-Tensor. Alternierende k-Tensoren (sogenannte k-Formen) können verwendet werden, um k-dimensionale

Volumina zu definieren. Dies sind Objekte, die man über k-dimensionale Untermannigfaltigkeiten integrieren kann - 1-Formen kann man entlang Kurven integrieren, 2-Formen über Flächen integrieren usw. Mehr dazu in einer Vorlesung über DIFFERENTIALGEOMETRIE.

Notation 10.1.21 (Tensorprodukte über verschiedenen Körpern)**.** Ist V ein Vektorraum über einem Körper $\mathbb{L}$ und ist $\mathbb{K}$ ein Unterkörper von $\mathbb{L}$, so können wir V auch als $\mathbb{K}$-Vektorraum auffassen. Ist W ein weiterer $\mathbb{L}$-Vektorraum, so ist es wichtig, zwischen $\mathbb{L}$-linearen und $\mathbb{K}$-linearen Abbildungen von V nach W zu unterscheiden. Analog muss man auch sorgfältig zwischen $\mathbb{L}$-multilinearen und $\mathbb{K}$-multilinearen Abbildungen unterscheiden. Entsprechend kann mman nun für V und W das Tensorprodukt $V \otimes_{\mathbb{L}} W$ und das Tensorprodukt $V \otimes_{\mathbb{K}} W$ unterscheiden: Ersteres ist ein $\mathbb{L}$-Vektorraum, kommt mit einer $\mathbb{L}$-linearen Abbildung $\iota_{\mathbb{L}} : V \times W \to V \otimes_{\mathbb{L}} W$ und setzt $\mathbb{L}$-bilineare Abbildungen $\mathbb{L}$-linear fort, letzteres ist ein $\mathbb{K}$-Vektorraum, kommt mit einer $\mathbb{K}$-linearen Abbildung $\iota_{\mathbb{K}} : V \times W \to V \otimes_{\mathbb{K}} W$ und setz $\mathbb{K}$-bilineare Abbildungen $\mathbb{K}$-linear fort.

Alle wichtigen Konstruktionen der linearen Algebra, wie z.B. die direkte Summe und die Konstruktion von Quotientenvektorräumen sind in einem geeigneten Sinne verträglich mit linearen Abbildungen. Dies ist auch für das Tensorprodukt der Fall:

Konstruktion 10.1.22 (Tensorprodukt von linearen Abbildungen)**.** Nachdem wir uns überlegt haben, dass man mittels Tensorprodukt aus zwei (endlichdimensionalen) $\mathbb{K}$-Vektorräumen V, W einen neuen Vektorraum $V \otimes W$ basteln kann, wollen wir uns nun fragen, wie diese Konstruktion mit linearen Abbildungen verträglich ist. Dazu betrachten wir die folgende Situation: Es (V_1, W_1) und (V_2, W_2) zwei Paare von $\mathbb{K}$-Vektorräumen und $f : V_1 \to V_2$ und $g : W_1 \to W_2$ zwei $\mathbb{K}$-lineare Abbildungen. Wir schreiben $\iota_1 : V_1 \times W_1 \to V_1 \otimes W_1$ bzw. $\iota_2 : V_2 \times W_2 \to V_2 \otimes W_2$ für die kanonischen Abbildungen.

Da f und g linear sind, ist die Abbildung

$$f \times g : V_1 \times W_1 \to V_2 \times W_2, \quad (v, w) \mapsto (f(v), g(w))$$

bilinear. Daher ist auch die Verkettung

$$\iota_2 \circ (f \times g) : V_1 \times W_1 \xrightarrow{f \times g} V_2 \times W_2 \xrightarrow{\iota_2} V_2 \otimes W_2, \quad (v, w) \mapsto f(v) \otimes g(w).$$

bilinear, und nach der universellen Eigenschaft von $(V_1 \otimes W_1, \iota_1)$ existiert eine eindeutige lineare Fortsetzung

$$f \otimes g : V_1 \otimes W_1 \to V_2 \otimes W_2, \quad v \otimes w \mapsto f(v) \otimes g(w).$$

Wir nennen $f \otimes g$ das *Tensorprodukt* von f und g. Wenn wir die Abhängigkeit vom Grundkörper $\mathbb{K}$ betonen wollen, schreiben wir auch $f \otimes_{\mathbb{K}} g$ statt $f \otimes g$.

Nach Definition ist $f \otimes g$die eindeutige lineare Abbildung, so dass das Diagramm

$$\begin{array}{ccc} V_1 \times W_1 & \xrightarrow{f \times g} & V_2 \times W_2 \\ \downarrow{\scriptstyle \iota_1} & & \downarrow{\scriptstyle \iota_2} \\ V_1 \otimes W_1 & \xrightarrow{f \otimes g} & V_2 \otimes W_2 \end{array}$$

kommutiert. Insbesondere gilt: Sind f und g Isomorphismen, so ist auch $f \times g$ ein Isomorphismus (mit inversem Isomorphismus $f^{-1} \times g^{-1}$) und daher auch $f \otimes g$ ein Isomorphismus (mit inversem Isomorphismus $f^{-1} \otimes g^{-1}$). Insbesondere hängt das Tensorprodukt von V und W bis auf Isomorphie nur von den Isomorphieklassen von V und W ab.

Wir wollen nun noch eine für die lineare Algebra wichtige Anwendung des Tensorprodukts von Abbildungen diskutieren. Zur Motivation betrachten wir das folgende Problem:

Bemerkung 10.1.23. Ist $A \in \mathbb{R}^{n\times n}$ eine reelle Matrix, so können wir A auch als komplexe Matrix in $\mathbb{C}^{n\times n}$ auffassen. Dann definiert A sowohl eine reell-lineare Abbildung $\Phi_{\mathbb{R}} : \mathbb{R}^n \to \mathbb{R}^n$ als auch eine komplex-lineare Abbildung $\Phi_{\mathbb{C}} : \mathbb{C}^n \to \mathbb{C}^n$, und diesen Sachverhalt haben wir uns sehr oft zunutze gemacht.

Hat hat man nun eine abstrakte reell-lineare Abbildung $\Phi_{\mathbb{R}} : V \to W$ zwischen endlichdimensionalen reellen Vektorräumen, so kann man Basen wählen und Φ bzgl. dieser Basen durch eine Matrix A darstellen. Diese Matrix kann man dann wieder als komplexe Matrix auffassen, und damit eine komplex-lineare Abbildung zwischen komplexen Vektorräumen definieren. Diese Konstruktion hängt aber von einer Vielzahl von Wahlen ab. Kann man das ganze auch kanonischer machen, also ohne so viele Wahlen zu treffen?

Beispiel 10.1.24 (Von $\mathbb{R}^n$ zu $\mathbb{C}^n$)**.** Wir betrachten die Abbildung $m : \mathbb{C} \times \mathbb{R}^n \to \mathbb{C}^n$ gegeben durch $m(z,v) := zv = (zv_1, \dots, zv_n)^\top$. Diese ist $\mathbb{R}$-bilinear und induziert daher eine $\mathbb{R}$-lineare Abbildung

$$\mu : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \to \mathbb{C}^n.$$

Diese ist eindeutig bestimmt durch die Formel

$$\mu(z \otimes_{\mathbb{R}} v) = zv.$$

Wir behaupten, dass μ sogar ein *Isomorphismus* von $\mathbb{R}$-Vektorräumen ist. Wegen

$$\dim_{\mathbb{R}} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n = \dim_{\mathbb{R}}(\mathbb{C}) \dim_{\mathbb{R}}(\mathbb{R}^n) = 2n = \dim_{\mathbb{R}}(\mathbb{C}^n)$$

genügt es zu zeigen, dass Bild(μ) eine $\mathbb{R}$-Basis von $\mathbb{C}^n$ enthält, denn dann ist μ surjektiv, also bijektiv. Nun gilt aber

$$\mu[\{1 \otimes_{\mathbb{R}} e_1, i \otimes_{\mathbb{R}} e_1, \dots 1 \otimes_{\mathbb{R}} e_n, i \otimes_{\mathbb{R}} e_n\}] = \{e_1, ie_1, \dots, e_n, ie_n\},$$

und diese Menge ist offensichtlich eine $\mathbb{R}$-Basis von $\mathbb{C}^n$. Wir sehen also, dass $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \times \mathbb{C}^n$ via μ.

Der $\mathbb{R}$-Vektorraum $\mathbb{C}^n$ ist in natürlicher Weise ein $\mathbb{C}$-Vektorraum, und wir können den Isomorphismus μ benutzen, um diese Struktur auf $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$ zu übertragen. Dies liefert dann die Struktur eines $\mathbb{C}$-Vektorraums auf $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$. Ist $w \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$ und $z \in \mathbb{C}$, so definieren wir also $zw \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$ als das eindeutige Element mit $\mu(zw) = z\mu(w)$. Wie kann man sich zw konkret vorstellen? Wir behaupten, dass

$$w = \sum_{j=1}^{m} z_j \otimes v_j \implies zw \sum_{j=1}^{m} (zz_j) \otimes v_j. \tag{10.1.2}$$

Insbesondere hängt dieser Ausdruck nicht von der gewählten Darstellung von w als Summe elementarer Tensoren ab. In der Tat rechnet man sofort nach, dass

$$z\mu(w) = z \sum_{j=1}^{m} z_j v_j = \sum_{j=1}^{m} (zz_j) v_j = \mu(zw).$$

Definieren wir die komplexe Skalarmultiplikation auf $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$ durch (10.1.2), so ist also μ ein Isomorphismus von $\mathbb{C}$-Vektorräumen $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$.

Beispiel 10.1.24 gibt uns nun eine Idee, wie man ganz allgemein aus einem $\mathbb{R}$-Vektorraum einen $\mathbb{C}$-Vektorraum machen kann.

Konstruktion 10.1.25 (Komplexifizierung reeller Vektorräume)**.** Es sei V ein endlichdimensionaler $\mathbb{R}$-Vektorraun. Wir definieren die *Komplexifizierung* von V als

$$V_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V.$$

Wir wählen nun eine geordnete $\mathbb{R}$-Basis $(v_1, \dots, v_n)$ von V. Eine geordnete $\mathbb{R}$-Basis von $V_{\mathbb{C}}$ ist dann gegeben durch $(1 \otimes_{\mathbb{R}} v_1, i \otimes_{\mathbb{R}} v_1, \dots, 1 \otimes_{\mathbb{R}} v_n, i \otimes_{\mathbb{R}} v_n)$ eine geordnete $\mathbb{R}$-Basis von $V_{\mathbb{C}}$.

Wir wollen nun $V_{\mathbb{C}}$ wie in Beispiel 10.1.24 zu einem $\mathbb{C}$-Vektorraum machen. Dazu betrachten wir für festes $w \in \mathbb{C}$ zunächst die Abbildung

$$\lambda_w^o : \mathbb{C} \times V \to V_{\mathbb{C}}, \quad (z, v) \mapsto (wz) \otimes v.$$

Da $\mathbb{C}$ eine $\mathbb{R}$-Algebra ist, ist die Abbildung $\mathbb{C} \to \mathbb{C}$, $z \mapsto wz$ $\mathbb{R}$-linear, und folglich ist λ_w^o $\mathbb{R}$-bilinear. Nach der universellen Eigenschaft der Tensorprodukts existiert dann eine eindeutige $\mathbb{R}$-lineare Abbildung

$$\lambda_w : V_{\mathbb{C}} \to V_{\mathbb{C}} \quad \text{mit} \quad z \otimes v \mapsto (wz) \otimes v$$

Wir definieren nun eine Multiplikation

$$\mathbb{C} \times V_{\mathbb{C}} \to V_{\mathbb{C}}, \quad (w, \tau) \mapsto w \cdot \tau := \lambda_w(\tau).$$

Für die obigen Basisvektoren gilt z.B. für alle $a, b \in \mathbb{R}$, dass

$$(a + bi) \cdot (1 \otimes_{\mathbb{R}} v_j) = a(1 \otimes_{\mathbb{R}} v_j) + b(i \otimes_{\mathbb{R}} v_j) \quad \text{und} \quad (a + bi) \cdot (i \otimes_{\mathbb{R}} v_j) = -b(1 \otimes_{\mathbb{R}} v_j) + a(i \otimes_{\mathbb{R}} v_j).$$

Es ist nun eine Routinerechnung zu überprüfen, dass $V_{\mathbb{C}}$ mit dieser Skalarmultiplikation wieder ein $\mathbb{C}$-Vektorraum ist. Wir nennen diesen die *Komplexifizierung* von V.

Allgemein stellen wir fest: Ist w reell, so ist

$$w \cdot (z \otimes_{\mathbb{R}} v) = (wz) \otimes_{\mathbb{R}} v = z \otimes_{\mathbb{R}} (wv),$$

d.h. die reellen Skalare wirken auf Vektoren aus V wie bisher und ignorieren den ersten Faktor. Insbesondere erhalten wir einen Monomorphismus von $\mathbb{R}$-Vektorräumen

$$V \to V_{\mathbb{C}}, \quad v \mapsto 1 \otimes v,$$

genannt die *kanonische Einbettung*. Die nicht-reellen komplexen Zahlen verarzten wir geeignet mit dem ersten Faktor. Es gilt dann insbesondere

$$\mathbb{C} \cdot (1 \otimes v_j) = \mathbb{R} \cdot 1 \otimes v_j \oplus \mathbb{R} \cdot i \otimes v_j.$$

Inbesondere ist $(1 \otimes v_1, \dots, 1 \otimes v_n)$ eine $\mathbb{C}$-Basis des $\mathbb{C}$-Vektorraums $V_{\mathbb{C}}$. Diese Basis ist in kanonischer Bijektion mit unserer alten Basis (insbesondere gilt also $\dim_{\mathbb{C}} V_{\mathbb{C}} = \dim_{\mathbb{R}} V$), aber wir dürfen jetzt eben mit komplexen (statt reellen) Skalaren multiplizieren.

Das entscheidende an dieser Konstruktion ist nun, dass $V_{\mathbb{C}}$ unabhängig von der Wahl einer Basis von V konstruiert wurde. Als Konsequenz induziert jede beliebige $\mathbb{R}$-Basis $(w_1, \dots, w_n)$ von V eine $\mathbb{C}$-Basis $(1 \otimes w_1, \dots, 1 \otimes w_n)$ von $V_{\mathbb{C}}$. Man hängt also einfach an jeden Basisvektor ein „Säckchen“, in das man bei Bedarf die komplexen Skalare einpacken kann.

[12.06.24]

Konstruktion 10.1.26 (Komplexifizierung einer reell-linearen Abbildung)**.** Es seien nun V und W zwei $\mathbb{R}$-Vektorräume und $f : V \to W$ eine $\mathbb{R}$-lineare Abbildung. Die $\mathbb{R}$-bilineare Abbildung

$$\mathrm{Id} \times f : \mathbb{C} \times V \to \mathbb{C} \times W$$

setzt sich dann fort zu einer $\mathbb{R}$-linearen Abbildung

$$f_{\mathbb{C}} := \mathrm{Id} \otimes_{\mathbb{R}} f : V_{\mathbb{C}} \to W_{\mathbb{C}}.$$

Diese ist eindeutig durch die Bilder der elementaren Tensoren festgelegt, und nach Konstruktion gilt

$$f_{\mathbb{C}}(z \otimes_{\mathbb{R}} v) = z \otimes_{\mathbb{R}} f(v). \tag{10.1.3}$$

Aus (10.1.3) folgt nun, dass $f_{\mathbb{C}}$ sogar $\mathbb{C}$-linear ist. Da $f_{\mathbb{C}}$ additiv ist, genügt es, die Multiplikativität unter komplexen Skalaren für elementare Tensoren nachzurechnen. Es gilt aber

$$z' \cdot f_{\mathbb{C}}(z \otimes_{\mathbb{R}} v) = z' \cdot (z \otimes_{\mathbb{R}} f(v)) = (z'z) \otimes_{\mathbb{R}} f(v) = f_{\mathbb{C}}((z'z) \otimes_{\mathbb{R}} v) = f_{\mathbb{C}}(z' \cdot (z \otimes_{\mathbb{R}} v)).$$

Zu jeder $\mathbb{R}$-linearen Abbildung $f : V \to W$ gibt es also eine $\mathbb{C}$-lineare Abbildung $f_{\mathbb{C}} : V_{\mathbb{C}} \to W_{\mathbb{C}}$, und man überlegt sich leicht, dass dies die eindeutige $\mathbb{C}$-lineare Abbildung ist, so dass das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow & & \downarrow \\ V_{\mathbb{C}} & \xrightarrow{f_{\mathbb{C}}} & W_{\mathbb{C}} \end{array}$$

kommutiert. Wählen wir nun $\mathbb{R}$-Basen von V und W und die entsprechenden $\mathbb{C}$-Basen von $V_{\mathbb{C}}$ und $W_{\mathbb{C}}$, so besitzen f und $f_{\mathbb{C}}$ dieselbe darstellende Matrix (einmal aufgefasst als reelle und das andere Mal als komplexe Matrix). Dabei spielt es keine Rolle, welche Basen wir für V und W wählen - die Konstruktion ist komplett kanonisch, d.h. unabhängig von der Basiswahl.

Konstruktion 10.1.27 ($\mathbb{L}$-ifizierung)**.** Ganz allgemein zeigt das obige Argument: Ist $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$ mit[4] $\dim_{\mathbb{K}} \mathbb{L} < \infty$, so kann man für jeden $\mathbb{K}$-Vektorraum V die $\mathbb{L}$-*ifizierung* $V_{\mathbb{L}} := \mathbb{L} \otimes_{\mathbb{K}} V$ definieren. Diese ist ein $\mathbb{L}$-Vektorraum, wobei die Skalarmultiplikation durch die Formel

$$l' \cdot (l \otimes v) := (l'l) \otimes v$$

eindeutig bestimmt ist. Ist $f : V \to W$ eine $\mathbb{K}$-lineare Abbildung, so erhalten wir eine kanonische $\mathbb{L}$-lineare Abbildung $f_{\mathbb{L}} : V_{\mathbb{L}} \to W_{\mathbb{L}}$ mit $f_{\mathbb{L}}(l \otimes v) = l \otimes f(v)$.

Implizit haben wir diese Konstruktion bereits seit den Anfänge dieser Vorlesung benutzt, nämlich immer dann, wenn wir eine Matrix über einem Körper $\mathbb{K}$ als Matrix über einem größeren Körper $\mathbb{L}$ aufgefasst haben (und das war sehr oft!). Damals mussten wir immer einige Verrenkungen machen: Wir haben lineare Abbildungen durch Basiswahl in Matrizen übersetzt, diese Matrizen uminterpretiert und dann wieder als lineare Abbildungen aufgefasst. Wenn man mit dem Tensor-Formalismus vertraut ist, sind solche Verrenkungen nicht mehr nötig.

[4] Diese unnötige Annahme werden wir im nächsten Abschnitt loswerden.

Zusammenfassung von Abschnitt 10.1.

(1) Das Tensorprodukt endlichdimensionaler Vektorräumen ist ein endlichdimensionaler Vektorraum, der durch eine universelle Eigenschaft definiert ist, die es erlaubt, multilineare Abbildungen in lineare umzuwandeln. Seine Dimension ist das Produkt der Dimensionen der Ausgangsräume.

(2) Elemente des Tensorprodukts heißen Tensoren und können als Summen sogenannter elementarer Tensoren geschrieben werden. Nicht jeder Tensor ist elementar!

(3) Multilinearformen und Endomorphismen können als spezielle Tensoren aufgefasst werden.

(4) Lineare Abbildungen zwischen Vektorräumen induzieren lineare Abbildungen zwischen den entsprechenden Tensorprodukten.

(5) Mittels Tensorprodukt kann man jedem reellen Vektorraum eine Komplexifizierung und jeder reell-linearen Abbildung eine komplex-lineare Abbildung zwischen den Komplexifizierungen zuordnen. Dieselbe Konstruktion funktioniert für beliebige Körpererweiterungen.

10.2 Einschub: Unendlichdimensionale Vektorräume

Bevor wir uns weiter mit Tensorprodukten beschäftigen können, benötigen wir ein wenig Hintergrundmaterial über unendlichdimensionale Vektorräume. Wir haben diese bislang sehr stiefmütterlich behandelt. Für die elementare lineare Algebra sind sie nicht von entscheidender Bedeutung, aber irgendwann kommt man nicht mehr an ihnen vorbei. Alles, was wir in diesem Abschnitt sagen, hätten wir auch schon im ersten Teil der Vorlesung sagen können, wir haben dies aber bewusst vermieden, insbesondere haben wir unendliche Basen nicht ausführlich diskutiert. Wir holen dies nun nach und kehren dazu im Wesentlichen noch einmal zu Abschnitt 2.4 zurück. Wir wollen vor allem auf die Unterschiede eingehen, dies sich zwischen dem endlichdimensionalen und dem unendlichdimensionalen Fall ergeben. Im Folgenden sei $\mathbb{K}$ ein Körper. Wir interessieren uns für Vektorräume der folgenden Form:

Notation 10.2.1. Ist M eine nicht-leere Menge, so schreiben wir $\mathbb{K}^M$ für den Vektorraum der Abbildungen von M nach $\mathbb{K}$ mit Addition und Skalarmultiplikation gegeben durch

$$(f+g)(m) := f(m) + g(m) \quad \text{und} \quad (\lambda f)(m) := \lambda f(m) \quad (f, g \in \mathbb{K}^M, m \in M, \lambda \in \mathbb{K}).$$

Wir schreiben dann δ_m für das Element von $\mathbb{K}^M$ mit $\delta_m(m') = \delta_{mm'}$ für alle $m' \in M$.

Beispiel 10.2.2 (Der endliche Fall)**.** Ist M endlich, so ist $\{\delta_m \mid m \in M\}$ eine Basis von $\mathbb{K}^M$, und daher ist $\mathbb{K}^M$ endlichdimensional mit $\dim \mathbb{K}^M = |M|$. Für $f \in \mathbb{K}^m$ gilt dann

$$f = \sum_{m \in M} f(m)\delta_m, \tag{10.2.1}$$

d.h. die Funktionswerte von f sind genau die Koordinaten von f bzgl. der obigen Basis.

Bemerkung 10.2.3. Es ist wichtig sich klarzumachen, dass Beispiel 10.2.2 für unendliche Mengen M so nicht funktioniert. Ist nämlich $f \in \mathbb{K}^M$, so könnte man zunächst versucht sein, f wieder wie in (10.2.1) darzustellen, aber Vorsicht! Wir machen hier Algebra und keine Analysis,

d.h. uns stehen nur *endliche* und keine *unendlichen* Summen zur Verfügung. Wann ist eine Funktion $f \in \mathbb{K}^M$ nun als *endliche* Linearkombination der Funktionen δ_m darstellbar? Da die Funktionen δ_m nur an einem Punkt von 0 verschieden sind, ist dies offensichtlich genau dann der Fall, wenn

$$f \in \mathbb{K}^{(M)} := \{f \in \mathbb{K}^M \mid f(m) = 0 \text{ für alle bis auf endlich viele } m \in M\}.$$

Ist M endlich, so gilt natürlich $\mathbb{K}^{(M)} = \mathbb{K}^M$, aber für unendliche M ist $\mathbb{K}^{(M)} = \langle \delta_m \mid m \in M \rangle$ ein echter Unterraum von $\mathbb{K}^M$. Dieser Vektorraum ist im Allgemeinen sogar „beträchtlich kleiner“ als der $\mathbb{K}^M$.

Beispiel 10.2.4. Es sei $\mathbb{K}$ ein endlicher Körper. Wir behaupten, dass die Menge $\mathbb{K}^{(\mathbb{N})}$ abzählbar ist, dass also eine Bijektion $\mathbb{N} \to \mathbb{K}^{(\mathbb{N})}$ existiert. Das sieht man so: Für $f \in \mathbb{K}^{(\mathbb{N})}$ definieren wir den *Träger* (engl. „support“) $\operatorname{supp}(f)$ von f als die endliche(!) Menge

$$\operatorname{supp}(f) := \{m \in M \mid f(m) \neq 0\} \subseteq \mathbb{N}$$

Wir setzen $n(f) := \max \operatorname{supp}(f) \in \mathbb{N}$. Für jedes feste $n \in \mathbb{N}$ gibt es nur endlich viele f mit $n(f) = n$. Wir nummerieren die $f \in \mathbb{K}^{(\mathbb{N})}$ mit $n(f) = 1$ durch als $f_1, \ldots, f_{n_1}$. Anschließend nummerieren wir die $f \in \mathbb{K}^{(\mathbb{N})}$ mit $n(f) = 1$ durch als $f_{n_1+1}, \ldots, f_{n_2}$ usw. Es gilt dann

$$\mathbb{K}^{(\mathbb{N})} = \{f_1, f_2, \ldots\},$$

also ist $\mathbb{K}^{\mathbb{N}}$ abzählbar.

Wir behaupten, dass die Menge $\mathbb{K}^{\mathbb{N}}$ überabzählbar (also unendlich und nicht abzählbar) ist. Wir nehmen der Einfachheit halber an, dass $|\mathbb{K}| \geq 10$ gilt, etwa $\mathbb{K} = \{x_0, x_2, \ldots, x_q\}$ mit $q \geq 9$. Wir betrachten nun die Teilmenge $G := \{(z_1, z_2, \ldots) \in \mathbb{K}^{\mathbb{N}} \mid z_j \in \{x_0, \ldots, x_9\}\}$. Die Abbildung

$$G \to [0,1), \quad (x_{i_1}, x_{i_2}, \ldots) \mapsto 0, i_1 i_2 \ldots$$

ist dann surjektiv, es gilt also $\mathbb{K}^{\mathbb{N}} \geq G \geq [0,1)$, und die Menge $[0,1)$ ist nach dem zweiten Cantorschen Diagonalargument überabzählbar. Daher ist auch $\mathbb{K}^{\mathbb{N}}$ überabzählbar und in diesem Sinne „echt größer als $\mathbb{K}$.

Übung 10.2.5. Zeigen Sie: Ist $\mathbb{K}$ abzählbar, so ist $\mathbb{K}^{(\mathbb{N})}$ noch immer abzählbar, aber $\mathbb{K}^{\mathbb{N}}$ ist überabzählbar.

Bemerkung 10.2.6. Wir erinnern daran, dass eine (möglicherweise unendliche) Teilmenge B eines Vektorraums *endlich linear unabhängig* heißt, wenn sie leer ist oder für alle $n \in \mathbb{N}$ alle paarweise verschiedenen $b_1, \ldots, b_n \in B$ linear unabhängig sind (vgl. Definition 2.4.16). Die Teilmenge $\{\delta_m \mid m \in M\}$ ist nach Beispiel 10.2.1 linear unabhängig, aber kein Erzeugendensystem von $\mathbb{K}^M$. Sie ist aber ein endlich linear unabhängiges Erzeugendensystem von $\mathbb{K}^{(M)}$. Wir erinnern daran, dass das genau unsere Definition einer Basis ist. Der Raum $\mathbb{K}^{(M)}$ besitzt also eine „Standardbasis“ $\{\delta_m \mid m \in M\}$.

Für den Vektorraum $\mathbb{K}^M$ ist es hingegen nicht ohne Weiteres möglich, eine Basis anzugeben. Wir wollen uns nun überlegen, wieso das so schwierig ist. Es ist hilfreich, die folgende Notation zu verwenden.

Notation 10.2.7 (Formal unendliche Summen)**.** Ist V ein $\mathbb{K}$-Vektorraum, so schreiben wir

$$V^{(M)} := \{f : V \to M \mid f(m) = 0 \text{ für alle bis auf endlich viele } m \in M\}.$$

Ist $f \in V^{(M)}$, so definieren wir den *Träger* (engl. „support“) von f als die endliche Menge

$$\operatorname{supp}(f) := \{m \in M \mid f(m) \neq 0\}.$$

Wir definieren dann die *formal unendliche Summe* über f (analog zu Bemerkung 5.4.1) als

$$\sum_{m \in M} f(m) := \sum_{m \in \operatorname{supp}(f)} f(m).$$

Man beachte, dass die Summe auf der rechten Seite endlich ist, wir summieren also de facto nur endlich viele Terme (auch wenn die Summe auf der linken Seite rein formal wie eine unendliche Summe aussieht).

Mit dieser Notation können wir Satz 2.4.17 wie folgt formulieren:

Satz 10.2.8 (Charakterisierung von Basen)**.** *Für eine Teilmenge $B \subseteq V$ sind die folgenden Aussagen äquivalent:*

(i) B ist eine Basis von V (d.h. ein endlich linear unabhängiges Erzeugendensystem).

(ii) B ist ein Erzeugendensystem von V und keine echte Teilmenge $B' \subsetneq B$ ist ein Erzeugendensystem.

(iii) B ist ein Erzeugendensystem und jede endliche Teilmenge $B' \subseteq B$ ist eine endliche Basis von $\langle B' \rangle$.

(iv) Für jedes $v \in V$ existiert ein eindeutiges $\lambda_v \in \mathbb{K}^{(V)}$ mit

$$v = \sum_{b \in B} \lambda_v(b) b. \tag{10.2.2}$$

(v) B ist endlich linear unabhängig und $B \cup \{v\}$ ist nicht endlich linear unabhängig für jedes $v \in V \setminus B$.

Man beachte, dass wegen $\lambda_v \in \mathbb{K}^{(V)}$ die Summe in (10.2.2) nur formal unendlich ist.

Bemerkung 10.2.9 (Modelle für unendlichdimensionale Vektorräume)**.** Ist B eine Basis von V, so erhalten wir mittels (10.2.2) eine injektive Abbildung

$$V \to \mathbb{K}^{(B)}, \quad v \mapsto \lambda_v.$$

Diese ist sogar bijektiv mit Umkehrabbildung

$$\lambda \mapsto \sum_{b \in B} \lambda(b) b,$$

und man rechnet nach, dass sie auch linear ist. Die Wahl einer Basis B liefert also einen Isomorphismus $V \to \mathbb{K}^{(B)}$. Umgekehrt liefert jeder Isomorphismus $V \to \mathbb{K}^{(M)}$ eine Basis (das Urbild der Standardbasis von $\mathbb{K}^{(M)}$). In diesem Sinne entsprechen Basen also Wahlen von Isomorphismen in einen „Modellraum“ $\mathbb{K}^{(M)}$.

Wie in der LA 1 erwähnt, kann man in gewissen Modellen der Mengenlehre abstrakt zeigen, dass jeder Vektorraum eine Basis besitzt (und daher isomorph zu einem Modellraum $\mathbb{K}^{(M)}$ ist)[5], aber der Beweis ist nicht konstruktiv. In diesen Modellen gilt insbesondere $\mathbb{K}^M \cong \mathbb{K}^{(M')}$ für eine Menge M', aber es wird Ihnen nicht gelingen, einen expliziten Isomorphismus anzugeben. Ist $\mathbb{K}$ endlich, so folgt aus Beispiel 10.2.4 dass eine Basis von $\mathbb{K}^{\mathbb{N}}$ überabzählbar sein muss. Allgemeiner kann man zeigen: Ist M' eine Basis für $\mathbb{K}^M$ mit M unendlich, so ist M' echt mächtiger als M, d.h. es existiert eine Surjektion von M' auf M, aber keine Surjektion von M auf M'.

Notation 10.2.10 (Koordinaten)**.** Ist v wie in (10.2.2) und $b \in B$, so definieren wir die *b-Koordinate von v (bzgl. B)* als

$$b^*(v) := \lambda_v(b).$$

Man beachte, dass nach Konstruktion alle bis auf endlich viele Koordinaten 0 sind!

Im endlichdimensionalen Fall haben wir gesehen, dass die Koordinatenfunktionen $\{b^* \mid b \in B\}$ linear sind und eine Basis des Dualraums bilden. Wie sieht dies nun im unendlichdimensionalen Fall aus?

Lemma 10.2.11. *Die Koordinatenfunktionen $\{b^* \mid b \in B\}$ zu einer Basis $B \subseteq V$ sind linear und bilden eine endlich linear unabhängige Teilmene der V^*.*

Beweis. Der Beweis aus dem endlichdimensionalen Fall geht durch: Sind $v, w \in V$ mit

$$v = \sum_{b \in B} b^*(v)b \quad \text{und} \quad w = \sum_{b \in B} b^*(w)b,$$

und $\alpha, \beta \in \mathbb{K}$, so gilt

$$\alpha v + \beta w = \sum_{b \in B} (\alpha b^*(v) + \beta b^*(w))b \implies b^*(\alpha v + \beta w) = \alpha b^*(v) + \beta b^*(w),$$

also ist $b^* \in V^*$. Nach Definition gilt weiter $b^*(b') = \delta_{bb'}$ für alle $b, b' \in B$. Es bleibt zu zeigen, dass für alle paarweise verschiedenen $b_1, \ldots, b_n \in B$ die Menge $\{b_1^*, \ldots, b_n^*\} \subseteq V^*$ linear unabhängig ist. Für $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ und $j \in \{1, \ldots, n\}$ gelten die Implikationen

$$\sum_{i=1}^{n} \lambda_j b_i^* = 0 \implies \left(\sum_{i=1}^{n} \lambda_j b_i^* \right)(b_j) = 0 \implies \lambda_j = 0.$$

Damit ist alles gezeigt. □

Beispiel 10.2.12 (Keine duale Basis!)**.** Es sei $\mathbb{K}$ ein endlicher Körper und $V = \mathbb{K}^{(\mathbb{N})}$. Wir behaupten, dass dann V nicht isomorph zu V^* ist. Insbesondere gilt also: Ist B eine Basis von V, so ist $\{b^* \mid b \in B\}$ *kein* Erzeugendensystem von V^*.

Zum Beweis macht man sich klar, dass jedes $f \in \mathbb{K}^{\mathbb{N}}$ eine lineare Abbildung

$$m_f : V \to \mathbb{K}, \quad g \mapsto \sum_{n=1}^{\infty} f(n)g(n)$$

definiert, wobei die Summe wieder nur formal unendlich ist. Weiter macht man sich klar, dass die Abbildung

$$\mathbb{K}^{\mathbb{N}} \to V^*, \quad f \mapsto m_f$$

injektiv ist. Daher ist V^* überabzählbar, während V abzählbar ist, und V und V^* können daher nicht isomorph sein.

[5] Insbesondere sind die Räume $\mathbb{K}^{(M)}$ (und nicht die Räume $\mathbb{K}^M$) die natürlichen unendlichdimensionalen Verallgemeinerungen de Räume $\mathbb{K}^n$.

Das hier gesehene Phänomen gilt ganz allgemein für unendliche Mengen M (wobei der Beweis nur etwas mehr Mengenlehre benötigt): Ist V ein unendlichdimensionaler Vektorraum über einem beliebigen Körper V, so ist V^* echt mächtiger als V.

Bemerkung 10.2.13 (Bidualraum)**.** Wie im endlichdimensionalen Fall hat man ganz allgemein für jeden Vektorraum V einen Monomorphismus

$$\kappa : V \to V^{**}, \quad \kappa(v)(\lambda) := \lambda(v).$$

Der Beweis ist genau wie im endlichdimensionalen Fall. Ist V unendlichdimensional, so ist nun aber V^{**} echt mächtiger als V^* und daher echt mächtiger als V, und daher kann κ in diesem Fall niemals surjektiv sein.

Wir haben gesehen, dass sich der $\mathbb{K}^n$ auf zwei Weisen verallgemeinert, zum $\mathbb{K}^M$ (leicht zu definieren, schlechte Eigenschaften) und zum $\mathbb{K}^{(M)}$ (komplizierter zu definieren, bessere Eigenschaften). Analog verallgemeinert sich auf die direkte Summe auf zwei Arten.

Konstruktion 10.2.14 (Direktes Produkt und direkte Summe)**.** Es sei M eine Menge und für jedes $m \in M$ sei V_m ein $\mathbb{K}$-Vektorraum. Wir definieren dann das *direkte Produkt* der Vektorräume $(V_m)_{m\in M}$ wie folgt:

- Die zugrundeliegende Menge ist

  $$\prod_{m\in M} V_m := \{f : M \to \bigcup_{m\in M} V_m \mid f(m) \in V_m\}.$$

  Statt f schreiben wir auch $(f(m))_{m\in M}$ (besonders im Fall $M = \mathbb{N}$). Elemente dieser Menge sind also durch M indizierte Tupel.

- Die Vektoraddition und Skalarmultiplikation sind wieder koordinatenweise definiert, also

  $$(f+g)(m) = f(m) + g(m) \text{ und } (\lambda f)(m) = \lambda f(m) \quad (f, g \in \prod_{m\in M} V_m, \lambda \in \mathbb{K}),$$

  bzw. in der alternativen Notation

  $$(f_m)_{m\in M} + (g_m)_{m\in M} = (f_m + g_m)_{m\in M} \text{ und } \lambda(f_m)_{m\in M} = (\lambda f_m)_{m\in M}.$$

Die Vektorraumaxiome für das direkte Produkt folgen sofort aus den entsprechenden Axiomen der einzelnen V_m. Ein wichtiger Unterraum des direkten Produkts ist die *direkte Summe* der Vektorräume $(V_m)_{m\in M}$, die gegeben ist durch

$$\bigoplus_{m\in M} V_m := \{(f_m)_{m\in M} \in \prod_{m\in M} V_m \mid f(m) = 0 \text{ für alle bis auf endlich viele } m \in M\}.$$

Die Konstruktion der direkten Summe ist auf den ersten Blick wieder komplizierter als die des direkten Produkts, aber die kompliziertere Konstruktion ist wieder die bessere. Ist z.B. B_m eine Basis von V_m für jedes $m \in M$, so ist die Vereinigung dieser Basen eine Basis für die direkte Summe (nicht aber das direkte Produkt) der V_m. Weiter gilt (mit demselben Beweis wie im endlichdimensionalen Fall): Eine Teilmenge eines Vektorraums V ist genau dann eine Basis, wenn die Abbildung

$$\bigoplus_{b\in B} \mathbb{K}b \to V, \quad (\lambda_b b)_{b\in B} \to \sum_{b\in B} \lambda_b b$$

ein Isomorphismus ist. Die direkte Summe verhält sich also genau so, wie wir das aus dem endlichdimensionalen Fall gewöhnt sind.

Beachten Sie, dass für jedes $m_0 \in M$ das Bild der natürlichen Inklusion

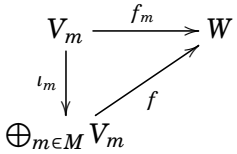
$$\iota_{m_0} : V_{m_0} \to \prod_{m \in M} V_m, \quad (\iota_{m_0}(v))(m) = \begin{cases} v, & m_0 = m \\ 0, & \text{sonst} \end{cases}$$

in der direkten Summe enthalten ist, und dass die Bilder diese Inklusionen genau die direkte Summe aufspannen.

Bemerkung 10.2.15 (Universelle Eigenschaft der direkten Summe)**.** In den Übungen werden Sie sich überlegen, dass die direkte Summe von Vektorräumen die folgende universelle Eigenschaft hat: Ist W ein fester Vektorraum und ist für jedes $m \in M$ eine lineare Abbildung $f_m : V_m \to W$ gegeben, so existiert eine eindeutige lineare Abbildung

$$f = \bigoplus_{m \in M} f_m : \bigoplus_{m \in M} V_m \to W$$

so dass für jedes $m \in M$ das Diagramm

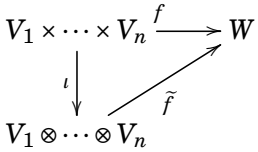


kommutiert.

Bemerkung 10.2.16 (Anwendung der universellen Eigenschaft)**.** Hier ist eine typische Anwendung dieser Eigenschaft: Ist B eine Basis eines Vektorraums V (möglicherweise unendlichdimensional) und $f_0 : B \to W$ eine beliebige Abbildung, so erhalten wir zunächst für jedes $b \in B$ eine lineare Abbildung $f_b : \mathbb{K}b \to W$ durch $f_b(\lambda b) = \lambda f_0(b)$. Da V (im Wesentlichen) die direkte Summe dieser Geraden ist, setzen sich diese Abbildungen zusammen zu einer linearen Abbildung $f : V \to W$. Dies zeigt also, dass sich jede beliebige Abbildung von einer Basis von V nach W eindeutig zu einer linearen Abbildung $V \to W$ fortsetzen lässt. Dies ist die allgemeine Version des Fortsetzungssatzes aus der Linearen Algebra I.

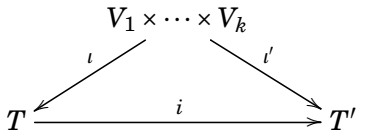
Man kann zeigen, dass auch das direkte Produkt eine universelle Eigenschaft hat (vgl. die Übungen), aber diese ist für unsere Zwecke weniger nützlich. Wir werden auf unendliche direkte Summen im nächsten Abschnitt im Zusammenhang mit der Tensoralgebra zurückkommen. Wir wollen nun aber zuerst überlegen, wie sich der Tensorformalismus des letzten Abschnitts auf den unendlichdimensionalen Fall überträgt. Die Definition eines Tensorprodukts ergibt auch im unendlichdimensionalen Fall Sinn:

Definition 10.2.17. Es seien $V_1, \ldots, V_k$ beliebige (also nicht notwendig endlichdimensionale) $\mathbb{K}$-Vektorräume. Ein *Tensorprodukt* von $V_1, \ldots V_k$ ist ein Paar $(V_1 \otimes \cdots \otimes V_k, \iota)$ bestehend aus einem $\mathbb{K}$-Vektorraum $V_1 \otimes \cdots \otimes V_k$ und einer k-linearen Abbildung $\iota : V_1 \times \cdots \times V_n \to V_1 \otimes \cdots \otimes V_n$, so dass es für jede n-lineare Abbildung $f : V_1 \times \cdots \times V_n \to W$ in einen $\mathbb{K}$-Vektorraum W eine eindeutig bestimmte lineare Abbildung $\widetilde{f} : V_1 \otimes \cdots \otimes V_n \to W$ gibt, so dass das folgende Diagramm kommutiert:



Wir sind nun in der Lage, den folgenden Satz ganz allgemein zu beweisen:

Satz 10.2.18 (Existenz und Eindeutigkeit von Tensorprodukten)**.** *Sind $V_1,\dots,V_k$ beliebige $\mathbb{K}$-Vektorräume, so existiert stets ein Tensorprodukt (T,ι) von $V_1,\dots,V_k$. Ist (T',ι') ein weiteres Tensorprodukt, so existiert ein eindeutiger Isomorphismus $i : T \to T'$, so dass das Diagramm*



kommutiert.

Der Beweis der Eindeutigkeit erfolgt wieder mittels des üblichen Highlanderarguments (Übung!). Um die Notation einfach zu halten, geben wir den Existenzbeweis nur für den Fall $k = 2$. Dafür geben wir zwei Beweise:

1. Beweis. Nach Basiswahl dürfen wir annehmen, dass $V_1 = \mathbb{K}^{(M_1)}$ und $V_2 = \mathbb{K}^{(M_2)}$ für Mengen M_1, M_2 gilt. Wir setzen dann $T := \mathbb{K}^{(M_1 \times M_2)}$ und definieren

$$\iota : V_1 \times V_2 \to T, \quad \iota(f,g)(m_1,m_2) := f(m_1)g(m_2) \quad (m_1 \in M_1, m_2 \in M_2).$$

Das ist im wesentlichen dieselbe Konstruktion wie im Beweis von Satz 10.1.7, und den Rest des Beweises geht im wesentlichen (mit kleineren Notationsanpassungen) durch. □

Wir wollen nun noch einen anderen Existenzbeweis geben, der nicht auf der Existenz von Basen beruht und sich daher auf andere algebraische Strukturen (wie z.B. abelsche Gruppen) übertragen lässt, in denen es keine Basen gibt. Wir beschränken uns wieder auf den Fall $k = 2$.

2. Beweis. Um Indizes zu sparen setzen wir $V := V_1$ und $W := V_2$. Wir hätten gerne, dass es in unserem Tensorprodukt T für jedes $v \in V$ und $w \in W$ ein Symbol $v \otimes w$ gibt, und dass diese den üblichen Rechenregeln

$$(v_1 + v_2) \otimes (w_1 + w_2) - (v_1 \otimes w_1) - (v_1 \otimes w_2) - (v_2 \otimes w_1) - (v_2 \otimes w_2) = 0 \tag{10.2.3}$$

genügen. Das sind unendlich viele Wünsche auf einmal, aber mittels unendlichdimensionaler Vektorräume können wir uns diese erfüllen.

In einem ersten Schritt bauen wir uns zunächst einmal einen Vektorraum, in dem es die passenden Symbole gibt (noch ohne die passenden Rechenregeln). Wir betrachten dazu den gigantisch großen Vektorraum $G := \mathbb{K}^{(V \times W)}$. Selbst wenn V und W endlichdimensional ist, ist dieser möglicherweise unendlichdimensional (nämlich wenn $\mathbb{K}$ unendlich ist). Für jedes $v \in V$ und $w \in W$ haben wir dann ein Element $v \hat{\otimes} w := \delta_{(v,w)} \in G$. Diese Elemente erfüllen aber noch nicht die gewünschten Relationen. Anders ausgedrückt, die kanonische Abbildung

$$\iota_0 : V \times V \to G, \quad (v,w) \mapsto v \hat{\otimes} w,$$

ist nicht bilinear. In einem zweiten Schritt wollen wir nun diese Bilinearität mit Gewalt erzwingen. Wir betrachten daher nun die Teilmenge $M \subseteq G$, die aus allen Elementen besteht, die uns nerven. Dazu gehören alle Elemente der Form

$$(v_1 + v_2) \hat{\otimes} (w_1 + w_2) - (v_1 \hat{\otimes} w_1) - (v_1 \hat{\otimes} w_2) - (v_2 \hat{\otimes} w_1) - (v_2 \hat{\otimes} w_2)$$

mit $v_1, v_2 \in V$, $w_1, w_2 \in W$, aber auch die Elemente der Form

$$(\lambda v)\hat{\otimes} w - \lambda(v\hat{\otimes} w) \quad \text{und} \quad v\hat{\otimes}(\lambda w) - \lambda(v\hat{\otimes} w)$$

für beliebige $\lambda \in \mathbb{K}$ und $v \in V$ und $w \in W$. Es sei nun $N \leq G$ der von M aufgespannte Unterraum und $T := G/N$ der Quotientenraum mit kanonischer Projektion $\pi : G \to T$. Setzen wir $v \otimes w := \pi(v\hat{\otimes} w)$, so gelten für diese Elemente die gewünschten Relationen wie z.B. (10.2.3). Daraus folgt, dass die Abbildung

$$\iota := \pi \circ \iota_0 : V \times W \to T$$

bilinear ist. Ist nun weiter $f : V \times W \to U$ eine bilineare Abbildung in einen dritten $\mathbb{K}$-Vektorraum U, so existiert nach Bemerkung 10.2.16 eine eindeutige lineare Abbildung $f^\sharp : G \to U$ mit

$$f^\sharp(v\hat{\otimes} w) = f(v,w) \quad (v \in V, w \in W).$$

Die Tatsache, dass f bilinear ist, bedeutet genau, dass $f^\sharp|_M = 0$ gilt. Z.B. gilt

$$\begin{aligned} &f^\sharp((v_1+v_2)\hat{\otimes}(w_1+w_2) - (v_1\hat{\otimes} w_1) - (v_1\hat{\otimes} w_2) - (v_2\hat{\otimes} w_1) - (v_2\hat{\otimes} w_2)) \\ &= f^\sharp((v_1+v_2)\hat{\otimes}(w_1+w_2)) - f^\sharp(v_1\hat{\otimes} w_1) - f^\sharp(v_1\hat{\otimes} w_2) - f^\sharp(v_2\hat{\otimes} w_1) - f^\sharp(v_2\hat{\otimes} w_2) \\ &= f(v_1+v_2, w_1+w_2) - f(v_1,w_1) - f(v_1,w_2) - f(v_2,w_1) - f(v_2,w_2) = 0, \end{aligned}$$

und analog für die anderen Element von M. Da $f^\sharp$ linear ist, folgt dann aber auch $f^\sharp|_N = 0$, und daher ist die Abbildung

$$\widetilde{f} : T \to U, \quad \widetilde{f}(\pi(v,w)) = f^\sharp(v,w)$$

wohldefiniert (und linear). Nach Definition ist dann $\widetilde{f}$ die gewünschte lineare Fortsetzung. □

Der Nachteil des 2. Beweises ist, dass wir kein Gefühl für die wahre Größe des Tensorprodukts bekommen - wir konstruieren zunächst einen unendlichdimensionalen Raum und teilen dann einen anderen unendlichdimensionalen Raum heraus. Der 2. Beweis ist daher ungeeignet zum Beweis der Dimensionsformel $\dim(V \times W) = \dim V \dim W$.

Zusammenfassung von Abschnitt 10.2.

(1) Die Räume $\mathbb{K}^n$ besitzen zwei verschiedene unendlichdimensionale Verallgemeinerungen, die Räume $\mathbb{K}^M$ bzw. $\mathbb{K}^{(M)}$. Letztere sind die besseren Modellräume: Ein Vektorraum mit Basis B ist isomorph zum Modellraum $\mathbb{K}^{(B)}$.

(2) Jeder Vektorraum bettet in seinen Bidualraum ein. Ist V unendlichdimensional, so sind V^* und V^{**} echt mächtiger als (und daher nicht isomorph zu) V.

(3) Im Falle von unendlich vielen Faktoren/Summanden muss man sorgfältig zwischen direkten Summen und direkten Produkten von Vektorräumen unterscheiden. Direkte Summen haben die nützlichere universelle Eigenschaft.

(4) Tensorprodukte (mit den üblichen Eindeutigkeitseigenschaften) existieren auch für unendlichdimensionale Vektorräume.

[17.07.24]

10.3 Tensoralgebren und ihre Quotientenalgebren

Es sei stets $\mathbb{K}$ ein Körper.

Proposition 10.3.1 (Multiplikation von Tensoren)**.** *Ist V ein $\mathbb{K}$-Vektorraum und sind $k,l \in \mathbb{N}$, so existiert eine eindeutige bilineare Abbildung*

$$m_{k,l} : V^{\otimes k} \times V^{\otimes l} \to V^{\otimes(k+l)},$$

so dass $m_{k,l}((v_1 \otimes \cdots \otimes v_k),(v_{k+1} \otimes \cdots \otimes v_{k+l})) = v_1 \otimes \cdots \otimes v_{k+l}$.

Beweis. Es seien zunächst $v_{k+1},\ldots,v_{k+l} \in V$ fest gewählt. Dann ist die Abbildung

$$V^k \to V^{\otimes(k+l)}, \quad (v_1,\ldots,v_k) \mapsto v_1 \otimes \cdots \otimes v_{k+l}$$

k-linear, und nach der universellen Eigenschaft des Tensorprodukts gibt es daher eine eindeutige lineare Abbildung

$$V^{\otimes k} \to V^{\otimes(k+l)} \quad \text{mit} \quad v_1 \otimes \cdots \otimes v_k \mapsto v_1 \otimes \cdots \otimes v_{k+l}.$$

Für festes $v_1 \otimes \cdots \otimes v_k \in V^{\otimes k}$ erhalten wir dann umgekehrt eine wohldefinierte l-lineare Abbildung

$$V^l \to V^{\otimes(k+l)}, \quad (v_{k+1},\ldots,v_{k+l}) \mapsto v_1 \otimes \cdots \otimes v_{k+l},$$

und diese induziert eine eindeutige lineare Abbildung

$$V^{\otimes l} \to V^{\otimes(k+l)}, \quad \text{mit} \quad v_{k+1} \otimes \cdots \otimes v_{k+l} \mapsto v_1 \otimes \cdots \otimes v_{k+l}.$$

Wir erhalten also insgesamt die gewünschte bilineare Abbildung. □

Notation 10.3.2. Sind $\alpha \in V^{\otimes k}$ und $\beta \in V^{\otimes l}$ Tensoren so schreiben wir $\alpha \otimes \beta$ für $m_{k,l}(\alpha,\beta)$. Wir definieren auch noch $V^{\otimes 0} := \mathbb{K}$, und ist $\alpha \in V^{\otimes k}$ und $\lambda \in V^{\otimes 0}$, so schreiben wir $\lambda \otimes \alpha := \alpha \otimes \lambda := \lambda\alpha$. Damit ist das Produkt $\alpha \otimes \beta$ für beliebige $\alpha \in \mathbb{K}^{\otimes k}$ und $\beta \in \mathbb{K}^{\otimes l}$ mit $k,l \in \mathbb{N}_0$ definiert.

Konstruktion 10.3.3 (Tensoralgebra)**.** Zu einem gegebenen Vektorraum V definieren wir einen neuen Vektorraum $\mathcal{T}(V)$ durch

$$\mathcal{T}(V) := \bigoplus_{n=0}^{\infty} V^{\otimes n} = V \oplus V^{\otimes 2} \oplus V^{\otimes 3} \oplus V^{\otimes 4} \oplus \ldots$$

Wir nennen Elemente von $V^{\otimes k}$ in diesem Kontext *homogen* vom *Grad* k. Nach Definition ist jedes Element von $\mathcal{T}(V)$ eine *endliche* Summe homogener Elemente (möglicherweise von verschiedenem Grad). Sind also z.B. $v_1,\ldots,v_8 \in V$, so ist

$$v_1 \otimes v_2 + v_3 \otimes v_4 \otimes v_5 + v_6 \otimes v_7 \otimes v_8 \in \mathcal{T}(V).$$

Wir können jedes Element von $\mathcal{T}(V)$ eindeutig schreiben als formal unendliche Summe

$$\alpha = \sum_{n=0}^{\infty} \alpha_n,$$

wobei $\alpha_n \in V^{\otimes n}$ für fast alle $n \in \mathbb{N}$ gleich 0 ist. Wir nennen α_n die *homogene Komponente* von α vom Grad n und definieren ein Produkt auf $\mathscr{T}(V)$ durch

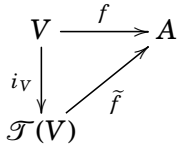
$$\alpha \otimes \beta = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \alpha_k \otimes \beta_{n-k} \right).$$

Für beliebige $v_1, \ldots, v_8 \in V$ gilt also z.B. die Gleichheit

$$\begin{aligned}(v_1 \otimes v_2 + v_3 \otimes v_4 \otimes v_5) \otimes (v_6 + v_7 \otimes v_8) \quad &= \quad v_1 \otimes v_2 \otimes v_6 + v_1 \otimes v_2 \otimes v_7 \otimes v_8 \\ &\quad + v_3 \otimes v_4 \otimes v_5 \otimes v_6 + v_3 \otimes v_4 \otimes v_5 \otimes v_7 \otimes v_8.\end{aligned}$$

Insbesondere gilt $1 \otimes \alpha = \alpha \otimes 1$ für alle $\alpha \in \mathscr{T}(V)$. Aus der Bilinearität der Produkte $m_{k,l}$ folgt leicht, dass dies eine bilineare Verknüpfung auf $\mathscr{T}(V)$ definiert, und man kann sich leicht überlegen, dass diese assoziativ ist. Daher ist $\mathscr{T}(V)$ eine assoziative $\mathbb{K}$-Algebra, genannt die *Tensoralgebra* von V. Indem wir V mit $V^{\otimes 1}$ identifizieren erhalten wir eine Einbettung $i_V : V \hookrightarrow \mathscr{T}(V)$. Ist $V \neq \{0\}$, so ist diese stets unendlichdimensional über $\mathbb{K}$ (selbst wenn V endlichdimensional ist).

Satz 10.3.4 (Universelle Eigenschaft der Tensoralgebra)**.** *Ist V ein $\mathbb{K}$-Vektorraum, so existiert für jede $\mathbb{K}$-Algebra $\mathscr{A}$ und jede $\mathbb{K}$-lineare Abbildung $f : V \to \mathscr{A}$ ein eindeutiger Morphismus $\widetilde{f} : \mathscr{T}(V) \to \mathscr{A}$ von $\mathbb{K}$-Algebren, so dass das folgende Diagramm kommutiert:*



Beweis. Nehmen wir zunächst an, dass $\widetilde{f}$ existiert - wie muss $\widetilde{f}$ dann aussehen? Da $\widetilde{f}$ ein Morphismus von Algebren ist, muss $\widetilde{f}(1) = 1$ und daher $\widetilde{f}(\lambda) = \lambda$ für alle $\lambda \in V^{(0)} = \mathbb{K}$ gelten. Für $v \in V$ muss wegen der Kommutativität des Diagramms gelten, dass $\widetilde{f}(v) = v$. Ist nun $v_1 \otimes \cdots \otimes v_k$ ein beliebiger elementarer Tensor, so folgt dann aus der Multiplikativität von $\widetilde{f}$, dass

$$\widetilde{f}(v_1 \otimes \cdots \otimes v_k) = f(v_1) \otimes \cdots \otimes f(v_k). \tag{10.3.1}$$

Da die Tensoralgebra als Vektorraum von den elementaren Tensoren aufgespannt wird, ist $\widetilde{f}$ durch (10.3.1) eindeutig festgelegt. Es gibt also höchstens eine Abbildung $\widetilde{f}$ wie im Satz und diese muss notwendigerweise durch (10.3.1) gegeben sein.

Wir zeigen nun die Existenz: Für jedes $k \in \mathbb{N}$ ist die Abbildung

$$V^k \to \mathscr{A}, \quad (v_1, \ldots, v_k) \to f(v_1) \otimes \cdots \otimes f(v_k)$$

k-linear. Es existiert daher eine eindeutige lineare Abbildung $V^{\otimes k} \to \mathscr{A}$ mit der Eigenschaft, dass $v_1 \otimes \cdots \otimes v_k \mapsto f(v_1) \otimes \cdots \otimes f(v_k)$. Diese linearen Abbildungen kombinieren sich (nach der universellen Eigenschaft der direkten Summen) dann zu einer linearen Abbildung $\widetilde{f} : \mathscr{T}(V) \to \mathscr{A}$, die (10.3.1) erfüllt (wobei wir für 0-Tensoren noch $\widetilde{f}(\lambda) := \lambda$ setzen).

Man muss nun noch nachrechnen, dass das so konstruierte f in der Tat ein Morphismus von $\mathbb{K}$-Algebren ist. Für elementare Tensoren ist die Multiplikativität sofort klar, und für Summen folgt diese aus der Bilinearität (Details als Übung!). □

Beispiel 10.3.5 (Tensoralgebra als Funktor)**.** Ist $f : V \to W$ eine lineare Abbildung zwischen Vektorräumen, so erhalten wir eine lineare Abbildung $\iota_W \circ f : V \to \mathcal{T}(W)$. Nach der universellen Eigenschaft erhalten wir dann einen eindeutigen Morphismus $\mathcal{T}(f) : \mathcal{T}(V) \to \mathcal{T}(W)$ von $\mathbb{K}$-Algebren mit $\mathcal{T}(f)(v) = f(v)$. Auf elementaren Tensoren ist dieser durch $v_1 \otimes \cdots \otimes v_k \mapsto f(w_1) \otimes \cdots \otimes f(w_k)$ gegeben.

Bemerkung 10.3.6 (Erzeugendensysteme)**.** Wir erinnern an die folgenden Begriffe und Notationen: Ist S eine Teilmenge, so schreiben wir $\langle S \rangle_{\mathbb{K}-\mathrm{Alg}}$ für die kleinste $\mathbb{K}$-Unteralgebra von $\mathcal{A}$, die S enthält. Die Elemente dieser Algebra sind genau die endlichen Linearkombinationen von endlichen Produkten von Elementen von S. Wir nennen S ein *Erzeugendensystem* von $\mathcal{A}$, falls $\mathcal{A} = \langle S \rangle_{\mathbb{K}-\mathrm{Alg}}$ gilt. $\mathcal{A}$ heißt *endlich erzeugt* (als $\mathbb{K}$-Algebra), falls sie ein endliches Erzeugendensystem besitzt. Man beachte: Jede endlichdimensionale $\mathbb{K}$-Algebra ist endlich erzeugt (z.B. durch eine beliebige Basis), aber nicht jede endlich erzeugte $\mathbb{K}$-Algebra ist endlichdimensional!

Für die Tensoralgebra können wir Erzeugendensysteme wie folgt konstruieren: Da jeder elementare Tensor ein Produkt von Elementen aus V oder ein Vielfaches der 1 ist (die nach Definition in jeder Unteralgebra enthalten ist) aus Elementen von $\mathbb{K}^{(0)}$ ist, und jeder Tensor und daher auch jedes Element der Tensoralgebra eine endliche Summe elementarer Tensoren ist, folgt dass

$$\mathcal{T}(V) = \langle V \rangle_{\mathbb{K}-\mathrm{Alg}}.$$

Damit haben wir für $\mathcal{T}(V)$ ein kanonisches aber leider unendliches Erzeugendensystem angegeben. Das geht noch effizienter: Ist B eine Basis von V, so muss jede $\mathbb{K}$-Algebra, die B enthält, auch V enthalten. Wir sehen daher, dass dann

$$\mathcal{T}(V) = \langle B \rangle_{\mathbb{K}-\mathrm{Alg}}.$$

Ist V endlichdimensional von Dimension n, so wird $\mathcal{T}(V)$ daher von n Elementen erzeugt. Insbesondere ist die Tensoralgebra eines endlichdimensionalen Vektorraums endlich erzeugt (als $\mathbb{K}$-Algebra).

Konstruktion 10.3.7. Es sei $\mathcal{A}$ eine beliebige assoziative $\mathbb{K}$-Algebra und es sei B ein Erzeugendensystem von $\mathcal{A}$. Nach der universellen Eigenschaft von $\mathbb{K}^{(B)}$ finden wir dann eine eindeutige lineare Abbildung $f : \mathbb{K}^{(B)} \to \mathcal{A}$ mit $\delta_b \mapsto b$ für alle $b \in B$. Nach der universellen Eigenschaft der Tensoralgebra finden wir dann einen eindeutigen Homomorphismus $\widetilde{f} : \mathcal{T}(\mathbb{K}^{(B)}) \to \mathbb{K}$ mit $f(\delta_b) = b$. Das Bild $\mathrm{Bild}(\widetilde{f})$ ist dann eine $\mathbb{K}$-Algebra, die B enthält. Da B ein Erzeugendensystem ist, ist daher $\widetilde{f}$ surjektiv.

Wir sehen also: Jede assoziative $\mathbb{K}$-Algebra ist das homomorphe Bild einer Tensoralgebra und jede endlich erzeugte assoziative $\mathbb{K}$-Algebra ist das homomorphe Bild einer Tensoralgebra über einem endlichdimensionalen Vektorraum. Nach dem Homomorphiesatz sind die homomorphen Bilder einer assoziativen $\mathbb{K}$-Algebra $\mathcal{A}$ genau die Quotienten von $\mathcal{A}$ nach *zweiseitigen Idealen*, also Untervektorräumen $\mathcal{I} < \mathcal{A}$, die unter Multiplikation von links und rechts mit Elementen aus $\mathcal{A}$ abgeschlossen sind. Damit haben wir den folgenden Satz bewiesen.

Satz 10.3.8. *Ist $\mathcal{A}$ eine assoziative $\mathbb{K}$-Algebra, so existiert ein Vektorraum V und ein zweiseitiges Ideal $\mathcal{I} \lhd \mathcal{T}(V)$ mit $\mathcal{A} \cong \mathcal{T}(V)/\mathcal{I}$. Ist $\mathcal{A}$ endlich erzeugt, so kann V endlichdimensional gewählt werden.* □

Konstruktion 10.3.9 (Erzeugende und Relationen)**.** Wie können wir Beispiele für endlich erzeugte $\mathbb{K}$-Algebren konstruieren? Um eine Algebra mit n Erzeugern zu konstruieren, können

wir mit $\mathscr{T}(\mathbb{K}^n)$ anfangen. Diese wird von den Standarderzeugern $e_1,\dots,e_n$ erzeugt. Elemente sind also endliche Summen von Produkten dieser Standarderzeuger. Diese Algebra ist aber ziemlich langweilig: Zwei Summen von Produkten von Erzeugern sind (wegen der linearen Unabhängigkeit der Produkte der Erzeuger) genau dann gleich, wenn sie „gleich aussehen“. Es gilt also z.B. $e_1 \otimes e_2 \neq e_2 \otimes e_1$ und $e_1 \neq 3e_2 \otimes e_3$. Wie können wir nun interessantere Algebren bauen?

Nehmen wir an, wir wollen, dass für unsere Erzeuger $\bar{e}_1,\dots,\bar{e}_n$ die Beziehung („Relation“) $\bar{e}_1 = 3\bar{e}_2 \otimes \bar{e}_3$ bzw.

$$\bar{e}_1 - 3\bar{e}_2 \otimes \bar{e}_3 = 0$$

gelten soll. Wir können dann in $\mathscr{T}(\mathbb{K}^n)$ ein beliebiges Ideal $\mathscr{I}$ wählen, dass das Element $e_1 - 3e_2 \otimes e_3$ enthält. Im Quotienten $\mathscr{T}(\mathbb{K}^n)/\mathscr{I}$ gilt für die Äquivalenzklassen $\bar{e}_1,\dots,\bar{e}_n$ der Standarderzeuger dann die gewünschte Relation. Wir können für $\mathscr{I}$ z.B. das *kleinste* Ideal wählen, das $e_1 - 3e_2 \otimes e_3$ enthält. Dieses besteht aus allen Summen von Produkten von $e_1 - 3e_2 \otimes e_3$ mit beliebigen Elementen der Tensoralgebra von beiden Seiten, ist also gigantisch groß. Die Algebra $\mathscr{T}(\mathbb{K}^n)/\mathscr{I}$ ist dann die größte Algebra mit n Erzeugern, in der die gewünschte Relation gilt. Man schreibt für diese Algebra dann auch

$$\langle e_1,\dots,e_n \mid e_1 - 3e_2 \otimes e_3 \rangle.$$

Will man, dass mehrere (gerne auch unendlich viele!) Relationen gelten sollten, so kann man für $\mathscr{I}$ einfach das Ideal nehmen, das von diesen Relationen erzeugt wird. Für eine solcherart durch „Erzeugende und Relationen“ definierte Algebra schreibt man dann etwa

$$\mathscr{A} = \langle e_1, e_2, e_3 \mid e_1 \otimes e_2 - e_2 \otimes e_1, e_1 \otimes e_3 - e_3 \otimes e_1 \rangle.$$

Wenn man möchte, kann man auch unendliche Erzeugendenmengen zulassen.

Warnung! Man kann beweisen, dass es keinen Algorithmus gibt, der entscheiden könnte, ob es sich bei einer beliebigen durch Erzeugende und Relationen definierte endlich erzeugte Algebra um die triviale Algebra $\mathscr{A} = \mathbb{K}1$ handelt oder nicht. Wir können uns zwar wünschen was wir wollen, aber die Mathematik liefert dann auch genau das, was wir uns gewünscht haben, nämlich die größtmögliche Algebra mit den gewünschten Erzeugern und Relationen. Diese kann sehr klein sein!

Wir betrachten nun noch einige spezielle Beispiele, in denen wir das Ergebnis kontrollieren können.

Beispiel 10.3.10 (Symmetrische Algebra)**.** Es sei V ein beliebiger Vektorraum und $\mathscr{I}$ das kleinste Ideal von $\mathscr{T}(V)$, das alle Elemente der Form $v \otimes w - w \otimes v$ mit $v, w \in V$ erhält. Dann ist $\mathrm{Sym}(V) := \mathscr{T}(A)/\mathscr{I}$ eine Algebra, die von V erzeugt wird. Die Relationen in dieser Algebra besagen gerade, dass für alle $v, w \in V$ schon $[v] \otimes [w] = [w] \otimes [v]$ gilt. Es handelt sich also um eine *kommutative* assoziative $\mathbb{K}$-Algebra. Diese heißt die *symmetrische Algebra* über V.

Wir betrachten nun spezielle den Fall $V = \mathbb{K}^n$. In diesem Fall ist $\mathrm{Sym}(\mathbb{K}^n)$ eine kommutative assoziative $\mathbb{K}$-Algebra mit n Erzeugern $[e_1],\dots,[e_n]$. Ist $\mathscr{A}$ eine beliebige andere kommutative assoziative $\mathbb{K}$-Algebra $\mathscr{A}$ mit n-Erzeugern $E_1,\dots,E_n$, so existiert nach der universellen Eigenschaft ein Morphismus $f : \mathscr{T}(\mathbb{K}^n) \to \mathscr{A}$ mit $f(e_j) = E_j$. Für alle $v, w \in V$ gilt dann

$$f(v \otimes w - w \otimes v) = f(v)f(w) - f(w)f(v) = 0 \implies \mathscr{I} \subseteq \ker(f).$$

Daher faktorisiert f durch den Quotienten $\mathrm{Sym}(\mathbb{K}^n)$. Die Algebra $\mathrm{Sym}(\mathbb{K}^n)$ ist daher die *größte* kommutative assoziative $\mathbb{K}$-Algebra mit n Erzeugern und jede andere solche Algebra ist ein Quotient von $\mathrm{Sym}(\mathbb{K}^n)$. Insbesondere existiert ein eindeutiger surjektiver Morphismus

$$i : \mathrm{Sym}(\mathbb{K}^n) \to \mathbb{K}[X_1,\dots,X_n] \quad \text{mit} \quad [e_j] \mapsto X_j.$$

Insbesondere ist $\mathrm{Sym}(\mathbb{K}^n)$ unendlichdimensional. In den Übungen werden Sie sich überlegen, dass die Polynomalgebra $\mathbb{K}[X_1,\dots,X_n]$ selbst schon die obige universelle Eigenschaft erfüllt, und daher ist die Abbildung i ein Isomorphismus. Wir haben also Polynomalgebren durch Erzeuger und Relationen beschrieben.

Tensor-Algebren und symmetrische Algebren sind unendlichdimensional und daher den Methoden der Linearen Algebra nur begrenzt zugänglich. Unsere bisher einzigen Beispiele für endlichdimensionale Algebren waren entweder kommutativ ($\mathbb{K}$, $\mathbb{K}[X]$ oder zyklische Matrixalgebren, die Quotienten von $\mathbb{K}[X]$ sind) oder hochgradig kompliziert (z.B. $\mathbb{K}^{n\times n}$). Wir betrachten daher nun zum Abschluss noch eine besonders wichtige Klasse von nicht-kommutativen endlichdimensionalen $\mathbb{K}$-Algebren, die in der Geometrie eine große Rolle spielen und zugleich einfach zu beschreiben sind.

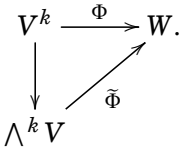
Bis zum Ende dieses Abschnitts sei $\mathbb{K}$ ein Körper der Charakteristik $\neq 2$.

Es seien V und W zwei $\mathbb{K}$-Vektorräume. Wir erinnern daran, dass eine lineare Abbildung $\Phi : V^k \to W$ *schiefsymmetrisch* heißt, falls

$$\Phi(v_{\sigma(1)},\dots,v_{\sigma(k)}) = \mathrm{sgn}(\sigma)\Phi(v_1,\dots,v_k)$$

für alle $v_1,\dots,v_k \in V$ und $\sigma \in \mathrm{Sym}_k$. Wegen $\mathrm{char}(\mathbb{K}) \neq 2$ ist das gleichbedeutend damit, dass Φ alternierend ist.

Proposition 10.3.11 (Existenz von äußeren Potenzen)**.** *Für jeden $\mathbb{K}$-Vektorraum V und jedes $k \in \mathbb{N}$ existiert ein $\mathbb{K}$-Vektorraum $\bigwedge^k V$ zusammen mit einer Abbildung $i : V^k \to \bigwedge^k V$ mit der folgenden universellen Eigenschaft: Für jeden $\mathbb{K}$-Vektorraum W und jede schiefsymmetrische k-lineare Abbildung $\Phi : V^k \to W$ existiert eine lineare Abbildung $\widetilde{\Phi} : \bigwedge^k V \to W$, so dass das folgende Diagramm kommutiert:*



Beweis. Ist $V = U^*$ ein Dualraum, so haben wir $\bigwedge^k U^*$ mit der entsprechenden universellen Eigenschaft bereits im Kapitel über Determinanten konstruiert, nämlich als Raum der alternierenden k-Linearformen über U. Ist V endlichdimensional, so können wir uns wegen $V = (V^*)^*$ auf diesen Fall zurückziehen, Wir können $\bigwedge^k U^*$ aber auch ganz einfach abstrakt konstruieren:

Es sei U der Untervektorraum von $V^{\otimes k}$, der von allen Elementen der Form

$$v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(k)} - \mathrm{sgn}(\sigma) \cdot (v_1 \otimes \cdots \otimes v_k)$$

mit $v_1,\dots,v_k \in V$ und $\sigma \in \mathrm{Sym}_k$ erzeugt wird. Wir definieren

$$\bigwedge^k V := V^{\otimes k}/U \quad \text{und} \quad i : V^k \xrightarrow{\iota} V^{\otimes k} \to \bigwedge^k V.$$

Sei nun Φ wie in der Proposition. Da Φ multilinear ist, gibt es genau eine lineare Fortsetzung $V^{\otimes k} \to W$, und dass Φ schief-symmetrisch ist, bedeutet genau, dass diese Fortsetzung auf U verschwindet. Daraus folgt die Behauptung. □

Definition 10.3.12. Der Vektorraums $\bigwedge^k V$ heißt die *k-te äußere Potenz* von V. Für $v_1,\dots,v_k \in V$ schreiben wir $v_1 \wedge \cdots \wedge v_k := i(v_1,\dots,v_k)$ für das entsprechende Bild in $\bigwedge^k V$.

Bemerkung 10.3.13 (Rechnen in äußeren Potenzen)**.** Wie rechnet man in äußeren Potenzen? Es gelten dieselben Rechengesetze wie in Tensorprodukten, nur dass man jetzt die Reihenfolge von Faktoren um den Preis eines Vorzeichens umdrehen darf, d.h. für alle $v_1, v_2 \in V$ gilt $v_1 \wedge v_2 = -v_2 \wedge v_1$. Dies impliziert insbesondere, dass für alle $v \in V$,

$$v \wedge v = -v \wedge v = 0.$$

Betrachten wir als Beispiel die äußeren Potenzen von $V := \mathbb{K}^2$. In $\bigwedge^2 V$ gilt

$$e_1 \wedge e_1 = 0 \quad \text{und} \quad e_1 \wedge e_2 = -e_2 \wedge e_1 \quad \text{und} \quad e_2 \wedge e_2 = 0.$$

In $\bigwedge^3 V$ gilt z.B.

$$e_1 \wedge e_2 \wedge e_1 = -e_1 \wedge e_1 \wedge e_2 = -0 \wedge e_2 = 0.$$

Allgemein gilt: Kommt in einem Ausdruck wie dem obigen mindestens zweimal der Term e_1 (oder e_2) vor, so können wir solange Vertauschen (unter Hinzunahme von Vorzeichen), bis zwei Kopien von e_1 (oder e_2) nebeneinander stehen, und sehen dann, dass das Produkt gleich 0 ist.

Proposition 10.3.14 (Basen von äußeren Potenzen)**.** *Ist $(v_1,\dots,v_n)$ eine geordnete Basis von V, so ist*

$$\{v_{i_1} \wedge \cdots \wedge v_{i_k} \mid 1 \le i_1 < \cdots < i_k \le n\}$$

eine Basis von $\bigwedge^k V$. Insbesondere gilt $\bigwedge^k V = \{0\}$ für $k > n$ und

$$\dim \bigwedge^k V = \binom{n}{k} \quad \textit{für} \quad 0 \le k \le n.$$

Bevor wir die Proposition beweisen, schauen wir uns eine wichtige Konsequenz an. Wir können nämlich mittels äußerer Potenzen eine *endlichdimensionale* $\mathbb{K}$-Algebra erzeugen:

Konstruktion 10.3.15 (Äußeres Produkt)**.** Wir betrachten für $k \in \mathbb{N}$ die Quotientenabbildungen

$$p_k : V^{\otimes k} \to \bigwedge^k V \quad \text{mit } v_1 \otimes \cdots \otimes v_k \mapsto v_1 \wedge \cdots \wedge v_k.$$

In Proposition 10.3.1 haben wir die Tensormultiplikation

$$m_{k,l} : V^{\otimes k} \times V^{\otimes l} \to V^{\otimes (k+l)}$$

eingeführt. Wir wollen nun eine ähnliche Multiplikation auf den äußeren Potenzen einführen. Dazu beobachten wir, dass für $k, l \in \mathbb{N}$ die Abbildung

$$V^k \times V^l \to V^{\otimes k} \times V^{\otimes l} \xrightarrow{m_{k,l}} V^{\otimes (k+l)} \xrightarrow{p_{k+1}} \bigwedge^{k+l} V$$

in jedem der beiden Faktoren V^k und V^l bilinear und alternierend ist. Durch zweimaliges Anwenden der universellen Eigenschaft erhalten wir daher eine bilineare Abbildung

$$\bigwedge^k V \times \bigwedge^l V \to \bigwedge^{k+l} V \quad \text{mit} \quad ((v_1 \wedge \cdots \wedge v_k),(w_1 \wedge \cdots \wedge w_l)) \mapsto v_1 \wedge \cdots \wedge v_k \wedge w_1 \wedge \cdots \wedge w_l.$$

Setzen wir wieder $\bigwedge^0 V = \mathbb{K}$, so können wir das Produkt noch auf $k, l \in \mathbb{N}_0$ ausdehnen. Die direkte Summe

$$\bigwedge^\bullet V := \bigoplus_{k=0}^{\infty} \bigwedge^k V$$

ist dann mit der linearen Fortsetzung dieses Produkts eine $\mathbb{K}$-Algebra, und wir erhalten ein kommutierendes Diagramm der Form

$$\begin{array}{ccc} \mathcal{T}(V)\times\mathcal{T}(V) & \longrightarrow & \mathcal{T}(V) \\ \downarrow & & \downarrow \\ \bigwedge^\bullet V \times \bigwedge^\bullet V & \longrightarrow & \bigwedge^\bullet V, \end{array}$$

wobei die horizontalen Abbildungen die jeweiligen Algebramultiplikationen und die vertikalen Abbildungen die Quotientenabbildungen sind.

Definition 10.3.16. Die $\mathbb{K}$-Algebra $\bigwedge^\bullet V$ heißt die *Graßmann*[6]*-Algebra* (oder auch *äußere Algebra*) über V.

Korollar 10.3.17. *Ist* $\dim V = n < \infty$*, so ist auch* $\bigwedge^\bullet V$ *endlichdimensional mit*

$$\dim \bigwedge^\bullet V = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Beweis. Die Summenformel folgt sofort aus Proposition 10.3.14. Für die zweite Formel rechnet man mittels binomischer Formel, dass

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k},$$

woraus die Behauptung folgt. □

Wir kommen nun zum Beweis von Proposition 10.3.14. Die erste Hälfte ist ganz leicht:

Lemma 10.3.18. *Ist* $(v_1,\ldots,v_n)$ *eine geordnete Basis von* V*, so ist*

$$\{v_{i_1} \wedge \cdots \wedge v_{i_k} \mid 1 \le i_1 < \cdots < i_k \le n\}$$

ein Erzeugendensystem von $\bigwedge^k V$*. Insbesondere gilt* $\bigwedge^k V = \{0\}$ *für* $k > n$*.*

Beweis. Weil $\bigwedge^k V$ ein Quotient des Tensorprodukts $V^{\otimes k}$ ist, wird es zumindest einmal von den Elementen der Form $\{v_{i_1} \wedge \cdots \wedge v_{i_k} \mid i_1,\ldots,i_k \in \{1,\ldots,n\}\}$ erzeugt. Nun können wir aber jedes Element der Form $v_{i_1} \wedge \cdots \wedge v_{i_k}$ bis auf Vorzeichen so umsortieren, dass $i_1 \le \cdots \le i_k$. Kommt nun einer der Indizes doppelt vor, so ist der entsprechende Ausdruck schon 0. Es bleiben also nur die im Lemma genannten Erzeuger übrig. Ist $k > n$ so kommt immer mindestens ein Index doppelt vor, und daher sind alle potentiellen Erzeuger schon 0. □

Deutlich schwieriger ist es zu zeigen, dass die verbliebenen Erzeuger tatsächlich linear unabhängig sind. Hier verwendet man Determinanten!

[6] nach Hermann Graßmann (1809-1877), Gymnasiallehrer in Stettin - zu einer Zeit, in der von Gymnasiallehrern neben ihrer Lehre und einem zweiten Fach (in Graßmanns Fall Sprachwissenschaften) noch eine eigenständige Forschungsleistung und Fachpublikationen erwartet wurden

[19.07.24]

Wir erinnern daran, dass wir $\bigwedge^k V$ als Quotienten von $V^{\otimes k}$ modulo dem Unterraum U, der von Tensoren der Form $w_{\sigma(1)} \otimes \cdots \otimes w_{\sigma(k)} - \operatorname{sgn}(\sigma) \cdot (w_1 \otimes \cdots \otimes w_k)$ wird, definiert haben.

Beweis von Proposition 10.3.14. Es sei $k \leq n$ und

$$\mathscr{I} := \{I = (i_1, \ldots, i_k) \in \{1, \ldots, n\}^k \mid 1 \leq i_1 < \cdots < i_k \leq n\}$$

Für $I = (i_1, \ldots, i_k) \in \mathscr{I}$ setzen wir $v_I := v_{i_1} \wedge \cdots \wedge v_{i_k}$. Wir wollen zeigen, dass $\{v_I \mid I \in \mathscr{I}\}$ linear unabhängig ist.

Es sei $\iota : V \to \mathbb{K}^n$ der Koordinatenisomorphismus zu $(v_1, \ldots, v_n)$ und es sei $p_I : \mathbb{K}^n \to \mathbb{K}^k$ die Projektion, die nur die Einträge in I auswählt. Es ist dann

$$\pi_I := p_I \circ \iota : V \to \mathbb{K}^k, \quad \sum_{i=1}^n \lambda_i v_i = (\lambda_{i_1}, \ldots, \lambda_{i_k})^\top.$$

Es sei nun $\operatorname{Det} : (\mathbb{K}^k)^k \to \mathbb{K}$ die Determinantenform (mit Normalisierung $\operatorname{Det}(e_1, \ldots, e_k) = 1$). Für jedes $I \in \mathscr{I}$ erhalten wir nun eine k-lineare Abbildung

$$\Phi_I : V^k \to \mathbb{K}, \quad (w_1, \ldots, w_k) \mapsto \operatorname{Det}(\pi_I(w_1), \ldots, \pi_I(w_k)),$$

und diese ist schiefsymmetrisch, weil die Determinantenform schiefsymmetrisch ist. Aufgrund der universellen Eigenschaft des äußeren Produkts erhalten wir also eine lineare Abbildung

$$\widetilde{\Phi}_I : \bigwedge^k V \to \mathbb{K}, \quad \text{mit} \quad w_1 \wedge \cdots \wedge w_k \mapsto \operatorname{Det}(\pi_I(w_1), \ldots, \pi_I(w_k)).$$

Man überlegt sich nun zwei Dinge: Erstens erhalten wir

$$\widetilde{\Phi}_I(v_I) = \widetilde{\Phi}_I(v_{i_1} \wedge \cdots \wedge v_{i_k}) = \operatorname{Det}(\pi_I(e_{i_1}), \ldots \pi_I(e_{i_k})) = \operatorname{Det}(e_1, \ldots, e_k) = 1.$$

Ist andererseits $J = (j_1, \ldots, j_k) \neq I$, so existiert ein $p \in \{1, \ldots, k\}$ mit $\pi_I(e_{j_p}) = 0$ und daher

$$\widetilde{\Phi}_I(v_j) = \widetilde{\Phi}_I(v_{j_1} \wedge \cdots \wedge v_{j_k}) = \operatorname{Det}(\pi_I(e_{j_1}), \ldots \pi_I(e_{j_k})) = 0.$$

Ließe sich nun ein v_I als Linearkombination der anderen v_J schreiben, etwa

$$v_I = \sum_{J \in \mathscr{I} \setminus \{I\}} \lambda_J v_J,$$

so erhielten wir den Widerspruch

$$1 = \widetilde{\Phi}_I(v_I) = \sum_{J \in \mathscr{I} \setminus \{I\}} \lambda_J \widetilde{\Phi}_I(v_J) = 0. \qquad \square$$

Da Graßmann-Algebren endlich-erzeugt sind, kann man sie auch durch Erzeugende und Relationen beschreiben. Wir überlegen uns:

Proposition 10.3.19. *Es sei*

$$\mathscr{G}_n := \langle e_1, \ldots, e_n \mid \forall\, i, j \in \{1, \ldots, n\} : e_i \otimes e_j + e_j \otimes e_i \rangle$$

Dann existiert ein eindeutiger Isomorphismus $i : \mathscr{G}_n \to \bigwedge^\bullet \mathbb{K}^n$ von $\mathbb{K}$-Algebren mit

$$i([e_1 \otimes \cdots \otimes e_k]) = e_1 \wedge \cdots \wedge e_k.$$

Beweis. Die Eindeutigkeit ist klar, da die obigen Elemente $[e_1 \otimes \cdots \otimes e_k]$ schon $\mathscr{G}_n$ erzeugen. Für die Existenzaussage gibt es wieder einen einfachen Teil (rein formal) und einen schwierigen Teil (der unser obiges Determinantenargument verwendet).

Der einfache Teil geht so: Nach der universellen Eigenschaft der Tensoralgebra existiert ein eindeutiger Morphismus $q : \mathscr{T}(\mathbb{K}^k) \to \bigwedge^\bullet \mathbb{K}^n$ mit $q(e_i) = e_i$. Dieser ist surjektiv, da die e_i die Graßmann-Algebra erzeugen. Für $i, j \in \{1, \ldots, n\}$ gilt $q(e_i \otimes e_j + e_j \otimes e_i) = e_i \wedge e_j + e_j \wedge e_i = 0$. Bezeichnet $\mathscr{J} \lhd \mathscr{T}(\mathbb{K}^n)$ das Ideal mit $\mathscr{G}_n = \mathscr{T}(\mathbb{K}^n)/\mathscr{J}$, so gilt also $\mathscr{J} \subseteq \ker(q)$, und daher induziert q einen surjektiven Morphismus $i : \mathscr{G}_n \to \bigwedge^\bullet \mathbb{K}^n$ mit $i([e_1 \otimes \cdots \otimes e_k]) = e_1 \wedge \cdots \wedge e_k$.

Der schwierige Teil ist die Injektivität von i. Wie im Beweis von Lemma 10.3.18 sieht man, dass die Elemente $[e_{i_1} \otimes \cdots \otimes e_{ik}]$ mit $k \in \{1, \ldots, n\}$ $1 \leq i_1 < \cdots < i_k \leq n$ den Vektorraum $\mathscr{G}_n$ erzeugen. Daher gilt

$$\dim \mathscr{G}_n \leq \binom{n}{0} + \cdots + \binom{n}{n} = 2^n = \dim \bigwedge^\bullet \mathbb{K}^n.$$

Aus Dimensionsgründen muss daher i ein Isomorphismus sein. □

Beispiel 10.3.20 (Rechnen in Grassmannalgebren)**.** Durch Rechnen mit Erzeugern und Relationen erhält man z.B.

$$(1e_1 + 2e_2 + 3e_3) \wedge (4e_1 + 5e_2 + 6e_3) = (1 \cdot 5 - 2 \cdot 4)e_1 \wedge e_2 + (1 \cdot 6 - 3 \cdot 4)e_1 \wedge e_3 + (2 \cdot 6 - 3 \cdot 5)e_2 \wedge e_3.$$

Allgemein überlegt man sich, dass die Koeffizienten in einem k-fachen Produkt von Elementen von $\mathscr{G}_n$ durch die k-Minoren der Matrix gegeben sind, die entsteht, wenn man die entsprechenden Vektoren nebeneinander schreibt.

Bemerkung 10.3.21 (Geometrische Interpretation der Graßmann-Algebra)**.** Was bedeutet es für zwei k-Tupel $(v_1, \ldots, v_k)$ und $(w_1, \ldots, w_k)$ linear unabhängiger Vektoren in $\mathbb{R}^n$, dass die Bedingung

$$v_1 \wedge \cdots \wedge v_k = w_1 \wedge \cdots \wedge w_k$$

gilt? In der Übung werden Sie sich überlegen, das aus dieser Bedingung sofort folgt, dass $\langle v_1, \ldots, v_k \rangle = \langle w_1, \ldots, w_k \rangle$ folgt. Die zugehörigen Parallelepipede $P(v_1, \ldots, v_k)$ und $P(w_1, \ldots, w_k)$ liegen also im selben k-dimensionalen Vektorraum V. Darüber hinaus muss für eine (und daher jede beliebige) orientierte Volumenform D dieses Vektorraums gelten, dass

$$D(v_1, \ldots, v_k) = D(w_1, \ldots, w_k).$$

Dies bedeutet gerade, dass die beiden Parallelepipede dasselbe Volumen und dieselbe Orientierung haben. Das bedeutet, dass sie durch Scherungen und Drehungen (keine Streckungen, Stauchungen oder Spiegelungen!) innerhalb von V auseinander hervorgehen. Elementare Tensoren in der Grassmannalgebra entsprechen also gewissen Äquivalenzklassen von Parallelepipeden.

Bemerkung 10.3.22 (Funktorialität)**.** Ist $f : V \to W$ eine lineare Abbildung, so ist die zugehörige Abbildung

$$V^k \xrightarrow{f \times f \cdots \times f} W^k \to \bigwedge^k W, \quad (v_1, \ldots, v_k) \mapsto f(v_1) \wedge \cdots \wedge f(v_k)$$

k-linear und alternierend und induziert daher mittels universelle Eigenschaft eine wohldefinierte Abbildung

$$\bigwedge^k f : \bigwedge^k V \to \bigwedge^k W, \quad v_1 \wedge \cdots \wedge v_k \mapsto f(v_1) \wedge \cdots \wedge f(v_k).$$

Diese Abbildungen fügen sich dann zu einer Abbildung

$$\bigwedge^\bullet f : \bigwedge^\bullet V \to \bigwedge^\bullet W$$

zusammen, und diese ist nach Definition der Multiplikation ein Morphismus von $\mathbb{K}$-Algebren. Jede lineare Abbildung induziert also einen Morphismus von Graßmann-Algebren.

Bemerkung 10.3.23 (Duale Tensoralgebra und duale Graßmann-Algebra)**.** In den Anwendungen in der Differentialgeometrie ist häufig die Algebra $\mathcal{T}(V^*)$ nützlicher als $\mathcal{T}(V)$, da wir uns Elemente von $(V^*)^{\otimes k}$ als k-lineare Abbildungen auf V vorstellen können. Wir nennen $\mathcal{T}(V^*)$ die *duale Tensoralgebra* von V. Ist $f : V \to W$ eine lineare Abbildung, so induziert diese eine duale lineare Abbildung $f^* : W^* \to V^*$ in die umgekehrte Richtung und daher einen Morphismus

$$f^* : \mathcal{T}(W^*) \to \mathcal{T}(V^*).$$

Analog definiert man die *duale Graßmann-Algebra* von V als $\bigwedge^\bullet V^*$ und erhält zu jeder linearen Abbildung $f : V \to W$ einen Morphismus

$$f^* : \bigwedge^\bullet W^* \to \bigwedge^\bullet V^*.$$

Wir nennen $f^*\alpha$ den *Rückzug* (engl. „pullback“) von α entlang f. Dies ist genau der Rückzug von kontravarianten Tensoren, wie wir ihn im Abschnitt über Determinanten studiert haben.

Beispiel 10.3.24 (Noch einmal Determinanten)**.** Ist $\Phi : V \to V$ ein Endomorphismus eines n-dimensionalen Vektorraums, so ist $\bigwedge^{n*} V$ eindimensional, und daher ist die lineare Abbildung

$$\bigwedge^{n*} \Phi : \bigwedge^{n*} V \to \bigwedge^{n*} V$$

durch Multiplikation mit einem Skalar aus $\mathbb{K}$ (aufgefasst als (1×1)-Matrix) gegeben. Diese Zahl ist nach Definition genau die Determinante von Φ.

Die Graßmann-Algebra gibt also einen konzeptuellen Rahmen für die Theorie der Determinanten. Umgekehrt haben wir Determinanten verwendet, um zu zeigen, dass die vermuteten Erzeuger der Graßmann-Algebra tatsächlich nicht trivial sind.

Zusammenfassung von Abschnitt 10.2.

(1) Die Tensoralgebra des $\mathbb{K}^n$ ist eine assoziative $\mathbb{K}$-Algebra mit n Erzeugern. Ihre universelle Eigenschaft besagt, dass zwischen den Erzeugern keinerlei nicht-triviale Relationen bestehen.

(2) Man erhält beliebige endlich-erzeugte Algebren als Quotienten solcher Tensoralgebren, also indem man zu den Erzeugern Relationen hinzufügt.

(3) Verlangt man, dass alle Erzeuger vertauschen, so erhält man eine symmetrische Algebra (=Polynomalgebra). Verlangt man, dass alle Erzeuger anti-vertauschen, so erhält man die Graßmann-Algebra.

(4) Die Graßmann-Algebra liefert den abstrakten Rahmen für den Determinantenkalkül und lässt sich auch geometrisch interpretieren.

11 Die Matrizenexponentialfunktion

11.1 Matrizen und Potenzreihen

Konstruktion 11.1.1 (Formale Potenzreihen)**.** Ist $\mathbb{K}$ ein Körper, so können wir den Vektorraum $\mathbb{K}^{(\mathbb{N}_0)}$ mit dem Raum der formalen Polynome (in einer Veränderlichen) über $\mathbb{K}$ identifizieren. Statt $(a_0, a_1, \dots)$ schreiben wir $a_0 + a_1 X + \dots$. Die Polynommultiplikation entspricht dann der Faltung

$$(a_n) * (b_n) := (c_n) \quad \text{mit} \quad c_n = \sum_{k+l=n} a(k)b(l). \tag{11.1.1}$$

Ist $\mathscr{A}$ eine $\mathbb{K}$-Algebra, so können wir ein Element $a \in \mathscr{A}$ in Polynome einsetzen, indem wir formal X^k durch a^k ersetzen.

Analog betrachten wir nun Elemente von $\mathbb{K}^{\mathbb{N}_0}$ als *formale Potenzreihen* über $\mathbb{K}$. Dazu schreiben wir formal

$$\sum_{n=0}^{\infty} a_n X^n := (a_n).$$

Die Faltungsformel (11.1.1) ergibt auch für formale Potenzreihen Sinn, da wir ja jeweils nur endlich viele Koeffizienten multiplizieren und addieren müssen. Mit dieser Multiplikation ist dann $\mathbb{K}[[X]]$ eine kommutative assoziative $\mathbb{K}$-Algebra. Das Einsetzen von Elementen ist aber problematisch: Mit den Mitteln der Algebra können wir ja unendliche Summen nicht ausführen. Daher müssen wir jetzt die reine Algebra verlassen und uns der Analysis zuwenden.

Bemerkung 11.1.2. In der Analysis haben sie gelernt, wie man reelle Zahlen in Potenzreihen einsetzt. Dies erfordert einen *Konvergenzbegriff*. Hier wollen wir nun (reelle oder komplexe) Matrizen in Potenzreihen einsetzen. Dafür benötigen wir nun einen Konvergenzbegriff für Matrizen. Zum Glück wissen Sie aus der Analysis bereits, dass man in jedem normierten Vektorraum einen Konvergenzbegriff hat, und auf dem Vektorraum der (reellen oder komplexen) Matrizen haben wir mit der Operatornorm eine natürliche Norm eingeführt. Wir fassen noch einmal zusammen, was wir in Abschnitt 8.4 über die Operatornorm gelernt haben.

Proposition 11.1.3 (C^*-Algebra der Matrizen)**.** *Für $\mathscr{A} := \mathbb{C}^{n\times n}$ und $\|\cdot\| := \|\cdot\|_{\mathrm{op}}$ gilt:*

(i) $\mathscr{A}$ ist eine assoziative $\mathbb{C}$-Algebra.

(ii) $\|\cdot\|$ ist eine Norm auf $\mathscr{A}$, und $(\mathscr{A}, \|\cdot\|)$ ist vollständig.

(iii) $\|\cdot\|$ ist submultiplikativ.

(iv) $x \mapsto x^*$ ist eine Involution auf $\mathscr{A}$ und es gilt $\|x^*\| = \|x\|$ für alle $x \in \mathscr{A}$.

(v) Es gilt $\|x^* x\| = \|x\|^2$ für alle $x \in \mathscr{A}$.

Beweis. (i) ist klar.

(ii), (iii) Dass die Operatornorm eine submultiplikative Norm ist haben wir in Proposition 8.4.23 gesehen. Aus der Analysis wissen Sie, dass jede Norm auf einem *endlichdimensionalen* Vektorraum vollständig ist.

(iv) Es gilt $\|x\| = \rho(\sqrt{x^*x}) = \rho(\sqrt{xx^*})$, und dieser Ausdruck ändert sich nicht, wenn wir x durch x^* ersetzen.

(v) Da x^*x normal ist, gilt $\|x^*x\| = \rho(x^*x) = \sqrt{\rho(x^*x)}^2 = \|x\|^2$. □

Definition 11.1.4. Eine Algebra, $\mathscr{A}$ mit einer Norm $\|\cdot\|$, die Eigenschaften (i)-(iii) erfüllt, heißt *Banach[1]-Algebra*. Gilt zuätzlich (iv) so heißt $(\mathscr{A}, \|\cdot\|, ^*)$ eine B^*-Algebra[2], und gelten (iv) und (v), so heißt $(\mathscr{A}, \|\cdot\|, ^*)$ eine C^*-Algebra[3].

Konstruktion 11.1.5 (Einsetzen in formale Potenzreihen)**.** Es sei $(\mathscr{A}, \|\cdot\|)$ eine (endlichdimensionale[4]) Banach-Algebra und $f = \sum a_n X^n \in \mathbb{R}[[X]]$ eine formale Potenzreihe über $\mathbb{R}$. (Natürlicher wäre es, komplexe Potenzreihen zu verwenden, aber die hatten Sie in der Analysis noch nicht.) Wir nehmen an, dass der *Konvergenzradius*

$$R := (\limsup_{n\to\infty}(\sqrt[n]{|a_n|}))^{-1} > 0$$

positiv ist. Aus der Analyis sind die folgenden Fakten bekannt:

- Die Potenzreihe
$$f(x) := \sum_{k=0}^{\infty} a_k x^k \tag{11.1.2}$$
konvergiert für jedes $x \in (-R, R)$ absolut.
- Die Konvergenz ist gleichmäßig auf jedem kompakten Intervall $[-r, r]$ mit $r < R$, und daher definiert f eine stetige Funktion auf $(-R, R)$.

Es sei nun $A \in \mathscr{A}$ mit $\|A\| < R$. Wir wollen dann ebenfalls A in f einsetzen. Die folgende Proposition besagt, dass dies wohldefiniert ist.

Proposition 11.1.6. *Besitzt $f = \sum a_n X^n \in \mathbb{R}[[X]]$ den Konvergenzradius R und ist $A \in \mathscr{A}$ mit $\|A\| < R$, so konvergieren die Partialsummen*

$$S_n := \sum_{k=0}^{n} a_k B^k \in \mathscr{A}$$

bzgl. der Norm $\|\cdot\|$ gegen ein Element

$$f(A) := \sum_{n=0}^{\infty} a_n A^n \in \mathscr{A}.$$

Beweis. Es sei $r := \|A\|$. Wir verwenden, dass die durch f definierte Potenzreihe auf $[-r, r]$ absolut konvergiert. Dies impliziert, dass die absoluten Partialsummen

$$\widetilde{S}_n := \sum_{k=0}^{n} |a_k| r^k$$

[1] STEFAN BANACH (1892-1945), poln. Mathematiker, einer der Gründerväter der Funktionalanalysis
[2] B für Banach
[3] Den Mathematikern ist tatsächlich nichts besseres eingefallen, als den nächsten Buchstaben zu nehmen.
[4] Diese Annahme ist nicht wirklich nötig.

eine Cauchy-Folge bilden. Da die Norm $\|\cdot\|$ submultiplikativ ist, folgt mit Induktion, dass $\|B^k\| \leq \|B\|^k$. Mit der Dreiecksungleichung folgt, dass für alle $m \geq n$,

$$\|S_m - S_n\| = \left\| \sum_{k=n+1}^{m} a_k B^k \right\| \leq \sum_{k=n+1}^{m} \|a_k B^k\| \leq \sum_{k=n+1}^{m} |a_k| \|B\|^k \leq \sum_{k=n+1}^{m} |a_k| r^k = |\widetilde{S}_m - \widetilde{S}_n|.$$

Da $(\widetilde{S}_n)$ eine Cauchy-Folge ist, ist dann aber auch (S_n) eine Cauchy-Folge, und da $\mathscr{A}$ vollständig bzgl. $\|\cdot\|$ ist, ist diese konvergent. □

Wir können also in eine reelle (oder komplexe) Potenzreihe mit positivem Konvergenzradius nicht nur reelle Zahlen, sondern auch komplexe Zahlen, reelle Matrizen, komplexe Matrizen oder Elemente einer beliebigen Banach-Algebra einsetzen, so lange deren Norm kleiner als der Konvergenzradius ist. Ist $R = \infty$, so definiert dies eine Funktion auf ganz $\mathscr{A}$.

Beispiel 11.1.7 (Matrizenexponentialfunktion)**.** Die vermutlich wichtigste reelle Potenzreihe ist die *Exponentialreihe* $\exp = \sum X^n/n!$. Diese hat unendlichen Konvergenzradius und definiert daher die *Matrizenexponentialfunktion*

$$\exp : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}, \quad B \mapsto \sum_{n=0}^{\infty} \frac{B^n}{n!}.$$

Konkret gilt z.B.

$$\exp\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^0 + \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^1 + \frac{1}{2}\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^2 + \ldots = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

Hier war die Rechnung besonders einfach, da die Matrix nilpotent war und somit fast alle Summanden 0 waren. Betrachtet man hingegen eine Diagonalmatrix, so ist dies nicht der Fall: Es gilt z.B.

$$\exp(\mathrm{diag}(2,3)) = \mathrm{diag}(1,1) + \mathrm{diag}(2,3) + \frac{1}{2}\mathrm{diag}(2^2,3^2) + \frac{1}{6}\mathrm{diag}(2^3,3^3) + \cdots = \mathrm{diag}(e^2, e^3),$$

und hier müssen wir nun wirklich unendlich viele Matrizen addieren.

Wie wir noch sehen werden, übertragen sich viele, aber nicht alle, Rechenregeln für Potenzreihen einer reellen Veränderlichen auf Potenzreihen von Matrizen. Hier ein sehr grundlegenden Beispiel:

Lemma 11.1.8 (Cauchy-Produkt-Formel)**.** *Es seien $x_n, y_n \in \mathscr{A}$ mit $\sum \|x_n\| < \infty$ und $\sum \|y_n\| < \infty$. Dann konvergieren $x := \sum x_n$ und $y := \sum y_n$ und es gilt*

$$x \cdot y = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} x_k y_{n-k} \right).$$

Beweis. Für $N \in \mathbb{N}_0$ definieren wir

$$X_N := \sum_{n=0}^{N} x_n, \quad Y_N := \sum_{n=0}^{N} y_n, \quad \widetilde{X}_n := \sum_{n=0}^{N} \|x_n\| \quad \text{und} \quad \widetilde{Y}_n := \sum_{n=0}^{N} \|y_n\|.$$

Für $M > N > 0$ gilt dann

$$\|X_M - X_N\| = \left\| \sum_{n=N+1}^{M} x_n \right\| \leq \sum_{n=N+1}^{M} \|x_n\| = \|\widetilde{X}_M - \widetilde{X}_n\|.$$

Nach Annahme ist $(\widetilde{X}_N)$ konvergent, also eine Cauchy-Folge, also ist auch (X_n) eine Cauchy-Folge und konvergiert gegen ein $x \in \mathscr{A}$; analog konvergiert (Y_n) gegen ein $y \in \mathscr{A}$. Wir behaupten nun, dass die Partialsummen

$$S_N := \sum_{n=0}^{N} \left(\sum_{k=0}^{n} x_k y_{n-k} \right) = \sum_{k=0}^{N} x_k \sum_{j=0}^{N-k} y_j.$$

gegen $x \cdot y$ konvergieren. Dazu rechnen wir

$$\begin{aligned}
\|x \cdot y - S_N\| &= \left\| (x - X_N) \cdot y + X_N \cdot y - \sum_{k=0}^{N} x_k \sum_{j=0}^{N-k} y_j \right\| \\
&\leq \|x - X_N\| \cdot \|y\| + \left\| \sum_{k=0}^{N} x_k \cdot (y - Y_{n-k}) \right\| \\
&\leq \|x - X_N\| \cdot \|y\| + \left\| \sum_{k=0}^{\lfloor N/2 \rfloor} x_k \cdot (y - Y_{N-k}) \right\| + \left\| \sum_{k=\lfloor N/2 \rfloor + 1}^{N} x_k \cdot (y - Y_{N-k}) \right\| \\
&\leq \|x - X_N\| \cdot \|y\| + \max_{N/2 \leq l \leq N} \|y - Y_l\| \cdot \|X_{\lfloor N/2 \rfloor}\| + \sup_{L \in \mathbb{N}} \|y - Y_L\| \cdot \left\| X_N - X_{\lfloor N/2 \rfloor} \right\|.
\end{aligned}$$

Die Terme $\|x - X_N\|$ sowie $\max_{N/2 \leq l \leq N} \|y - Y_l\|$ und $\left\| X_N - X_{\lfloor N/2 \rfloor} \right\|$ konvergieren für $N \to \infty$ gegen 0, und die übrigen Terme sind beschränkt. Daraus folgt, dass $S_N \to x \cdot y$. □

Beispiel 11.1.9 (Funktionalgleichung der Matrizenexponentialfunktion)**.** Sind $x, y \in \mathscr{A}$ zwei Elemente mit $xy = yx$, so gilt

$$\exp(x + y) = \exp(x) \exp(y).$$

Da x und y vertauschen gilt nämlich für alle $n \in \mathbb{N}_0$, dass

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

und damit erhält man wie im reellen Fall, dass

$$\begin{aligned}
\exp(x + y) &= \sum_{n=0}^{\infty} \frac{1}{n!} (x + y)^n = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} x^k y^{n-k} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^k}{k!} \frac{y^{n-k}}{(n-k)!} = \left(\sum_{n=0}^{\infty} \frac{x^n}{n!} \right) \left(\sum_{n=0}^{\infty} \frac{y^n}{n!} \right) \\
&= \exp(x) \exp(y).
\end{aligned}$$

Es ist aber wichtig, sich klarzumachen, dass diese Funktionalgleichung für nicht-vertauschende Matrizen im Allgemeinen nicht gilt. Ist z.B.

$$x = \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad y = \begin{pmatrix} 0 & 0 \\ -t & 0 \end{pmatrix},$$

für ein $t \in \mathbb{R}$, so gilt einerseits

$$\exp(x) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \wedge \exp(y) = \begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix} \Longrightarrow \exp(x) \exp(y) = \begin{pmatrix} 1 - t^2 & t \\ -t & 1 \end{pmatrix}$$

und andererseits

$$\exp(x + y) = \exp \begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix} = \begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix},$$

also gilt für $t \in \mathbb{R}^\times$, dass $\exp(x + y) \neq \exp(x) \exp(y)$.

Bemerkung 11.1.10 (Praktisches Berechnen der Matrizenexponentialfunktion)**.** Aus der Funktionalgleichung der Matrizenexponentialfunktion ergeben sich einige Hilfsmittel zu ihrer konkreten Berechnung.

(i) Zunächst beobachten wir, dass $\exp(0) = \mathbf{1}$. Da jedes $x \in \mathscr{A}$ mit seinem Negativen vertauscht folgt daraus

$$\exp(x)\exp(-x) = \exp(x+(-x)) = \exp(0) = \mathbf{1} \implies \exp(x) \text{ ist invertierbar mit } \exp(x)^{-1} = \exp(-x).$$

(ii) Ist $x \in \mathscr{A}$ nilpotent mit $x^{N+1} = 0$, so ist

$$\exp(x) = \sum_{n=0}^{N} \frac{x^n}{n!}$$

ein Polynom in x und lässt sich daher berechnen. Ist z.B. x ein nilpotenter Jordanblock, so gilt

$$x = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \implies \exp(x) = \begin{pmatrix} 1 & 1 & \frac{1}{2} & \frac{1}{6} & \dots \\ & 1 & 1 & \frac{1}{2} & \dots \\ & & 1 & 1 & \dots \\ & & & \ddots & \ddots \end{pmatrix}$$

(iii) Ist $y = sxs^{-1}$, so ist $y^n = sx^n s^{-1}$. Daher gilt

$$\exp(sxs^{-1}) = s\exp(x)s^{-1}.$$

(iv) Bis jetzt galten alle unsere Argumente ganz abstrakt in beliebigen Banach-Algebren. Im Falle der Matrizen kann man aber noch einen Schritt weiter gehen: Jedes $x \in \mathbb{C}^{n\times n}$ besitzt eine additive Jordan–Chevalley-Zerlegung $x = x_d + x_n$, wobei x_d eine diagonalisierbare und x_n eine nilpotente Matrix ist und x_d und x_n vertauschen. Es gilt dann also insbesondere

$$\exp(x) = \exp(x_d)\exp(x_n),$$

wobei $\exp(x_n)$ ein Polynom in x_n ist. Ist $x_d = s\operatorname{diag}(\lambda_1, \dots, \lambda_n)s^{-1}$ für ein $s \in \mathrm{GL}_n(\mathbb{C})$, so ist $\exp(x_d) = s\operatorname{diag}(e^{\lambda_1}, \dots, e^{\lambda_n})s^{-1}$, also können wir beide Faktoren von $\exp(x)$ explizit berechnen.

[24.07.24]

Beispiel 11.1.11 (Infinitesimale Drehung)**.** Nicht immer benötigt man Jordan-Theorie, um die Exponentialfunktion einer Matrix auszuwerten. Gerade für kleine Matrizen ist eine direkte Auswertung oft schneller. So gilt etwa

$$\begin{aligned}\exp\begin{pmatrix}0 & -b\\ b & 0\end{pmatrix} &= \mathbf{1} + \begin{pmatrix}0 & -b\\ b & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}-b^2 & 0\\ 0 & -b^2\end{pmatrix} + \frac{1}{6}\begin{pmatrix}0 & b^3\\ -b^3 & 0\end{pmatrix} + \frac{1}{24}\begin{pmatrix}b^4 & 0\\ 0 & b^4\end{pmatrix} + \dots\\ &= \begin{pmatrix}1 - b^2/2 + b^4/24 - \dots & -b + b^3/6 - \dots\\ b - b^3/6 + \dots & 1 - b^2/2 + b^4/24 - \dots\end{pmatrix} = \begin{pmatrix}\cos(b) & -\sin(b)\\ \sin(b) & \cos(b)\end{pmatrix}.\end{aligned}$$

Bemerkung 11.1.12 (Fehlende Injektivität und Surjektivität der Exponentialfunktion)**.** Sei $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. Die Funktion $\exp : \mathbb{K}^{n\times n} \to \mathrm{GL}_n(\mathbb{K})$ ist für $n \geq 2$ nicht injektiv. Für $\mathbb{K} = \mathbb{C}$ folgt die Nicht-Injektivität (sogar für $n = 1$) aus der Tatsache, dass $\exp(2\pi i) = \exp(0)$. Im Reellen sieht man ganz analog, dass

$$\exp\begin{pmatrix}0 & -2\pi\\ 2\pi & 0\end{pmatrix} = \exp\begin{pmatrix}\cos(2\pi) & -\sin(2\pi)\\ \sin(2\pi) & \cos(2\pi)\end{pmatrix} = \mathbf{1} = \exp(0).$$

Für $\mathbb{K} = \mathbb{R}$ ist sie auch nicht surjektiv: Für jede reelle Matrix ist $\det(\exp(A)) = \exp(\mathrm{tr}(A)) \geq 0$; eine Matrix mit negativer Determinante kann also nicht im Bild der Matrizenexponentialfunktion liegen. Für $\mathbb{K} = \mathbb{C}$ ist die Exponentialfunktion stets surjektiv. Wir werden darauf später noch zurückkommen.

Bemerkung 11.1.13 (Vergleich mit dem Spektralkalkül)**.** Es sei $f = \sum a_n X^n \in \mathbb{R}[[X]]$ eine formale Potenzreihe, der Einfachheit halber mit Konvergenzradius $R = \infty$ angenommen. Dann definiert f eine Funktion $F : \mathbb{C} \to \mathbb{C}$. Ist $B \in \mathbb{C}^{n\times n}$ normal, so hatten wir bereits mittels Spektralkalkül die Matrix $F(B)$ definiert. Wir behaupten nun, dass wir ebenfalls $F(B)$ erhalten, wenn wir B in f einsetzen, mit anderen Worten, für normale Matrizen B gilt

$$F(B) = \sum_{k=0}^{\infty} a_k B^k. \tag{11.1.3}$$

Zum Beweis betrachten wir die Spektralzerlegung der linearen Abbildung $\Phi_B : \mathbb{C}^n \to \mathbb{C}^n$, $v \mapsto Bv$. Sei diese gegeben durch

$$\Phi_B = \sum_{j=0}^{l} \lambda_j \pi_j.$$

Setzen wir nun Φ_B in die Partialsummen der Reihe ein, so erhalten wir

$$\sum_{k=0}^{n} a_k \Phi_B^k = \sum_{j=0}^{l} \left(\sum_{k=0}^{n} a_k \lambda_j^k\right) \pi_j.$$

Die innere Summe konvergiert nun für $n \to \infty$ gegen $F(\lambda_j)$. Es folgt daher, dass

$$\sum_{k=0}^{\infty} a_k B^k = \lim_{n\to\infty} \sum_{j=0}^{l} \left(\sum_{k=0}^{n} a_k \lambda_j^k\right) \pi_j = \sum_{j=0}^{l} \left(\lim_{n\to\infty} \sum_{k=0}^{n} a_k \lambda_j^k\right) \pi_j = \sum_{j=0}^{l} F(\lambda_j)\pi_j = F(B).$$

Unsere neue Definition von $f(B)$ erweitert also die Definition via Spektralkalkül auf beliebige (d.h. nicht notwendig normale) Matrizen. Hat f einen endlichen Konvergenzradius R, so ist f immerhin noch auf allen Matrizen von Operatornorm $< R$ definiert, ob sie normal sind oder nicht.

Wir halten fest: Normale Matrizen kann man (mittels Spektralkalkül) in beliebige Funktionen einsetzen, nicht-normale Matrizen nur in Funktionen, die durch Potenzreihen mit hinreichend großem Spektralradius gegeben sind.

Zusammenfassung von Abschnitt 11.1.

(1) Über beliebigen Körpern kann man formale Potenzreihen definieren.

(2) Über den reellen oder komplexen Zahlen kann man Elemente von Banachalgebren in Potenzreihen einsetzen, sofern deren Norm kleiner als der Konvergenzradius ist. Im Fall von Matrizen erweitert dies den Spektralkalkül normaler Matrizen.

(3) Die Matrizenexponentialfunktion genügt für vertauschende Matrizen A und B der Funktionalgleichung $\exp(A+B) = \exp(A)\exp(B)$. Dies ermöglicht die explizite Berechnung der Exponentialfunktion mittels Jordan–Chevalley-Zerlegung.

11.2 Einparameteruntergruppen von $\mathrm{GL}_n(\mathbb{R})$

Definition 11.2.1. Sei $U \subseteq \mathbb{R}^n$ eine offene Teilmenge und $I \subseteq \mathbb{R}$ ein Intervall (offen, abgeschlossen oder halboffen, beschränkt oder unbeschränkt). Eine stetige Abbildung $\gamma : I \to U$ heißt eine *parametrisierte Kurve*. Das Bild $\gamma[I]$ heißt dann die zugehörige *Spur*.

Im Folgenden wollen wir spezielle Kurven in der Gruppe $\mathrm{GL}_n(\mathbb{R})$ betrachten, die in engem Zusammenhang zur Matrizenexponentialfunktion stehen. Man beachte, dass wegen der Stetigkeit der Determinanten die Menge

$$\mathrm{GL}_n(\mathbb{R}) = \det^{-1}(\mathbb{R} \setminus \{0\})$$

eine offene Teilmenge von $\mathbb{R}^{n\times n}$ ist.

Definition 11.2.2. Eine Kurve $\gamma : \mathbb{R} \to \mathrm{GL}_n(\mathbb{R})$ heißt eine *parametrisierte Einparameteruntergruppe*, falls γ ein Gruppenhomomorphismus ist, d.h.

$$\gamma(t+s) = \gamma(t)\gamma(s) \quad (t,s \in \mathbb{R}).$$

Die Spur von γ ist dann eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$, genannt die zugehörige *Einparameteruntergruppe*.

Beispiel 11.2.3 (Erzeugte Einparameteruntergruppen)**.** Ist $X \in \mathbb{R}^{n\times n}$, so gilt wegen der Funktionalgleichung der Matrizenexponentialfunktion, dass

$$\exp((t+s)X) = \exp(tX + sX) = \exp(tX)\exp(sX) \quad (t,s \in \mathbb{R}).$$

Daher ist die Kurve

$$\gamma_X : \mathbb{R} \to \mathrm{GL}_n(\mathbb{R}), \quad t \mapsto \exp(tX)$$

eine parametrisierte Einparameteruntergruppe, genannt die *von X erzeugte parametrisierte Einparametergruppe*.

Unser nächstes Ziel ist es zu zeigen, dass diese Beispiele schon *alle* differenzierbaren Einparameteruntergruppen abdecken. Dazu benötigen wir:

Proposition 11.2.4 (Ableitungsformel)**.** *Für jedes $X \in \mathbb{R}^{n\times n}$ ist die Kurve γ_X differenzierbar mit*

$$\gamma_X'(t) = X\gamma(t). \tag{11.2.1}$$

Insbesondere ist $X = \gamma_X'(0)$ durch γ_X eindeutig bestimmt.

Beweis. Nach Definition ist γ_X genau dann differenzierbar mit Ableitung γ_X', wenn für alle $t \in \mathbb{R}$ eine Entwicklung der Form

$$\gamma_X(t+h) = \gamma_X(t) + h\gamma_X'(t) + r(t,h) \quad \text{mit} \quad \lim_{h\to 0} \frac{\|r(t,h)\|}{|h|} = 0$$

vorliegt. Wir wollen zeigen, dass $\gamma_X'(t) = X\gamma_X(t)$ gilt, und betrachten daher die Funktion

$$r(t,h) := \gamma_X(t+h) - \gamma_X(t) - hX\gamma_X(t).$$

Es gilt dann

$$r(t,h) \quad = \quad \gamma_X(h)\gamma_X(t) - \gamma_X(t) - hX\gamma_X(t) \quad = \quad (\gamma_X(h) - \mathbf{1} - hX)\gamma_X(t) \quad = \quad \sum_{n=2}^{\infty} \frac{h^n X^n}{n!}\gamma_X(t),$$

und folglich

$$\frac{\|r(t,h)\|}{|h|} \le |h| \cdot \sum_{n=2}^{\infty} \frac{|h|^{n-2}\|X\|^n}{n!}\|\gamma_X(t)\| \xrightarrow{|h|\to 0} 0. \qquad \square$$

Um aus Proposition 11.2.4 die Klassifikation der differenzierbaren Einparameteruntergruppen zu folgern, benötigen wir eine Form der Produktregel für matrizenwertige Funktionen.

Bemerkung 11.2.5 (Produktregel)**.** Sei $(V, \|\cdot\|)$ ein vollständiger normierter Vektorraum und $B : V \times V \to V$ stetig und bilinear. Sind $\gamma_1, \gamma_2 : \mathbb{R} \to V$ differenzierbare parametrisierte Kurven, so gilt

$$\gamma_j(t+h) = \gamma_j(t) + h\gamma_j'(t) + r_j(t,h)$$

für Funktionen r_j mit $\|r_j(t,h)\|/|h| \to 0$ für alle $t \in \mathbb{R}$. Definieren wir nun

$$\gamma(t) := B(\gamma_1(t), \gamma_2(t)),$$

so folgt, dass

$$\begin{aligned} \gamma(t+h) &= B(\gamma_1(t) + h\gamma_1'(t) + r_1(t,h), \gamma_2(t) + h\gamma_2'(t) + r_2(t,h)) \\ &= B(\gamma_1(t), \gamma_2(t)) + h(B(\gamma_1(t), \gamma_2'(t)) + B(\gamma_1'(t), \gamma_2(t))) + r(t,h), \end{aligned}$$

wobei $r(t,h) = B(\gamma_1(t) + h\gamma_1'(t), r_2(t,h)) + B(r_1(t,h), \gamma_2(t) + h\gamma_2'(t))$ und daher

$$r(t,h)/h = B(\gamma_1(t) + h\gamma_1'(t), r_2(t,h)/h) + B(r_1(t,h)/h, \gamma_2(t) + h\gamma_2'(t)) \to 0.$$

Es gilt daher $\gamma'(t) = B(\gamma_1(t), \gamma_2'(t)) + B(\gamma_1'(t), \gamma_2(t))$. Ist speziell $\mathscr{A}$ eine Banach-Algebra und B die Multiplikationsabbildung, so folgt die *Produktregel*

$$(\gamma_1(t)\gamma_2(t))' = \gamma_1(t)\gamma_2'(t) + \gamma_1'(t)\gamma_2(t). \tag{11.2.2}$$

Beispiel 11.2.6. Aus der Produktregel und (11.2.1) folgt sofort, dass

$$\gamma_X''(t) = (\gamma_X'(t))' = (X\gamma_X(t))' = X\gamma_X(t)' + X'\gamma_X(t) = X(X\gamma_X(t)) + 0\gamma_X(t) = X^2\gamma_X(t),$$

und induktiv $\gamma_X^{(n)}(t) = X^n\gamma_X(t)$ für alle $n \in \mathbb{N}$. Insbesondere ist γ_X beliebig oft differenzierbar.

Satz 11.2.7 (Klassifikation der differenzierbaren Einparameteruntergruppen)**.** *Sei* $X \in \mathbb{C}^{n\times n}$.

(i) Ist $\gamma : \mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$ *eine differenzierbare parametrisierte Kurve mit* $\gamma(0) = \mathbf{1}$ *und* $\gamma'(t) = X\gamma(t)$ *für alle* $t \in \mathbb{R}$*, so gilt* $\gamma = \gamma_X$.

(ii) γ_X *ist die eindeutig bestimmte differenzierbare parametrisierte Einparameteruntergruppe von* $\mathrm{GL}_n(\mathbb{C})$ *mit* $\gamma_X'(0) = X$.

Beweis. (i) Es sei γ eine differenzierbare Abbildung mit den genannten Eigenschaften, und $\sigma : \mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$ gegeben durch $t \mapsto \gamma_{(-X)}(t)\gamma(t)$. Aufgrund der Anfangswertbedingung gilt

$$\sigma(0) = \gamma_{(-X)}(0)\gamma(0) = \mathbf{1}$$

Aufgrund der Produktregel gilt weiterhin, dass

$$\sigma'(t) = \gamma'_{(-X)}(t)\gamma(t) + \gamma_{(-X)}(t)\gamma'(t) = -X\gamma_{(-X)}(t)\gamma(t) + \gamma_{(-X)}(t)X\gamma(t) = 0,$$

weil X und $\gamma_{-X}(t)$ vertauschen. Daher ist σ konstant gleich $\mathbf{1}$, und daher gilt für alle $t \in \mathbb{R}$, dass

$$\gamma(t) = \gamma_{(-X)}(t)^{-1} = \exp(-tX)^{-1} = \exp(tX) = \gamma_X(t).$$

(ii) Ist γ eine parametrisierte Einparametergruppe mit $\gamma'(0) = X$, so ist $\gamma(0) = \mathbf{1}$ (weil γ ein Homomorphismus ist), und es gilt

$$\gamma'(t) = \lim_{h\to 0} \frac{\gamma(t+h) - \gamma(t)}{h} = \lim_{h\to 0} \frac{\gamma(h) - \gamma(0)}{h}\gamma(t) = \gamma'(0)\gamma(t) = X\gamma(t).$$

Aus (i) folgt daher $\gamma = \gamma_X$. □

Korollar 11.2.8. *Ist eine parametrisierte Einparametergruppe differenzierbar, so ist sie beliebig oft differenzierbar.* □

Mit etwas mehr Analysis kann man zeigen, dass sogar jeder stetige parametrisierte Einparametergruppe differenzierbar (und daher beliebig oft differenzierbar) ist.

Bemerkung 11.2.9 (Geometrische Interpretation)**.** Da $\mathrm{GL}_n(\mathbb{C})$ eine offene Teilmenge von $\mathbb{C}^{n\times n}$ ist, können wir uns $\mathbb{C}^{n\times n}$ als die Menge der möglichen infinitesimalen Richtungen im Punkt $\mathbf{1} \in \mathrm{GL}_n(\mathbb{C})$ vorstellen („Tangentialraum“ an $\mathbf{1}$). Für jede mögliche infinitesimale Richtung, die wir uns vorgeben (also jedes $X \in \mathbb{C}^{n\times n}$) gibt es dann genau einen differenzierbaren Homomorphismus $\mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$, der in $\mathbf{1}$ in diese Richtung verläuft. Obwohl wir zunächst nur annehmen, dass dieser Homomorphismus einmal differenzierbar ist, stellt sich am Ende heraus, dass er beliebig oft differenzierbar ist.

Ersetzen wir eine Matrix X durch ein Vielfaches tX, so haben die Kurven γ_X und γ_{tX} dieselbe Spur, nur wird diese schneller/langsamer/in umgekehrter Richtung durchlaufen. Die Exponentialfunktion liefert daher eine Bijektion zwischen Geraden in $\mathbb{C}^{n\times n}$ und Einparametergruppen in $\mathrm{GL}_n(\mathbb{C})$. Analog erhalten wir eine Bijektion zwischen Geraden in $\mathbb{R}^{n\times n}$ und Einparametergruppen in $\mathrm{GL}_n(\mathbb{R})$.

Wir erhalten so ein gutes Verständnis von „eindimensionalen“ Untergruppen von $\mathrm{GL}_n(\mathbb{R})$ bzw. $\mathrm{GL}_n(\mathbb{C})$. Die Beschreibung höherdimensionaler Untergruppen (die von mehreren Parametern abhängen) ist viel schwieriger, weil die Funktionalgleichung der Exponentialfunktion für nichtkommutierende Matrizen versagt.

Wir betrachten nun eine wichtige Anwendung von Einparameteruntergruppen auf eine spezielle Klasse gewöhnlicher Differentialgleichungen.

Satz 11.2.10 (Differentialgleichungen mit konstanten Koeffizienten)**.** *Sei $A \in \mathbb{R}^{n\times n}$ und $v \in \mathbb{R}^n$. Dann existiert genau eine differenzierbare Funktion $f : \mathbb{R} \to \mathbb{R}^n$ mit*

$$\begin{cases} f'(t) = Af(t), \\ f(0) = v, \end{cases} \tag{11.2.3}$$

Diese ist gegeben durch $f(t) = \exp(tA)v$.

Beweis. Wir stellen zunächst eine Vorüberlegung an. Matrix-Vektor-Multiplikation definiert eine bilineare Abbildung $\mathbb{R}^{n\times n} \times \mathbb{R}^n \to \mathbb{R}^n$, $(A, v) \mapsto Av$. Unser Beweis der Produktregel für Banachalgebren hat lediglich die Bilinearität der Multiplikation verwendet und überträgt sich daher auf Matrix-Vektor-Multiplikation. Sind also $\gamma : \mathbb{R} \to \mathbb{R}^{n\times n}$ und $\sigma : \mathbb{R} \to \mathbb{R}^n$ differenzierbare Kurven, so ist $\gamma(t)\sigma(t)$ differenzierbar mit

$$(\gamma(t)\sigma(t))' = \gamma'(t)\sigma(t) + \gamma(t)\sigma'(t).$$

Wenden wir diese Regel nun auf die Funktion $f_{A,v}(t) := \exp(tA)v$ an, so erhalten wir

$$f'_{A,v}(t) = \exp(tA)'v + \exp(tA)v' = A\exp(tA)v + \exp(tA)0 = Af_{A,v}(t).$$

Nach Definition gilt weiter $f_{A,v}(0) = \exp(0)v = v$, also ist $f_{A,v}$ eine Lösung von (11.2.3).

Ist andererseits f eine beliebige Lösung und $g(t) := \exp(-tA)f(t)$, so gilt $g(0) = v$ und

$$g'(t) = (\exp(-tA))'f(t) + \exp(-tA)f'(t) = -A\exp(-tA)f(t) + \exp(-tA)Af(t) = 0,$$

also ist $g(t) = v$ für alle $t \in \mathbb{R}$. Daraus folgt, dass $f(t) = \exp(tA)v$ für alle $t \in \mathbb{R}$. □

Eine Differentialgleichung der Form

$$f'(t) = Af(t)$$

mit $f : \mathbb{R} \to \mathbb{R}^n$ und $A \in \mathbb{R}^{n\times n}$ heißt eine *Differentialgleichung erster Ordnung mit konstanten Koeffizienten*.

Beispiel 11.2.11 (Fadenpendel)**.** Bei einem idealisierten ungedämpften eindimensionalen Fadenpendel („harmonischer Oszillator“) ist die Beschleunigung proportional zur Auslenkung. In geeigneten Koordinaten ist die Auslenkung des Pendels daher eine Lösung der Differrentialgleichung

$$x''(t) = -x(t).$$

Dabei ist $x(t)$ die Auslenkung und $x''(t)$ die Beschleunigung; das Minuszeichen kommt hier daher, dass die Beschleunigung in Gegenrichtung der Auslenkung erfolgt. Es bezeichne $y(t) := x'(t)$ die Geschwindigkeit des Pendels; es gilt dann

$$x'(t) = y(t) \text{ und } y'(t) = x''(t) = -x(t) \implies \begin{pmatrix} x(t) \\ y(t) \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x(t) \\ y(t) \end{pmatrix}.$$

Dies ist nun eine Differentialgleichung erster Ordnung mit konstanten Koeffizienten. Sind x_0 und y_0 die Auslenkung bzw. Geschwindigkeit des Pendels zur Zeit $t = 0$, so gilt also

$$\begin{pmatrix} x(t) \\ y(t). \end{pmatrix} = \exp\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}.$$

Es gilt also

$$x(t) = \cos(t)x_0 + \sin(t)y_0,$$

insbesondere ist die Pendelbewegung periodisch.

Mehr zu Differentialgleichungen mit konstanten Koeffizienten lernen Sie in der Vorlesung ANALYSIS III. Zum expliziten Lösen solcher Differentialgleichungen muss man in der Lage sein, die Matrizenexponentialfunktion auszuwerten. Das wiederum läuft daraus hinauf, dass man die Jordan–Chevalley-Zerlegung einer Matrix explizit berechnen kann.

Bemerkung 11.2.12 (Langzeitverhalten von Lösungen)**.** In den Anwendungen interessiert man sich häufig für das Langzeitverhalten (d.h. $t \to \infty$) für Lösungen von Differentialgleichungen erster Ordnung mit konstanten Koeffizienten. Ist f die eindeutige differenzierbare Funktion, die (11.2.3) löst, so hängt das Verhalten von f sehr stark vom Anfangswert $v = f(0)$ ab:

- Ist v im Eigenraum zu einem reellen Eigenwert λ, so gilt

  $$f(t) = \exp(tA)v = \sum_{n=0}^{\infty} \frac{t^n A^n v}{n!} = \sum_{n=0}^{\infty} \frac{t^n \lambda^n v}{n!}.$$

  Ist $\lambda < 0$, so folgt $f(t) \to 0$. Ist $\lambda = 0$, so ist $f(t)$ konstant. Ist hingegen $a = \mathrm{Re}(\lambda) > 0$, so bewegt sich v entlang der Geraden $\mathbb{R}v$ nach ∞, und zwar mit exponentieller Geschwindigkeit.

- Ist A reell diagonalisierbar, so können wir v zerlegen als $v = v_{\lambda_1} + \cdots + v_{\lambda_k}$, wobei v_{λ_j} ein Eigenvektor zum Eigenwert λ_j ist. Wir dürfen annehmen, dass $\lambda_1 > \cdots > \lambda_k$ gilt. Es ist dann

  $$f(t) = e^{t\lambda_1}(v_{\lambda_1} + e^{t(\lambda_2-\lambda_1)}v_{\lambda_2} + \cdots + e^{t(\lambda_k-\lambda_1)}v_{\lambda_k}),$$

  wobei alle Summanden mit Ausnahme des ersten gegen 0 konvergieren. Das Langzeitverhalten hängt daher im Wesentlichen von λ_1 ab: Ist $\lambda_1 > 0$, so divergiert $f(t)$, ist $\lambda_1 < 0$, so konvergiert $f(t)$ gegen 0, und ist $\lambda_1 = 0$, so konvertiert f gegen v_{λ_1}. Stabilität ist dann gleichbedeutend mit $\lambda_1 \leq 0$. In jedem Fall nähert sich $f(t)$ mit exponentieller Geschwindigkeit der Eigengeraden $\mathbb{R}v_{\lambda_1}$ an.

- Es sei nun $(\lambda, \overline{\lambda})$ ein paar komplex-konjugierter nicht-reeller komplexer Eigenwerte von A und $v \in \mathbb{R}^n \cap (V_\lambda \oplus V_{\overline{\lambda}})$. Wir können uns auf den Fall zurückziehen, dass

  $$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad \text{und} \quad v = e_1,$$

  wobei $\lambda = a + ib$. Wegen

  $$\exp\left(t\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) = \begin{pmatrix} e^{ta}\cos(tb) & -e^{ta}\sin(tb) \\ e^{ta}\sin(bt) & e^{ta}\cos(bt) \end{pmatrix}.$$

  gilt dann

  $$f(t) = \begin{pmatrix} e^{ta}\cos(tb) \\ e^{ta}\sin(tb) \end{pmatrix} \quad \text{und} \quad \|f(t)\| = e^{ta}.$$

  Ist $a = \mathrm{Re}(\lambda) < 0$, so konvergiert $\|f(t)\|$ exponentiell schnell gegen 0, aber $f(t)$ verläuft jetzt nicht mehr entlang einer Geraden, sondern spiralförmig innerhalb einer Ebene. Ist $\mathrm{Re}(\lambda) > 0$, so divergiert $f(t)$ mit exponentieller Geschwindigkeit entlang einer sich öffnenden Spirale. Ist hingegen $\mathrm{Re}(\lambda) = 0$, so bewegt sich $f(t)$ entlang einer Kreisbahn. Die Bahnen sind also „stabil“ genau dann, wenn $\mathrm{Re}(\lambda) \leq 0$.

- Es sei nun A komplex-diagonalisierbar. Wir zerlegen dann wieder $v = v_{\lambda_1} + \cdots + v_{\lambda_k}$ mit $v_{\lambda_j} \in \mathbb{R}^n \cap (V_{\lambda_j} \oplus V_{\overline{\lambda_j}})$. Es dominieren dann die Eigenvektoren, deren Eigenwert den maximalen Realteil unter den λ_j hat. Es ist dann $f(t)$ genau dann stabil, wenn

$$M := \max\{\mathrm{Re}(\lambda_j) \mid 1 \le j \le n\} \le 0.$$

  Ist $M < 0$, so bewegt sich f exponentiell schnell gegen 0, im Falle eines eindeutigen Eigenwerts mit maximalem Realteil bis auf einen exponentiell kleineren Fehlerterm entlang einer Geraden oder Spiralen, ansonsten ist die Bahn komplizierter. Der Fall $M > 0$ bedeutet exponentiell schnelles Wachstum. Ist $M = 0$, so nähert sich $f(t)$ asymptotisch einer „stabilen Mannigfaltigkeit“, die in den einfachsten Fällen ein Punkt oder Kreis ist.

- Im allgemeinen Fall verwendet man statt der Eigenraumzerlegung die Hauptraumzerlegung. Wir betrachten der Einfachheit halber nur den Fall, wo v selbst in einem Hauptraum (zum Eigenwert $\lambda = a + bi$) liegt. Wir dürfen annehmen, dass A in reeller Jordannormalform ist; es gilt dann $f(t) \to 0$ bzw. $f(t) \to \infty$ (jeweils mit exponentieller Geschwindigkeit), falls $a < 0$ bzw. $a > 0$. Der Fall $a = 0$ ist interessant: Ist A komplex diagonalisierbar, so bewegt sich $f(t)$ entlang einer Kreisbahn oder ist konstant. Ist hingegen A nicht komplex-diagonalisierbar, so erhalten wir u.U. zusätzliche Terme aus dem nilpotenten Teil der Jordan–Chevalley-Zerlegung. In diesem Fall kann es dann vorkommen, dass $f(t)$ mit lediglich polynomieller Geschwindigkeit divergiert. Ein typisches Beispiel ist

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad v = e_2.$$

  Hier gilt dann

$$f(t) = \begin{pmatrix} t \\ 1 \end{pmatrix} \to \infty.$$

Mehr zum Langzeitverhalten von Differentialgleichungen können Sie in einer Vorlesung über DYNAMISCHE SYSTEME lernen.

Zusammenfassung von Abschnitt 11.2.

(1) Für $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ übersetzt die Matrizenexponentialfunktion Geraden in $\mathbb{K}^{n\times n}$ in Einparameteruntergruppen von $\mathrm{GL}_n(\mathbb{K})$.

(2) Jede parametrisierte Einparameteruntegruppe γ ist durch ihre Ableitung X in 0 eindeutig bestimmt und von der Form $t \mapsto \exp(tX)$.

(3) Die eindeutige Lösung der DGL $f'(t) = Af(t)$ mit Anfangswert $f(0) = v$ ist $f(t) = \exp(tA)v$. Diese lässt sich mittels Jordan-Theorie explizit ausrechnen und qualitativ analysieren.

[26.07.24]

11.3 Lokale Invertierbarkeit der Matrizenexponentialfunktion

Wir haben bereits gesehen, dass die (reelle) Matrizenexponentialfunktion weder injektiv noch surjektiv ist. Wir wollen uns nun noch überlegen, dass sie zumindest lokal in der Nähe der 0 eine Bijektion ist. Um dies nachzuweisen, können wir die folgende Konsequenz von Proposition 11.2.4 verwenden.

Korollar 11.3.1 (Ableitung der Exponentialfunktion an der 0)**.** *Sei* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. *Dann gilt für die Matrizenexponentialfunktion* $\exp : \mathbb{K}^{n\times n} \to \mathrm{GL}_n(\mathbb{K})$*, dass*

$$d\exp(0) = \mathrm{Id}.$$

Beweis. Für $X \in \mathbb{K}^{n\times n}$ gilt

$$d\exp(0)(X) = \exp(0 + tX)' = \gamma_X'(t) = X. \qquad \square$$

Bemerkung 11.3.2 (Lokale Invertierbarkeit)**.** Ein wichtiger Satz der Analysis, der sogenannte *Satz von der Umkehrfunktion*, besagt, dass eine differenzierbare Selbstabbildung $f : V \to V$ eines endlichdimensionalen normierten Vektorraums eine Umgebung U eines Punkts $p \in V$ bijektiv auf eine Umgebung U' von $f(p)$ abbildelt, falls die lineare Abbildung $df(p)$ bijektiv ist. In diesem Fall ist nicht nur die Einschränkung $f|_U^{U'}$, sondern auch ihre Umkehrabbildung differenzierbar - man nennt dann f einen *lokalen C^1-Diffeomorphismus* um p.

Aus Korollar 11.3.1 folgt, dass es eine Umgebung $U \subseteq \mathbb{K}^{n\times n}$ von 0 und eine Umgebung $V \subseteq \mathbb{K}^{n\times n}$ von $\mathbf{1} = \exp(0)$ in $\mathrm{GL}_n(\mathbb{C})$ gibt, so dass $\exp|_U^V : U \to V$ ein Diffeomorphismus ist. Wir werden im Folgenden eine lokale Umkehrabbildung explizit konstruieren.

Bemerkung 11.3.3 (Ableiten von Potenzreihen von Matrizen)**.** Die Aussage, dass $d\exp(0) = \mathrm{Id}$ verallgemeinert die Eigenschaft der klassischen Exponentialfunktion, wonach $\exp'(0) = \exp(0) = 1$. Was ist mit den Ableitungen der Exponentialfunktion an anderen Matrizen? Man kann diese in der Tat berechnen, aber das ist deutlich schwieriger. Das Problem wird bereits bei einer einfachen Matrizenfunktion wie

$$p_2 : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}, \quad X \mapsto X^2$$

deutlich. Man würde vielleicht naiv erwarten, dass $dp_2(X)(H) = 2XH$ gilt, in Wahrheit gilt aber Hier gilt

$$p_2(X+H) = (X+H)(X+H) = X^2 + XH + HX + H^2 = p_2(X) + (XH + HX) + H^2,$$

und folglich $dp_2(X)(H) = XH + HX$. Definiert man allgemeiner $p_n(X) := X^n$, so erhält man analog

$$dp_3(X)(H) = X^2H + XHX + HX^2, \quad dp_4(X)(H) = X^3H + X^2HX + XHX^2 + HX^3 \quad \text{usw.}$$

Für Potenzreihen von Matrizen gilt entsprechend

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \implies df(X)(H) = \sum_{n=1}^{\infty} a_n Dp_n(X)(H),$$

und das ist keine schöne Potenzreihe in X mehr, es sei denn X und H vertauschen miteinander.

Wir wenden uns nun der Frage zu, wie man die Exponentialfunktion explizit lokal invertieren kann. Für die Exponentialfunktion auf $\mathbb{R}$ kennen wir eine lokale Umkehrfunktion (den Logarithmus), die auch durch eine Potenzreihe um 1 gegeben ist. Kann man dieses Resultat einfach auf Matrizen übertragen? Nach der letzten Bemerkung scheint Vorsicht geboten. Wir schauen uns die entsprechende Frage zunächst für Polynome an.

Bemerkung 11.3.4 (Fortsetzen von Polynomidentitäten)**.** Nehmen wir an, wir haben Polynome $f,g \in \mathbb{R}[X]$ gegeben, und für alle $x \in \mathbb{R}$ gilt eine Identität wie z.B.

$$f(x)g(x) + 3g^2(x) = (f \circ g)(x). \tag{11.3.1}$$

Gilt dann automatisch auch $f(A)g(A) + 3g^2(A) = (f \circ g)(A)$ für alle $A \in \mathbb{C}^{n\times n}$?

Addition, Skalarmultiplikation und Multiplikation (und daher die linke Seite) sind harmlos: Ist $\mathscr{A}$ eine assoziative $\mathbb{R}$-Algebra und $a \in \mathscr{A}$ so ist die Auswertungsabbildung $\mathbb{K}[X] \to \mathscr{A}$, $f \mapsto f(a)$ bekanntlich ein Morphismus. Wie sieht es nun mit der Verkettung aus? Auch hier gibt es kein Problem: Sind $f = \sum a_n X^n$ und $g = \sum_n X^n$ formale Polynome, so können wir $f \circ g$ abstrakt definieren durch

$$f \circ g := \sum_{n=0}^{\deg(f)} a_n \left(\sum_{k=0}^{\deg(g)} b_k X^k \right)^n \tag{11.3.2}$$

Diese Definition ist gerade so gemacht, dass $f \circ g(a) = f(g(a))$ für alle $a \in \mathscr{A}$ gilt. Gilt also (11.3.1) für alle $x \in \mathbb{R}$ (und daher für die entsprechenden formalen Polynome), so gilt die entsprechende Gleichung auch für Matrizen.

Wir können sogar noch weiter gehen: Sind $f,g \in \mathbb{R}[X]$, so gilt $f = g$ in $\mathbb{R}[X]$ genau dann, wenn $f(x) = g(x)$ für alle x in einem Intervall der Form $(-\varepsilon,\varepsilon)$ mit $\varepsilon > 0$. Ist nämlich $f = \sum a_n X^n$, so ist $a_n = f^{(n)}(0)/n!$, und daher hängen die Koeffizienten nur von dem Verhalten von f bei 0 ab. Um die Ableitungen ausrechnen zu können, genügt es sogar die Funktion an einer beliebigen Folge zu kennen, die gegen 0 konvergiert. (Statt 0 kann man auch einen beliebigen anderen Entwicklungspunkt nehmen.)

Korollar 11.3.5 (Identitätssatz für Polynome)**.** *Es sei $\mathscr{A}$ eine assoziative $\mathbb{R}$-Algebra und $M \subseteq \mathbb{R}$ eine Menge mit mindestens einem Häufungspunkt. Sind $f,g,h \in \mathbb{R}[X]$ mit $f \circ g|_M = h|_M$, so gilt $f(g(a)) = h(a)$ für alle $a \in \mathscr{A}$.* □

Für Potenzreihen gilt im Grunde dasselbe, nur muss man hier aufpassen, dass alles konvergiert. Für die Algebra-Operationen ist dies sehr leicht einzusehen:

Übung 11.3.6. Zeigen Sie: Für jedes $R > 0$ bilden die formalen Potenzreihen mit Konvergenzradius $\geq R$ eine $\mathbb{R}$-Unteralgebra $\mathbb{R}[[X]]_{\geq R}$ von $\mathbb{R}[[X]]$. Ist $(\mathscr{A}, \|\cdot\|)$ eine Banach-Algebra und $B_R(0) := \{a \in \mathscr{A} \mid \|a\| < R\}$, so ist die Abbildung

$$\mathrm{ev} : \mathbb{R}[[X]]_{\geq R} \to \mathscr{A}^{B_R(0)}, \quad \mathrm{ev}(f)(a) := f(a)$$

ein Homomorphismus von $\mathbb{R}$-Algebren

Satz 11.3.7 (Identitätssatz für Potenzreihen)**.** *Es sei $(\mathscr{A}, \|\cdot\|)$ eine Banach-Algebra und es seien $f = \sum a_n X^n \in \mathbb{R}[[X]]_{\geq R}$ und $g = \sum b_n X^n, h = \sum c_n X^n \in \mathbb{R}[[X]]_{\geq S}$ reelle Potenzreihen. Es gelte*

$$\sum_{n=0}^{\infty} |b(n)| s^n < R \quad \text{für alle } s \in (0,S). \tag{11.3.3}$$

Falls eine Menge $M \subseteq \mathbb{R}$ mit Häufungspunkt 0 existiert mit

$$f(g(x)) = h(x) \quad \text{für alle } x \in M,$$

so gilt

$$f(g(A)) = h(A) \quad \text{für alle } x \in B_S(0) \subseteq \mathscr{A}.$$

Die Annahme (11.3.3) impliziert, dass $g[B_S(0)] \subseteq B_R(0)$, und daher ist $f \circ g$ auf $B_S(0)$ wohldefiniert. Der Beweis funktioniert dadurch, dass man die entsprechenden Potenzreihen durch Polynome approximiert und dann Korollar 11.3.5 anwendet. Die Schwierigkeit liegt darin, die Fehlerterme genau zu kontrollieren - das ist zwar mit Methoden der Analysis II machbar, aber durchaus anspruchsvoll. Wir lassen den Beweis hier aus und gegen stattdessen die gewünschte Anwendung.

Beispiel 11.3.8. Für alle $x \in (-1,1)$ gilt

$$-\log(1-x) = \int_0^x (-\log(1-t))'\,dt = \int_0^x \frac{1}{1-t}\,dt = \int_0^x \sum_{n=0}^{\infty} t^n\,dt = \sum_{n=1}^{\infty} \frac{x^n}{n},$$

oder äquivalent

$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.$$

Definieren wir nun also eine formale Potenzreihe

$$\ell := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} \in \mathbb{R}[[X]],$$

so hat diese den Konvergenzradius 1, und es gilt

$$\ell(x) = \log(1+x) \text{ für alle } x \in (-1,1), \quad \text{also} \quad \log(x) = \ell(x-1) \text{ für alle } x \in (0,2).$$

Ist $x \in (-\log 2, \log 2)$, so gilt $\exp(x) \in (0,2)$ und folglich

$$x = \log(\exp(x)) = \ell(\exp(x)-1) \quad \text{für alle } x \in (-\log 2, \log_2).$$

Analog gilt

$$y = \exp(\log(y)) = \exp(\ell(x-1)), \quad \text{falls } |x-1| < 1.$$

Definition 11.3.9. Der *Matrizenlogarithmus* ist die Funktion

$$\log : \{\in \mathbb{C}^{n\times n} \mid \|B - \mathbf{1}\| < 1\} \to \mathbb{C}^{n\times n}, \quad B \mapsto \ell(B-\mathbf{1}) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(B-\mathbf{1})^n}{n}.$$

Korollar 11.3.10. *Seien $A, B \in \mathbb{C}^{n\times n}$ mit $\|A\| < \log(2)$ und $\|B - \mathbf{1}\| < 1$. Dann gilt*

$$\log(\exp(A)) = A \quad \text{und} \quad \exp(\log(B)) = B.$$

Insbesondere ist log *die lokale Umkehrfunktion von* exp *bei* $\mathbf{1}$. □

Bemerkung 11.3.11 (Unipotente und nilpotente Matrizen)**.** Für $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ bezeichne $\mathrm{Nil}_n(\mathbb{K})$ bzw. $\mathrm{Uni}_n(\mathbb{K})$ die Menge der nilpotenten bzw. unipotenten Matrizen in $\mathbb{K}^{n\times n}$. Nach Definition gilt also $X \in \mathrm{Nil}_n(\mathbb{K})$ genau dann, wenn $\mathbf{1} + X \in \mathrm{Uni}_n(\mathbb{K})$.

Ist $X \in \mathrm{Nil}_n(\mathbb{K})$, so ist $X^n = 0$ und daher

$$\exp(X) = \mathbf{1} + X + \frac{1}{2}X^2 + \cdots + \frac{1}{(n-1)!}X^{n-1}.$$

Die Matrizen $X, \frac{1}{2}X^2, \ldots, \frac{1}{(n-1)!}X^{n-1}$ sind allesamt nilpotent und vertauschen miteinander, weswegen auch ihre Summe nilpotent ist. Folglich ist $\exp(X)$ unipotent und wir erhalten eine wohldefinierte Abbildung

$$\exp_n : \mathrm{Nil}_n(\mathbb{K}) \to \mathrm{Uni}_n(\mathbb{K}), \quad \exp_n(X) := \exp(X) = \mathbf{1} + X + \frac{1}{2}X^2 + \cdots + \frac{1}{n-1}X^{n-1}.$$

Korollar 11.3.12. *Die Abbildung* $\exp_n : \mathrm{Nil}_n(\mathbb{K}) \to \mathrm{Uni}_n(\mathbb{K})$ *ist bijektiv.*

Beweis. Wir behaupten, dass die Umkehrabbildung gegeben ist durch

$$\log_n : \mathrm{Uni}_n(\mathbb{K}) \to \mathrm{Nil}_n(\mathbb{K}), \quad \log_n(B) := \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(B-\mathbf{1})^k}{k} = \sum_{k=1}^{n-1} (-1)^{k+1} \frac{(B-\mathbf{1})^k}{k}.$$

Dass $\log_n$ wohldefiniert ist, folgt daraus, dass die Matrizen $(B-\mathbf{1})^k$ allesamt nilpotent sind und miteinander vertauschen. Es bleibt zu zeigen, dass die Polynomfunktionen $F := \exp_n \circ \log_n$ und $G := \log_n \circ \exp_n$ durch die Identität gegeben sind.

Sei zunächst $X \in \mathrm{Nil}_n(\mathbb{K})$. Für hinreichend kleine $t \in \mathbb{R}$ ist $tX \in B_{\log(2)}(0)$ und daher $\exp(X) \in B_1(1)$. Wegen Korollar **??** gilt dann

$$G(tX) = \log_n \circ \exp_n(tX) = \log_n(\exp(tX)) = \log(\exp(tX)) = tX.$$

Aber $t \mapsto G(tX)$ ist eine Polynomfunktion! Gilt daher $G(tX) = tX$ für kleine $t \in \mathbb{R}$, so gilt $G(tX) = tX$ für alle $t \in \mathbb{R}$, insbesondere $G(X) = X$. Analog zeigt man $F(\mathbf{1}+X) = \mathbf{1}+X$, indem man zunächst $\mathbf{1}+X$ durch $\mathbf{1}+tX$ ersetzt. □

Übung 11.3.13. Folgern Sie aus Korollar 11.3.12 und der Jordan–Chevalley-Zerlegung, dass die Exponentialfunktion $\exp : \mathbb{C}^{n\times n} \to \mathrm{GL}_n(\mathbb{C})$ surjektiv ist.

Zusammenfassung von Abschnitt 11.3.

(1) Die Matrizenexponentialfunktion ist in einer Umgebung von 0 ein lokaler Diffeomorphismus, d.h. bijektiv mit differenzierbare Umkehrfunktion.

(2) Eine lokale Umkehrfunktion ist durch den Matrizenlogarithmus gegeben. Dies folgt aus dem Identitätssatz für Potenzreihen.

(3) Die Exponentialfunktion definiert eine globale Bijektion zwischen nilpotenten und unipotenten Matrizen.

Ende des klaussurrelevanten Teils der Vorlesung

11.4 Ausblick: Lie-Algebren

Wir haben gesehen, dass die Matrizenexponentialfunktion

$$\exp : \mathbb{K}^{n\times n} \to \mathrm{GL}_n(\mathbb{K})$$

für $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ ein lokaler Diffeomorpismus ist, der Geraden in Einparametergruppen übersetzt. Im Laufe der Vorlesung haben wir eine ganze Reihe von Untergruppen von $\mathrm{GL}_n(\mathbb{K})$ kennengelernt, z.B. die Gruppe der invertierbaren Diagonalmatrizen, die Gruppe der invertierbaren oberen Dreiecksmatrizen oder die klassischen Gruppen (d.h. die allgemeinen oder speziellen orthogonalen, unitären und symplektischen Gruppen). Alle diese Gruppen können als Nullstellenmengen von Polynomen in den Matrixeinträgen beschrieben werden, sind also affin-algebraische Mengen in $\mathbb{R}^{n\times n}$.

Definition 11.4.1. Ist $G < \mathrm{GL}_n(\mathbb{R})$ eine Untergruppe und zugleich eine affin-algebraische Menge in $\mathbb{R}^{n\times n}$, so heißt G eine *lineare algebraische Gruppe*.

Da jede Untergruppe einer linear algebraischen Gruppe $G < \mathrm{GL}_n(\mathbb{R})$ auch eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$ ist, folgt aus Satz 11.2.7:

Korollar 11.4.2. *Es sei $G < \mathrm{GL}_n(\mathbb{R})$ eine lineare algebraische Gruppe und*

$$\mathfrak{g} := \{X \in \mathbb{R}^{n\times n} \mid \forall\, t \in \mathbb{R} :\ \exp(tX) \in G\}.$$

Dann gilt $\exp[\mathfrak{g}] \subseteq G$. Weiter induziert $\exp : \mathfrak{g} \to G$ eine Bijektion zwischen Geraden in $\mathfrak{g}$ und Einparameteruntergruppen in G. □

Es gilt der folgende tiefliegende Satz:

Satz 11.4.3. *Für jede lineare algebraische Gruppe $G < \mathrm{GL}_n(\mathbb{R})$ existiert eine Umgebung U der 0 in $\mathfrak{g}$ mit den folgenden Eigenschaften:*

(i) $V := \exp[U]$ ist eine offene Teilmenge von G.

(ii) Die Abbildung $\exp|_U^V : U \to V$ ist stetig und bijektiv mit stetiger Umkehrabbildung (d.h. ein „Homöomorphismus“).

Der Norweger Sophus Lie[5] war der erste, der eine Version von Satz 11.4.3 bewiesen hat. Ihm zu Ehren definiert man:

Definition 11.4.4. Die Menge $\mathfrak{g}$ heißt die *Lie-Algebra* der linearen algebraischen Gruppe G.

Beispiel 11.4.5. Es sei $G := \mathrm{SL}_n(\mathbb{R})$. Für Matrizen $A \in \mathbb{R}^{n\times n}$ in Jordannormalform gilt offensichtlich $\det(\exp(tA)) = e^{t\cdot\mathrm{tr}(A)}$, und da beide Seiten sich unter Basiswechsel nicht ändern, gilt dies auch ganz allgemein. Folglich ist die Lie-Algebra von G gegeben durch

$$\mathfrak{g} = \mathfrak{sl}_n(\mathbb{R}) = \{X \in \mathbb{R}^{n\times n} \mid \mathrm{tr}(X) = 0\}.$$

Man beachte, dass $\mathfrak{g}$ ein Vektorraum ist; folglich sieht die Gruppe $\mathrm{SL}_n(\mathbb{R})$ lokal so aus wie ein Vektorraum!

[5] SOPHUS LIE (1842-1899), norw. Mathematiker

Bemerkung 11.4.6. Auch wenn wie $\mathfrak{g}$ eine Lie-„Algebra“ nennen, so ist $\mathfrak{g}$ keineswegs eine Unteralgebra von $\mathbb{R}^{n\times n}$ - das Produkt von zwei Matrizen mit Spur 0 muss ja nicht Spur 0 haben! Hingegen gilt für alle Matrizen A,B (mit oder ohne Spur 0), dass

$$\operatorname{tr}(AB) = \operatorname{tr}(BA) \implies [A,B] := AB - BA \in \mathfrak{sl}_n(\mathbb{R}).$$

Das ist kein Zufall!

Satz 11.4.7 (Trotter-Cohn)**.** *Für Matrizen $A,B \in \mathbb{C}^{n\times n}$ gelten die folgenden Formeln:*

(i) $\exp(t(A+B)) = \lim_{n\to\infty}(\exp(tA/n)\exp(tB/n))^n$.

(ii) $\exp(t[A,B]) = \lim_{n\to\infty}(\exp(\sqrt{t/n}A)\exp(\sqrt{t/n}B)\exp(-\sqrt{t/n}A)\exp(-\sqrt{t/n}B))$.

Korollar 11.4.8. *Ist $\mathfrak{g}$ die Lie-Algebra einer linearen algebraischen Gruppe G, so ist $\mathfrak{g}$ ein $\mathbb{R}$-Vektorraum, und der Kommutator definiert eine bilineare Abbildung*

$$\mathfrak{g}\times\mathfrak{g} \to \mathfrak{g}, \quad (A,B) \mapsto [A,B] = AB - BA.$$

Insbesondere ist G lokal euklidisch, d.h. lokal homöomorph zu einem Vektorraum.

Bemerkung 11.4.9. Der Kommutator definiert eine bilineare Operation auf $\mathfrak{g}$, aber diese Operation ist *nicht* assoziativ. Stattdessen ist diese Operation schief-symmetrisch und es gilt die *Jacobi-Identität*

$$[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0.$$

Umgekehrt kann man zeigen, dass jeder $\mathbb{R}$-Vektorraum mit einer solchen Operation die Lie-Algebra einer linearen algebraischen Gruppe ist (*Satz von Ado*). Dies führt auf eine abstrakte algebraische Theorie von Lie-Algebren.

Beispiel 11.4.10 (Die Lie-Algebren der orthogonalen Gruppen)**.** Was ist die Lie-Algebra $\mathfrak{o}_n(\mathbb{R})$ von $\mathrm{O}_n(\mathbb{R})$? Nach Definition ist $g \in O_n(\mathbb{R})$ genau dann, wenn $g^\top g = \mathbf{1}$. Für $X \in \mathbb{R}^{n\times n}$ gilt also

$$X \in \mathfrak{o}_n(\mathbb{R}) \implies \forall\, t\in\mathbb{R}\colon \exp(tX)\exp(tX^\top) = \mathbf{1} \implies \left.\frac{d}{dt}\right|_{t=0} \exp(tX)\exp(tX^\top) = 0$$

Mit der Produktregel folgt, dass $X^\top + X = 0$, d.h X ist *schiefsymmetrisch*. Ist umgekehrt X schiefsymmetrisch, so gilt für alle $t\in\mathbb{R}$, dass

$$\exp(tX)\exp(tX)^\top = \exp(tX)\exp(tX^\top) = \exp(tX)\exp(-tX) = \mathbf{1}.$$

Folglich ist

$$\mathfrak{o}_n(\mathbb{R}) = \{X \in \mathbb{R}^{n\times n} \mid X = -X^\top\}$$

die Lie-Algebra der schiefsymmetrischen Matrizen.

Übung 11.4.11. Berechnen Sie analog durch „Ableiten und Einsetzen“ die Lie-Algebren aller klassischer Gruppen, sowie die Lie-Algebra der oberen Dreiecksmatrizen und Diagonalmatrizen.

Bemerkung 11.4.12 (Polarzerlegung der klassischen Gruppen)**.** In den Übungen haben Sie gesehen: Ist $G < \mathrm{GL}_n(\mathbb{R})$ eine reduktive (d.h. transpositionsinvariante) lineare algebraische Gruppe und definieren wir

$$K := G \cap \mathrm{O}_n(\mathbb{R}) \quad \text{und} \quad \mathfrak{p} := \{X \in \mathfrak{g} \mid X = X^\top\},$$

so ist die Abbildung

$$K \times \mathfrak{p} \to G, \quad (k, X) \mapsto k \exp(X)$$

eine Bijektion. Folglich ist jede reduktive lineare algebraische Gruppe (insbesondere jede klassische Gruppe) in geeigneten Koordinaten das Produkt einer kompakten Gruppe K mit einem Vektorraum $\mathfrak{p}$, und zwar global und nicht nur lokal.

Wenn Sie möchten, geht es an dieser Stelle im nächsten Semester in der Vorlesung „Lie-Algebren (Lineare Algebra 3)“ weiter.