Lineare Algebra und Geometrie I und II
Wintersemester 2000/2001
und Sommersemester 2001

Erwin Bolthausen

28. September 2001

Inhaltsverzeichnis

1 Mengen, Abbildungen, Relationen

1.1 Grundlegende Mengenbegriffe

Eine **Menge** ist eine beliebige Kollektion von Objekten, wie z.B. Zahlen, geometrischen Objekten, etc., den **Elementen** der Menge.

Notation 1.1
- $a \in M$ *bedeutet: a ist Element der Menge M.*
- $a \notin M$ *bedeutet: a ist* ***nicht*** *Element der Menge M.*

Es gibt verschiedenen Möglichkeiten, Mengen darzustellen; die einfachste ist, die Elemente der Menge einfach aufzulisten. Man schreibt diese Elemente üblicherweise dann in geschweifte Klammern:

$$M = \{1, 4, 7, 9\}\,. \tag{1.1}$$

Diese Menge enthält 4 Elemente, nämlich die Elemente $1, 4, 7$ und 9. Die Anzahl der Elemente einer Menge nennt man die **Kardinalität** der Menge. Die durch (1.1) gegebene Menge hat also die Kardinalität 4. Schwierig wird diese Darstellungsweise dann, wenn die Menge sehr viele oder gar unendlich viele Elemente enthält. Man behilft sich dann oft mit "Pünktchen". Z.B. ist die Menge

$$M = \{1, 3, 5, 7, 9, \ldots\}$$

einfach die Menge der ungeraden natürlichen Zahlen. Diese Menge enthält natürlich unendlich viele Elemente. Man sagt dann auch, die Kardinalität sei ∞.

Es ist üblich, Mengen mit grossen lateinischen Buchstaben wie A, B oder M zu bezeichnen, und die Elemente mit kleinen. Dies kann jedoch nicht streng durchgehalten werden, denn oft sind die Elemente einer Menge auch selbst wieder Mengen. Wir werden uns nach Möglichkeit an diese Konvention halten; es wird jedoch auch viele Ausnahmen geben.

Nachfolgend ist eine Auflistung der für uns wichtigsten Mengen von Zahlen. Es ist hier üblich, diese mit grossen lateinischen Buchstaben mit "Doppelstrichen" zu bezeichnen. Die entsprechenden Bezeichnungen sind ein für allemal für diese speziellen Mengen reserviert.

- $\mathbb{N}$ ist die Menge der **natürlichen Zahlen,** d.h.

  $$\mathbb{N} := \{1, 2, 3, 4, \ldots\}\,.$$

  Mit $\mathbb{N}_0$ bezeichnen wir die Menge der natürlichen Zahlen inklusive der Null: $\mathbb{N}_0 := \{0, 1, 2, 3, 4, \ldots\}\,.$

- $\mathbb{Z}$ ist die Menge der **ganzen Zahlen,** d.h.

  $$\mathbb{Z} := \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\}\,.$$

- $\mathbb{Q}$ ist die Menge der **rationalen Zahlen,** d.h. der Zahlen, die sich als Brüche von ganzen Zahlen (mit Nenner $\neq 0$) darstellen lassen. Also z.B. sind 3/4, 234/1875 rationale Zahlen, in unserer Sprechweise also Elemente von $\mathbb{Q}$.

- $\mathbb{R}$ ist die Menge der **reellen Zahlen**. Es macht schon sehr viel grössere Schwierigkeiten, genau zu beschreiben, wie diese Menge definiert ist. In der Vorlesung Differential- und Integralrechnung I (im folgenden kurz DI) wird dies genauer durchgeführt. Aus der Schule am besten bekannt ist wahrscheinlich die Beschreibung der reellen Zahlen als unendlich lange Dezimalbrüche.

- $\mathbb{C}$ ist die Menge der **komplexen Zahlen**. Die komplexen Zahlen werden ebenfalls in DI eingeführt. Wichtige Eigenschaften werden auch in dieser Vorlesung später vorgestellt werden.

Statt durch eine Aufzählung beschreibt man Mengen auch oft einfach durch die Angabe der Eigenschaften ihrer Elemente. Hier ein Beispiel:

$$M = \{x : x \in \mathbb{N},\, x \,\text{ist durch}\, 5 \,\text{teilbar}\}\,.$$

Dies bedarf einiger Erläuterungen. Die Menge M besteht hier aus denjenigen Elementen x, deren Eigenschaften hinter dem Doppelpunkt aufgezählt sind. Hier sind es zwei Eigenschaften: x muss eine natürliche Zahl sein und x ist durch 5 teilbar.

Eine aufzählende Beschreibung für diese Menge ist einfach

$$M = \{5, 10, 15, 20, \ldots\}\,.$$

Ein anderes Beispiel:

$$A = \left\{x : x \in \mathbb{R},\, x^2 = 1\right\}.$$

Das ist natürlich einfach die zweielementige Menge $\{-1, 1\}$.

Nun zu weiteren Definitionen über Mengen. Zwei Mengen A und B heissen **gleich**, wenn sie dieselben Elemente enthalten. Wir benützen die Gelegenheit, eine "stenographische" Kurzschreibweise solcher Aussagen einzuführen:

$$A = B \Leftrightarrow \forall x\ (x \in A \Leftrightarrow x \in B)\,. \tag{1.3}$$

Die Notationen sind vielleicht schon aus der Schule bekannt. $\forall$ ist einfach ein Kürzel für "für alle". $\forall x$ bedeutet einfach "für alle x gilt:". Der Doppelpfeil $\Leftrightarrow$ ist sicher aus der Schule bekannt. Es ist einfach eine Abkürzung für "gilt dann und nur dann wenn" oder "gilt genau dann wenn". Das Kryptogramm (1.3) besagt also einfach: A und B sind genau dann gleich, wenn für alle x gilt: x ist Element von A genau dann, wenn es Element von B ist. Etwas weniger

umständlich ausgedrückt: A und B sind genau dann gleich, wenn sie dieselben Elemente enthalten.

Eine bestimmte Menge spielt eine besondere Rolle, die sogenannte **leere Menge $\emptyset$**. Sie ist definiert als die Menge, die keine Elemente enthält. Es gibt offenbar nur eine leere Menge, denn zwei Mengen sind gleich, wenn sie dieselben Elemente enthalten. Da leere Mengen gar keine Elemente enthalten, sind offenbar zwei leere Mengen gleich, d.h. es gibt nur eine leere Menge.

A ist eine **Teilmenge** von B, wenn jedes Element von A auch Element von B ist. Man schreibt dann $A \subset B$. Wieder "stenographisch":

$$A \subset B \Leftrightarrow \forall x \; (x \in A \Rightarrow x \in B) \, .$$

Hier verwenden wir den einfachen Implikationspfeil $\Rightarrow$, der sicher auch aus der Schule bekannt ist. Natürlich ist B immer eine Teilmenge von B. Ferner ist die leere Menge $\emptyset$ eine Teilmenge jeder Menge. Man beachte, dass zwei Mengen A und B genau dann gleich sind, wenn $A \subset B$ und $B \subset A$ gelten. Mancherorts wird für die Teilmengenbeziehung auch noch die Schreibweise $\subseteq$ verwendet, die explizit andeutet, dass die Mengen auch gleich sein können. Wir werden diese Notation jedoch nicht verwenden.

Teilmengen einer Menge werden auch sehr oft durch Eigenschaften beschrieben. Ist M eine Menge und $\mathcal{E}$ eine Eigenschaft, so ist

$$A = \{x \in M : x \, \text{hat Eigenschaft} \, \mathcal{E}\}$$

einfach die Menge derjenigen Elemente von M, die die Eigenschaft $\mathcal{E}$ besitzen. Die Menge $\{-1, 1\}$ liesse sich dann auch durch

$$A = \left\{x \in \mathbb{R} : x^2 = 1\right\}$$

beschreiben.

Aus der Schule sind wahrscheinlich **Durchschnitt, Vereinigung und Komplement** bekannt: Es seien A und B zwei Mengen. Dann sind diese neuen Mengen wie folgt definiert:

$$\begin{aligned} A \cap B &:= \{x : x \in A \, \text{und} \, x \in B\} \, , \\ A \cup B &:= \{x : x \in A \, \text{oder} \, x \in B\} \, , \\ A \backslash B &:= \{x : x \in A \, \text{und} \, x \notin B\} \, . \end{aligned}$$

Wir werden oft Teilmengen einer festen Menge, nennen wir sie M, betrachten, die dann für eine längere Betrachtung nicht mehr wechselt. Dann schreibt man einfach A^c für $M \backslash A$. Das ist das Komplement von A in M. Natürlich müsste man eigentlich M in der Notation mit ausdrücken. Das wird jedoch stets aus dem Kontext ersichtlich sein. Für die obigen Mengenoperationen gelten einige Rechenregeln, die wir hier als bekannt voraussetzen, z.B.

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \, , \\ (A \cup B)^c &= A^c \cap B^c . \end{aligned} \tag{1.4}$$

Den Beweis, dass zwei Mengen, nennen wir sie F und G, gleich sind, führt man oft in zwei Schritten. Man zeigt zuerst, dass $F \subset G$ gilt, und dann, dass $G \subset F$ gilt. Wir exemplifizieren das mit einem Beweis von (1.4):

Beweis von (1.4). Sei $x \in A \cap (B \cup C)$. Dann ist x Element von A und von $B \cup C$. Ist $x \in B \cup C$, so ist x in B oder in C. Gilt Ersteres, so ist $x \in A \cap B$ und gilt Letzteres, so gilt $x \in A \cap C$. In jedem Fall folgt dann $x \in (A \cap B) \cup (A \cap C)$. Damit haben wir gezeigt, dass jedes Element von $A \cap (B \cup C)$ auch in $(A \cap B) \cup (A \cap C)$ ist. Damit haben wir nachgewiesen, dass

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C) \tag{1.5}$$

gilt.

Nun kommen wir zum zweiten Teil des Beweises. Sei $x \in (A \cap B) \cup (A \cap C)$. Dann ist $x \in A \cap B$ oder $x \in A \cap C$. x liegt also in A und B, oder in A und C. In jedem Fall liegt also x in A und dann in B oder C. Das bedeutet aber nichts anderes, dass $x \in A \cap (B \cup C)$ gilt. Wir haben also

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C) \tag{1.6}$$

nachgewiesen.

(1.5) und (1.6) implizieren (1.4). ■

Wir betrachten nun die Vereinigung oder den Durchschnitt von mehr als zwei Mengen, unter Umständen von unendlich vielen. In solchen Fällen sind die Mengen dann oft mit Hilfe von Indizes beschrieben: A_i, wobei i eine Indexmenge durchläuft, z.B. die natürlichen Zahlen: Sind $A_1, A_2, A_3, \ldots$ Mengen so schreiben wir $\bigcup_{i=1}^{\infty} A_i$ für die Vereinigung und $\bigcap_{i=1}^{\infty} A_i$ für den Durchschnitt dieser Mengen. Die Indexmenge, aus der i ist, braucht jedoch nicht die Menge der natürlichen Zahlen zu sein, sondern kann eine ganz beliebige Menge I sein (z.B. die Menge der reellen Zahlen). Wir schreiben dann $\bigcup_{i \in I} A_i$ bzw. $\bigcap_{i \in I} A_i$. Es gibt eine formal etwas abstraktere Schreibweise, die manchmal bequem ist. Die Darstellung einer Kollektion von Mengen mit Hilfe eines Indexes ist mathematisch nämlich meist überflüssig. Wir können statt dessen einfach Mengen betrachten, deren Elemente selbst Mengen sind. Ausgehend von der Folge $A_1, A_2, A_3, \ldots$ betrachten wir die Menge $\mathcal{A} \stackrel{\text{def}}{=} \{A_1, A_2, A_3, \ldots\}$. Deren Elemente sind nun gerade die A_i. Wir schreiben dann einfach $\bigcup \mathcal{A}$ für $\bigcup_{i=1}^{\infty} A_i$. Also: Ist $\mathcal{A}$ eine Menge deren Elemente selbst Mengen sind (oft sagt man dann auch eine "Familie von Mengen"), so ist $\bigcup \mathcal{A}$ die Vereinigung dieser Elemente. Entsprechend für den Durchschnitt. Hier noch die ganz formale Definition:

$$\bigcup \mathcal{A} = \{x : \exists A \in \mathcal{A} \,\text{mit}\, x \in A\},$$

wobei wir hier das Symbol $\exists$ verwenden, was einfach eine Abkürzung für "existiert" ist, und

$$\bigcap \mathcal{A} = \{x : x \in A \,\text{für}\, \forall A \in \mathcal{A}\}\,.$$

Wenn Sie im Moment noch etwas Schwierigkeiten mit diesen abstrakten Formulierungen haben, so ist das nicht allzu schlimm; Sie werden sich mit der Zeit daran gewöhnen.

Eine spezielle Familie von Mengen ist die sogenannte **Potenzmenge** einer Menge. Ist A eine Menge, so ist die Potenzmenge $\mathcal{P}(A)$ die Menge aller Teilmengen von A :

$$\mathcal{P}(A) := \{B : B \subset A\}\,.$$

Z.B. hat für $A = \{1, 2\}$ die Potenzmenge die vier Elemente $\emptyset$, $\{1\}$, $\{2\}$, $\{1, 2\}$, also

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

1.2 Abbildungen

A und B seien zwei Mengen. Eine **Abbildung** $f : A \to B$ ist eine Vorschrift, die jedem $x \in A$ genau ein Element $f(x) \in B$ zuordnet. $f(x)$ heisst dann das Bildelement von x.

Wir schreiben auch oft $A \ni x \longrightarrow f(x) \in B$.

Beispiel 1.1 *a) Wir betrachten die Abbildung* $f : \mathbb{R} \to \mathbb{R}$, *die jedem Element* x *sein Quadrat zuordnet.* $f(x) := x^2$.

b) f *sei die Abbildung* $\mathbb{N} \to \mathbb{N}$, *die jeder Zahl das Doppelte zuordnet:* $f(x) := 2x$.

Die beiden Beispiele oben waren sogenannte **Selbstabbildungen**, wo die Zielmenge B die gleiche wie die Ursprungsmenge A ist. Das braucht jedoch nicht so zu sein. Wir werden noch sehr viele Beispiele kennenlernen, wo das anders ist. Eine Selbstabbildung einer Menge A spielt eine besondere Rolle, die **identische Abbildung** $\mathrm{id}_A : A \to A$:

$$\mathrm{id}_A(x) := x$$

für alle $x \in A$.

Wir benötigen noch ein paar weitere Begriffsbildungen.

Definition 1.1 *Eine Abbildung* $f : A \to B$ *heisst* ***surjektiv****, wenn jedes Element von* B *als Bildelement eines Elementes in* A *vorkommt, d.h. für jedes* $y \in B$ *existiert (mindestens) ein* $x \in A$ *mit* $f(x) = y$. *In formaler "Stenographenschreibweise":*

$$f \,\text{surjektiv} \Longleftrightarrow \forall y \in B\, \exists x \in A\ (f(x) = y)\,.$$

Die Abbildung $\mathbb{R} \ni x \to x^2 \in \mathbb{R}$ ist offenbar nicht surjektiv, denn es gibt Elemente von $\mathbb{R}$, die nicht also Bildelemente vorkommen, nämlich die negativen reellen Zahlen. Auch die Abbildung $\mathbb{N} \ni x \to 2x \in \mathbb{N}$ ist nicht surjektiv, denn die ungeraden natürlichen Zahlen kommen nicht als Bildelemente vor.

Definition 1.2 *Eine Abbildung $f : A \to B$ heisst **injektiv,** wenn zwei verschiedene Elemente in A auch auf verschiedene Elemente in B abbgebildet werden: Falls $x, x' \in A$ und $x \neq x'$ gelten, so ist $f(x) \neq f(x')$. Eine Abbildung, die sowohl injektiv wie surjektiv ist, heisst **bijektiv.***

Die Abbildung $\mathbb{N} \ni x \to 2x \in \mathbb{N}$ ist offenbar injektiv, nicht aber $\mathbb{R} \ni x \to x^2 \in \mathbb{R}$, denn unter letzterer werden z.B. -1 und 1 auf dasselbe Element abgebildet.

Definition 1.3 *Sind $f : A \to B$ und $g : B \to C$ zwei Abbildungen, so ist die **Zusammensetzung** oder **Komposition** dieser Abbildungen $g \circ f : A \to C$ wie folgt definiert:*

$$(g \circ f)(x) := g(f(x)).$$

Man beachte, dass diese Komposition nur definiert ist, wenn die Zielmenge B der Abbildung f gleich der Ausgangsmenge der Abbildung g ist.

Bemerkung 1.1 *Die Schreibweise $g \circ f$ für diese Komposition ist leider etwas unglücklich, hat sich jedoch aus historischen Gründen offenbar unverrückbar eingebürgert. Es wird nämlich f zuerst ausgeführt und dann g. Die Schreibweise ergibt sich aus der Schreibweise $f(x)$ für das Bildelement von x unter f. Logischer wäre es an sich, $(x)f$ zu schreiben, denn man "nimmt" x und wendet dann die Abbildung f darauf an. Es hat erfolglose Anläufe gegeben, das in dieser Weise umzustellen.*

Beispiel 1.2 *Wir betrachten die folgenden zwei Funktionen $f, g : \mathbb{R} \to \mathbb{R} : f(x) = x^2$, $g(x) = \mathrm{e}^x$. Dann ist $f \circ g$ die Funktion $\mathbb{R} \ni x \to (\mathrm{e}^x)^2 = \mathrm{e}^{2x}$. Andererseits ist $g \circ f$ die Funktion $\mathbb{R} \ni x \to \mathrm{e}^{x^2}$. Man sieht also schon an diesem Beispiel, dass im Allgemeinen $f \circ g \neq g \circ f$ ist, selbst wenn beide Kompositionen definiert sind.*

Satz 1.1 *Es seien A, B, C Mengen und $f : A \to B$ und $g : B \to C$ seien Abbildungen.*

a) Sind f und g injektiv, so ist auch $g \circ f$ injektiv.

b) Sind f und g surjektiv, so ist auch $g \circ f$ surjektiv.

c) Sind f und g bijektiv, so ist auch $g \circ f$ bijektiv.

Beweis. c) folgt sofort aus a) und b). Wir beweisen nur a). Der Beweis von b) sei dem Leser überlassen.

Es seien a, a' zwei Elemente von A mit $g \circ f(a) = g \circ f(a')$. Nun ist aber per Definition der Komposition $g \circ f(a) = g(f(a))$. Also folgt $g(f(a)) = g(f(a'))$. Wegen der Injektivität von g folgt $f(a) = f(a')$. Aus der Injektivität von f ergibt sich daraus $a = a'$. Dies beweist, dass $g \circ f$ injektiv ist. ■

Von besonderer Bedeutung sind bijektive Abbildungen einer endlichen Menge, etwa $\{1, \ldots, n\}$, auf sich selbst.

Eine bijektive Abbildung $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ heisst **Permutation**. Üblicherweise verwendet man kleine griechische Buchstaben wie σ, τ, π um Permutationen zu bezeichnen. Wir werden die folgende Schreibweise für Permutationen verwenden

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Zum Beispiel ist

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$$

die Permutation σ die 1 nach 2, 2 nach 4, 3 nach 1, 4 nach 5 und 5 nach 3 schickt. Die Reihenfolge der Spalten in der obigen Anordnung spielt dann keine Rolle. So ist

$$\begin{pmatrix} 3 & 5 & 1 & 2 & 4 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

dieselbe Permutation. Die Schreibweise ist auch bequem, um Kompositionen von Permutationen zu berechnen. Wir geben dazu ein Beispiel. Wir nehmen als zweite Permutation

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}.$$

Dann sind

$$\begin{aligned} \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 2 & 4 & 5 & 1 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} \tau \circ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}. \end{aligned}$$

Auch hier sieht man, dass $\sigma \circ \tau \neq \tau \circ \sigma$ ist.

Zum Schluss dieses Abschnitts diskutieren wir noch die **Umkehrabbildungen**. $f : A \to B$ sei eine bijektive Abbildung. Dann gibt es wegen der Surjektivität zu jedem Element $y \in B$ ein Element $x \in A$ mit $f(x) = y$. Wegen der Injektivität gibt es zu jedem y nur *ein* derartiges Element x. Wir erhalten also eine eindeutig definierte Zuordnung $B \ni y \to x \in A$. Diese Zuordnung nennen wir die **Umkehrabbildung** von f und bezeichnen sie mit f^{-1}, also $f^{-1}(y) = x$. Wir formulieren einige Eigenschaften als Satz:

Satz 1.2 *a) Ist $f : A \to B$ bijektiv, so gibt es eine Umkehrabbildung f^{-1}, die eindeutig definiert ist durch die Festsetzung*

$$f(x) = y \Longleftrightarrow f^{-1}(y) = x. \tag{1.7}$$

b) f^{-1} erfüllt die beiden Gleichungen

$$\begin{aligned} f \circ f^{-1} &= \mathrm{id}_B, \\ f^{-1} \circ f &= \mathrm{id}_A. \end{aligned} \tag{1.8}$$

c) Ist $f : A \to B$ eine Abbildung und existiert eine Abbildung $g : B \to A$ mit

$$f \circ g = \mathrm{id}_B, \tag{1.9}$$

$$g \circ f = \mathrm{id}_A, \tag{1.10}$$

so ist f bijektiv und g ist die Umkehrabbildung von f.

Beweis. a) hatten wir uns schon vor der Formulierung des Satzes überlegt. (1.8) folgt sofort aus (1.7). Wir müssen uns nur den Teil c) noch überlegen.

Wir gehen also hier davon aus, dass f nur eine Abbildung ist (keine Voraussetzungen an Injektivität und Surjektivität), fordern aber die Existenz einer Abbildung g mit den angegebenen Eigenschaften. Wir zeigen zunächst, dass f dann surjektiv ist. Dazu betrachten wir ein beliebiges Element $y \in B$. Dies können wir mit g nach A abbilden. Wir setzen $x := g(y)$. Nach (1.9) ist

$$f(x) = f(g(y)) = (f \circ g)(y) = \mathrm{id}_B(y) = y.$$

Wir haben damit nachgewiesen, dass zu jedem $y \in B$ ein $x \in A$ existiert mit $f(x) = y$. Damit ist die Surjektivität bewiesen.

Wir kommen nun zur Injektivität. Es seien x und x' zwei Elemente von A mit $f(x) = f(x')$. Nennen wir dieses Element y : $y := f(x) = f(x')$. Wir wenden nun (1.10) an:

$$\begin{aligned} x &= \mathrm{id}_A(x) = (g \circ f)(x) = g(f(x)) = g(y) \\ &= g(f(x')) = (g \circ f)(x') = \mathrm{id}_A(x') = x'. \end{aligned}$$

Damit ist bewiesen, dass aus $f(x) = f(x')$ die Gleichung $x = x'$ folgt. Es ist damit gezeigt, dass f injektiv ist. Zusammen mit der schon gezeigten Surjektivität ist somit bewiesen, dass f bijektiv ist.

Wir müssen nun noch nachweisen, dass g tatsächlich die Umkehrabbildung ist. Dies ist aber nun einfach: Ist $y = f(x)$, so ist $g(y) = g(f(x)) = (g \circ f)(x) = \mathrm{id}_A(x) = x$. Das ist genau die geforderte Beziehung (1.7) für die inverse Abbildung. ■

Bemerkung 1.2 *Aus dem obigen Satz folgt sofort, dass die Umkehrabbildung f^{-1}einer bijektiven Abbildung f wieder bijektiv ist und $(f^{-1})^{-1} = f$ gilt.*

1.3 Relationen, Äquivalenzrelationen

Sind A, B zwei Mengen, so ist die sogenannte **Produktmenge $\boldsymbol{A \times B}$** die Menge der geordneten Paare (a, b) von Elementen $a \in A$ und $b \in B$. Für Mengen $A_1, A_2, \ldots, A_n$ ist die Produktmenge $A_1 \times A_2 \times \ldots \times A_n$ definiert als die Menge der sogenannten geordneten **n-Tupel** $(a_1, a_2, \ldots, a_n)$ von Elementen $a_i \in A_i$, $1 \leq i \leq n$. Es soll hier keine formal ganz präzise Definition dieser Menge gegeben werden — dies würde eine Axiomatisierung der Mengenlehre voraussetzen, die wir hier nicht einführen möchten. Das Wort "geordnet" bedeutet, dass auf die Reihenfolge geachtet wird: Sind $a \neq b$, so gilt $(a, b) \neq (b, a)$ und analog für die n-Tupel.

Sind A und B dieselben Mengen, so schreiben wir auch einfach A^2 anstelle von $A \times A$, und analog A^n für die Menge der n-Tupel.

Eine **Relation** R auf einer Menge A ist formal einfach eine Teilmenge $R \subset A \times A$. Für $a, b \in A$ schreiben wir dann auch aRb anstelle von $(a, b) \in R$. Das ist im Moment etwas abstrakt. Wir machen gleich einige Beispiele dazu.

Beispiel 1.3 *Sie kennen auf $\mathbb{R}$ die übliche Ordnungsrelation $a \leq b$. Wir können diese Ordnungsrelation auch einfach als Teilmenge von $\mathbb{R} \times \mathbb{R}$ auffassen. Die Elemente dieser Teilmenge sind die Elemente (a, b), für die $a \leq b$ gilt.*

Beispiel 1.4 *Betrachten Sie die Menge G der Geraden im dreidimensionalen Raum. Wir können die Relation R der "Parallelität" definieren: Zwei Geraden g_1 und g_2 stehen in dieser Relation, wenn sie parallel sind. Formaler ausgedrückt: $(g_1, g_2) \in R \Longleftrightarrow g_1$ und g_2 sind parallel.*

Definition 1.4 *R sei eine Relation auf A.*

*a) R heisst **symmetrisch**, wenn*

$$(a, b) \in R \Longleftrightarrow (b, a) \in R$$

gilt.

*b) R heisst **transitiv,** wenn*

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

gilt.

*c) R heisst **reflexiv**, wenn $(a,a) \in R$ für alle $a \in A$ gilt.*

Beispiel 1.5 *Die zweiteinfachste Relation auf A ist die "Gleichheit": $(a,b) \in R$ gilt genau dann, wenn $a = b$ ist. Offensichtlich ist diese Relation symmetrisch, transitiv und reflexiv. Noch trivialer ist $R = A \times A$. In diesem Fall stehen zwei beliebige Elemente von A in der Relation R.*

Beispiel 1.6 *Etwas weniger trivial ist das Beispiel 1.3 von oben. Die Ordnungsrelation $\leq$ auf $\mathbb{R}$ ist transitiv, denn aus $a \leq b$, $b \leq c$ folgt $a \leq c$, und reflexiv. Sie ist aber nicht symmetrisch, denn es gilt zwar $1 \leq 2$, aber nicht $2 \leq 1$.*

Definition 1.5 *a) Eine reflexive und transitive Relation R auf einer Menge A heisst eine **Ordnungsrelation** auf A, wenn zusätzlich die folgende Eigenschaft gilt:*

$$(a,b) \in R \,\text{und}\, (b,a) \in R \Longrightarrow a = b.$$

*b) Eine Ordnungsrelation heisst **Totalordnung,** wenn je zwei beliebige Elemente von A vergleichbar sind, d.h. wenn für beliebige Elemente $a, b \in A$ $(a,b) \in R$ oder $(b,a) \in R$ ist.*

*c) Eine reflexive, symmetrische und transitive Relation auf A heisst eine **Äquivalenzrelation.***

Üblicherweise schreibt man Ordnungsrelationen als $\leq$ oder $\prec$ oder ähnlich. Man schreibt dann auch $a \leq b$ anstelle von $(a,b) \in \leq$. Äquivalenzrelationen schreibt man üblicherweise als $\sim$, also $a \sim b$ für zwei Elemente, die in dieser Relation stehen.

Es gibt viele Beispiele von Ordnungsrelationen, die keine Totalordnungen sind. Die Gleichheitsrelation ist natürlich immer auch eine Ordnungsrelation. Es ist jedoch keine Totalordnung, ausser wenn A nur ein Element enthält. Hier noch ein weniger triviales Beispiel. Wir betrachten $A = \mathbb{R}^2$, die Menge der reellen Paare. Dann definieren wir $(a_1, a_2) \prec (b_1, b_2)$ wenn $a_2 = b_2$ und $a_1 \leq b_1$ gelten. $\prec$ ist eine Ordnungsrelation aber keine Totalordnung, denn z.B. $(1,2)$ und $(3,4)$ sind nicht vergleichbar.

Ein anderes Beispiel, das Sie schon kennen, tritt in folgender Situation auf. Wir betrachten eine beliebige Menge M. $\mathcal{P}(M)$ sei die **Potenzmenge** von M, d.h. die Menge aller Teilmengen von M. Ein Element von $\mathcal{P}(M)$ ist also nichts anderes als eine Teilmenge von M. Auf $\mathcal{P}(M)$ betrachten wir die übliche Inklusionsrelation: Zwei Elemente $B, C \in \mathcal{P}(M)$ (d.h. zwei Teilmengen von M) stehen in der Relation $\subset$, wenn B eine Teilmenge von C ist, also $B \subset C$ im üblichen

Sinn. $\subset$ ist ebenfalls eine Ordnungsrelation, aber keine Totalordnung (falls M mehr als ein Element enthält).

Soviel im Moment zu Ordnungsrelationen, die uns noch sehr oft begegnen werden.

Nun zu den Äquivalenzrelationen. Ein Beispiel ist wieder die Gleichheitsrelation. Die Ordnungsrelation $\leq$ auf $\mathbb{R}$ ist jedoch keine Äquivalenzrelation, denn sie ist nicht symmetrisch. Noch ein anderes Beispiel. Wir betrachten die Menge aller Geraden in einer Ebene. Wir definieren für zwei Geraden g_1 und $g_2 : g_1 \sim g_2$ wenn g_1 und g_2 parallel sind. Dies ist offensichtlich eine Äquivalenzrelation.

Äquivalenzrelationen stehen in engster Beziehung zu sogenannten Zerlegungen. Eine Zerlegung einer Menge A ist eine Aufteilung der Menge in nicht leere Teilmengen von A, die sich gegenseitig "nicht überlappen". Hier eine ganz formale Definition:

Definition 1.6 *A sei eine nicht leere Menge. Eine **Zerlegung** $\mathcal{Z}$ von A ist eine Familie von Teilmengen $C_i \subset A$ mit*
a) $\bigcup_i C_i = A$.
b) $C_i \neq \emptyset$ für alle i.
c) $C_i \cap C_j = \emptyset$ für $i \neq j$.

Zwei Mengen mit der Eigenschaft c) ("nicht überlappend", "haben leeren Schnitt") heissen übrigens **disjunkt**. Der Index i in der obigen Definition durchläuft irgendeine "Indexmenge" I, die endlich oder unendlich sein kann. Ein triviales Beispiel ist die "Zerlegung" in eine einzige Teilmenge, die dann natürlich A selbst sein muss. In diesem Fall gibt es nur ein C_1. Nach dem üblichen Sprachverständnis wäre das natürlich keine Zerlegung; die obigen Bedingungen sind jedoch erfüllt, auch c), denn da es gar keine zwei verschiedenen Indizes i, j gibt, ist das automatisch richtig. ("Alle vieräugigen, wiederkäuenden Amerikaner besitzen einen roten Ferrari" ist eine mathematisch korrekte Aussage).

Die Formulierung der Definition mit indizierten Mengen ist eigentlich überflüssig. Formal "schöner" ist die Definition von $\mathcal{Z}$ als Teilmenge der Potenzmenge $\mathcal{P}(A)$ mit den entsprechend formulierten Aussagen a)-c). Diese lauten dann

a) $\bigcup \mathcal{Z} = A$.

b) $C \neq \emptyset$ für alle $C \in \mathcal{Z}$.

c) $C \cap D = \emptyset$ für $C \neq D$, $C, D \in \mathcal{Z}$.

Zur Erinnerung $\bigcup \mathcal{Z} = \{x \in A : \exists C \in \mathcal{Z} \,\text{mit}\, x \in \mathcal{Z}\}$. Das ist vielleicht im Moment etwas abstrakt.

Hier ein Beispiel einer Zerlegung: Wir zerlegen $\mathbb{N}$ in die unendlich vielen Teilmengen: $\{1\}, \{2,3\}$,$\{4,5,6\}, \{7,8,9,10\}$, etc. Die Zerlegung ist dann

$$\mathcal{Z} = \{\{1\}, \{2,3\}, \{4,5,6\}, \{7,8,9,10\}, \ldots\}.$$

Es stellt sich nun heraus, dass Äquivalenzrelationen eigentlich nichts anderes als Zerlegungen sind. Zunächst ist es sehr einfach, einer Zerlegung $\mathcal{Z}$ von A eine Äquivalenzrelation auf A zuzuordnen. Wir bezeichnen diese mit $\sim_{\mathcal{Z}}$: Für Elemente $a, b \in A$ definieren wir $a \sim_{\mathcal{Z}} b$, wenn a und b in derselben Menge der Zerlegung sind:

$$a \sim_{\mathcal{Z}} b \Longleftrightarrow \exists C \in \mathcal{Z} \,\text{mit}\, a, b \in C.$$

Lemma 1.1 *Ist $\mathcal{Z}$ eine Zerlegung, so ist $\sim_{\mathcal{Z}}$ eine Äquivalenzrelation.*

Beweis. Zunächst die Reflexivität: Da $\mathcal{Z}$ eine Zerlegung ist, existiert zu jedem $a \in A$ eine Menge C der Zerlegung mit $a \in C$. Demzufolge gilt $a \sim_{\mathcal{Z}} a$.

Die Symmetrie von $\sim_{\mathcal{Z}}$ ist klar aus der Definition.

Nun zur Transitivität. Seien $a \sim_{\mathcal{Z}} b$, $b \sim_{\mathcal{Z}} c$. So wie die Relation definiert ist, existieren $C \in \mathcal{Z}$ mit $a, b \in C$ und $C' \in \mathcal{Z}$ mit $b, c \in C'$. Das Element b liegt also in C und C'. Demzufolge ist $C \cap C' \neq \emptyset$. Aus der Eigenschaft c) einer Zerlegung folgt also $C = C'$. Daraus folgt $a \sim_{\mathcal{Z}} c$. ■

Wir gehen nun umgekehrt vor und konstruieren zu einer beliebigen Äquivalenzrelation $\sim$ auf A eine Zerlegung. Dies geht über die sogenannten **Äquivalenzklassen.** Ist $a \in A$, so definieren wir die Äquivalenzklasse $[a] \subset A$ von a (bezüglich der Äquivalenzrelation $\sim$) durch

$$[a] := \{b \in A : b \sim a\}.$$

Die Äquivalenzklassen sind also Teilmengen von A.

Lemma 1.2 *Sei A eine nichtleere Menge und $\sim$ eine Äquivalenzrelation. Dann ist*

$$\mathcal{Z}_{\sim} := \{[a] : a \in A\}$$

eine Zerlegung von A.

Beweis. Wir müssen die Eigenschaften a)-c) nachprüfen. Zunächst ist wegen der Reflexivität der Äquivalenzrelation $a \in [a]$ für alle $a \in A$. Demzufolge sind die Äquivalenzklassen alle nicht leer, was b) ist, und weiter folgt sofort, dass die Vereinigung aller Äquivalenzklassen gleich A ist, was a) beweist. Es verbleibt der Beweis von c):

Es sei $[a] \cap [b] \neq \emptyset$. Dann exisiert ein Element c in diesem Durchschnitt. Per Definition gelten dann $c \sim a$ und $c \sim b$. Wegen der Symmetrie von $\sim$ folgt auch $a \sim c$. Zusammen mit $c \sim b$ und der Transitivität impliziert das also $a \sim b$. Wir haben also gezeigt:

$$[a] \cap [b] \neq \emptyset \Longrightarrow a \sim b.$$

Wir müssen nun noch zeigen, dass zwei äquivalente Elemente dieselbe Äquivalenzklasse haben. Sie x ein beliebiges Element $\in [a]$, d.h. $x \sim a$. Zusammen

mit $a \sim b$ und wieder der Transitivität folgt $x \sim b$, d.h. $x \in [b]$. Damit ist gezeigt, dass $[a] \subset [b]$. Auf die genau gleiche Art erhalten wir auch $[b] \subset [a]$ und demzufolge $[a] = [b]$. Wir haben also gezeigt:

$$a \sim b \Longrightarrow [a] = [b] .$$

Zusammen mit der vorherigen Implikation ergibt sich

$$[a] \cap [b] \neq \emptyset \Longrightarrow [a] = [b] .$$

Dies ist genau die geforderte Eigenschaft c) für eine Zerlegung. ■

Zusammenfassend ergibt sich aus den beiden obigen Lemmata:

Satz 1.3 *Sei A eine nichtleere Menge. Äquivalenzrelationen auf A und Zerlegungen von A entsprechen sich: Jeder Äquivalenzrelation $\sim$ wird mit $\mathcal{Z}_\sim$ eine Zerlegung zugeordnet und jeder Zerlegung $\mathcal{Z}$ wird mit $\sim_\mathcal{Z}$ eine Äquivalenzrelation zugeordnet. Diese Zuordnung ist eineindeutig: Die zu $\sim_\mathcal{Z}$ gehörende Zerlegung ist wieder $\mathcal{Z}$ und die zu $\mathcal{Z}_\sim$ gehörende Äquivalenzrelation ist wieder $\sim$.*

Beweis. Es bleibt nur noch zu zeigen, dass ausgehend von einer Zerlegung $\mathcal{Z}$ die zu $\sim_\mathcal{Z}$ gehörende Zerlegung wieder $\mathcal{Z}$ ist, und ausgehend von einer Äquivalenzrelation $\sim$ die zu $\mathcal{Z}_\sim$ gehörende Äquivalenzrelation wieder $\sim$ ist. Das ist ziemlich offensichtlich, und der formale Beweis sei dem Leser überlassen. ■

Ein Element einer Äquivalenzklasse nennt man einen **Repräsentanten** dieser Äquivalenzklasse. $a \in A$ ist nach der obigen Diskussion genau dann ein Repräsentant der Äquivalenzklasse C wenn $[a] = C$ gilt.

Beispiel 1.7 *Wir betrachten die folgende Äquivalenzrelation auf $\mathbb{Z}$: Wir definieren $a \sim b$, wenn ein $k \in \mathbb{Z}$ existiert mit $b = a + 6k$. (Übungsaufgabe: Überzeugen Sie sich davon, dass das eine Äquivalenzrelation ist). Die Äquivalenzklassen sind: $\{0, \pm 6, \pm 12, \ldots\}$, $\{\ldots, -5, 1, 7, 13, \ldots\}$, $\{\ldots, -4, 2, 8, 14, \ldots\}$ etc. Insgesamt gibt es offenbar 6 verschiedene Äquivalenzklassen. Jede Äquivalenzklasse enthält genau eine Zahl aus der Menge $\{0, 1, 2, 3, 4, 5\}$. Wir können daher die Menge der Äquivalenzklassen, d.h. die zur Äquivalenzrelation gehörende Zerlegung von $\mathbb{Z}$ auch einfach mit der Menge $\{0, 1, 2, 3, 4, 5\}$ identifizieren. Die obige Zerlegung bezeichnet man auch mit $\mathbb{Z}_6$. $\mathbb{Z}_6$ enthält 6 Elemente, nämlich die obigen Äquivalenzklassen. Wie schon erwähnt, können wir $\mathbb{Z}_6$ mit $\{0, 1, 2, 3, 4, 5\}$ identifizieren, was aber etwas irreführend ist.*

6 spielt in der obigen Diskussion keine besondere Rolle. Man kann statt dessen auch jede beliebige natürlich Zahl $n \geq 1$ nehmen. Die entsprechende Zerlegung bezeichnet man dann auch als $\mathbb{Z}_n$.

Der Übergang von einer Menge A und einer darauf definierten Äquivalenzrelation $\sim$ zur Menge der Äquivalenzklassen ist in der Mathematik ausserordentlich

wichtig und wird Ihnen wieder und wieder begegnen. Anschaulich sollte man sich vorstellen, dass jeweils äquivalente Elemente, die ja dann eine Äquivalenzklasse bilden, zu einem "neuen Punkt" zusammengefasst werden. Man "kontrahiert" gewissermassen die Äquivalenzklassen zu neuen Elementen. Die Begriffe in Anführungszeichen haben jedoch keine mathematische Bedeutung, sondern dienen (hoffentlich) nur der Veranschaulichung.

Statt $\mathcal{Z}_\sim$ schreibt man meist $A/\sim$. Das werden wir auch in Zukunft tun. Hier noch ein anderes

Beispiel 1.8 *G bezeichne die Menge aller Geraden im Raum. Für $g_1, g_2 \in G$ definieren wir $g_1 \sim g_2$, wenn g_1 und g_2 parallel sind. $G/\sim$ ist die sogenannte* ***projektive Ebene,*** *die in der Geometrie ausserordentlich wichtig ist.*

1.4 Abzählbare Mengen

Von Cantor wurde eine Methode entwickelt, mit der man auch unendliche Mengen "zählen" kann. Für endliche Mengen A und B ist offensichtlich, dass sie gleich viele Elemente enthalten, wenn es eine bijektive Abbildung von A nach B gibt. Wir verallgemeinern dies nun wie folgt:

Definition 1.7 *A und B seien zwei Mengen. Sie heissen* ***gleich mächtig****, wenn es eine bijektive Abbildung $f : A \to B$ gibt. B heisst* ***mindestens so mächtig*** *wie A, wenn es eine injektive Abbildung $f : A \to B$ gibt.*

Definition 1.8 *Eine Menge, die gleich mächtig wie $\mathbb{N}$ ist, heisst* ***abzählbar unendlich.***

Ist A abzählbar unendlich, so liefert uns die bijektive Abbildung $f : \mathbb{N} \to A$ eine **Abzählung** der Elemente von $A : A = \{a_1, a_2, a_3, \ldots\}$: Wir setzen einfach $a_i := f(i)$. Da f bijektiv ist, sind die Elemente a_i alle verschieden, und es sind auch alle Elemente von A.

Erstaunlich an unendlichen Mengen ist, dass sie echte Teilmengen enthalten, die gleich mächtig wie sie selbst sind. So ist z.B. $\mathbb{N}$ natürlich eine echte Teilmenge von $\mathbb{N}_0$, aber $\mathbb{N}_0 \ni i \to i + 1 \in \mathbb{N}$ definiert eine Bijektion.

Satz 1.4 *A und B seien zwei Mengen. Falls injektive Abbildungen $f : A \to B$ und $g : B \to A$ existieren, so existiert auch eine bijektive Abbildung von A nach B.*

Obwohl die Aussage des obigen Satzes intuitiv einleuchtet — wenn A mindestens so mächtig wie B und B mindestens so mächtig wie A ist, dann sind A und B gleich mächtig — ist der Beweis nicht ganz einfach, und wir lassen ihn hier weg. Beweisen wollen wir hingegen die folgende Aussage über Produkte von abzählbar unendlichen Mengen.

Satz 1.5 *A und B seien zwei abzählbar unendliche Mengen. Dann ist auch $A \times B$ eine abzählbar unendliche Menge.*

Beweis. Wir betrachten zunächst Abzählungen von A und B, also $A = \{a_1, a_2, a_3, \ldots\}$, $B = \{b_1, b_2, b_3, \ldots\}$. Die Produktmenge hat dann die Elemente (a_i, b_j), $i, j \in \mathbb{N}$. Wir können die Elemente dieser Menge von Paaren wie folgt abzählen: $(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), (a_3, b_1), (a_1, b_4), \ldots$. Schematisch sieht das dann wie folgt aus:

$$\begin{array}{cccccc}
(a_1,b_1) & \rightarrow & (a_1,b_2) & & (a_1,b_3) & (a_1,b_4) & \ldots \\
 & \swarrow & & \swarrow & & \swarrow & \\
(a_2,b_1) & & (a_2,b_2) & & (a_2,b_3) & (a_2,b_4) & \ldots \\
 & \swarrow & & \swarrow & & \swarrow & \\
(a_3,b_1) & & (a_3,b_2) & & (a_3,b_3) & (a_3,b_4) & \ldots \\
 & \swarrow & & \swarrow & & \swarrow & \\
(a_4,b_1) & & (a_4,b_2) & & (a_4,b_3) & (a_4,b_4) & \ldots \\
\vdots & & \vdots & & \vdots & \vdots & \ddots
\end{array}$$

Wir definieren also eine bijektive Abbildung $f : \mathbb{N} \to A \times B$ durch $f(1) = (a_1, b_1)$, $f(2) = (a_1, b_2)$, $f(3) = (a_2, b_1)$ usw. Es ist klar, dass das eine bijektive Abbildung definiert, denn jedes Element von $A \times B$ kommt in der Auflistung genau einmal vor. ■

Der obige Satz liefert die erstaunliche Tatsache, dass für zwei abzählbar unendliche Mengen A und B eine Bijektion von A nach $A \times B$ existiert. Ist nämlich $g : \mathbb{N} \to A$ eine bijektive Abbildung, so ist mit dem oben konstruierten f, die Abbildung $f \circ g^{-1}$ eine bijektive Abbildung $A \to A \times B$. Man könnte vielleicht auf die Idee kommen, dass alle unendlichen Mengen gleich mächtig sind. Dem ist aber nicht so, wie der folgende Satz zeigt.

Satz 1.6 *Für jede Menge A ist $\mathcal{P}(A)$ nicht gleich mächtig wie A.*

Beweis. Wir nehmen an, dass A und $\mathcal{P}(A)$ gleich mächtig sind und führen das zu einem Widerspruch. f sei also eine bijektive Abbildung $A \to \mathcal{P}(A)$. Für jedes $a \in A$ ist dann $f(a)$ eine Teilmenge von A. Wir bilden die folgende Menge

$$B := \{a \in A : a \notin f(a)\}.$$

Da B eine Teilmenge von A ist, und wir voraussetzen, dass f bijektiv, also insbesondere surjektiv ist, existiert ein $b \in A$ mit $B = f(b)$. Wir fragen uns nun: Ist $b \in B$? Wäre $b \in B = f(b)$, so folgt aus der Definition von B, dass $b \notin B$ ist. Das ist also nicht möglich. Wäre aber $b \notin B$, so folgt wieder aus der Definition von B, dass $b \in B$ gilt. Das ist also auch nicht möglich. Somit bleibt nur noch die Möglichkeit, dass es eine derartige Abbildung gar nicht gibt. ■

Aus dem obigen Satz folgt insbesondere, dass die Menge der Teilmengen von $\mathbb{N}$ nicht abzählbar unendlich ist. Man nennt eine derartige Menge **überabzählbar.**

Man kann beweisen, dass es eine bijektive Abbildung von $\mathcal{P}(\mathbb{N}) \to \mathbb{R}$ gibt. $\mathbb{R}$ ist also auch überabzählbar. Im Gegensatz dazu ist die Menge der rationalen Zahlen abzählbar:

Satz 1.7 *$\mathbb{Q}$ ist abzählbar unendlich.*

Beweis. Wir betrachten zunächst $\mathbb{Q}^+ := \{x \in \mathbb{Q} : x > 0\}$. Eine Zahl q ist genau dann in $\mathbb{Q}^+$, wenn es Zahlen $m, n \in \mathbb{N}$ gibt mit $q = m/n$. Durch Kürzen von gemeinsamen Faktoren in Zähler und Nenner können wir erreichen, dass diese Darstellung eindeutig ist: Zu jeder Zahl $q \in \mathbb{Q}^+$ existiert genau ein Zahlenpaar $(m, n) \in \mathbb{N} \times \mathbb{N}$ mit g.g.T.$(m, n) = 1$ und $q = m/n$. Dies definiert also eine injektive Abbildung $\mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$. Setzen wir das mit der bijektiven Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ zusammen, die es nach Satz 1.6 gibt, so erhalten wir eine injektive Abbildung $\mathbb{Q}^+ \to \mathbb{N}$. Andererseits existiert eine injektive Abbildung $\mathbb{N} \to \mathbb{Q}^+$: Jede natürliche Zahl ist ja auch eine rationale Zahl. Zusammen mit Satz 1.4 folgt dann, dass $\mathbb{N}$ und $\mathbb{Q}^+$ gleich mächtig sind.

Dass $\mathbb{Q}^+$ und $\mathbb{Q}$ gleich mächtig sind, ist nun sehr einfach zu sehen: Es sei $q_1, q_2, q_3, \ldots$ ein Abzählung der Elemente von $\mathbb{Q}^+$. Dann ist $0, q_1, -q_1, q_2, -q_2, \ldots$ eine Abzählung der Elemente von $\mathbb{Q}$. ■

1.5 Vollständige Induktion

Die Menge der natürlichen Zahlen $\mathbb{N}$ hat eine wichtige Eigenschaft: Sie ist unter der natürlichen Ordnungsrelation $\leq$, wie man sagt, **wohlgeordnet**. Eine Ordnungsrelation $\leq$ auf einer Menge A heisst eine **Wohlordnung**, wenn jede nichtleere Teilmenge B von A ein kleinstes Element hat, d.h. es existiert ein Element $b \in B$ mit $c \geq b$ für alle $c \in B$. Dass $\mathbb{N}$ wohlgeordnet ist, ist offensichtlich: Ist $B \subset \mathbb{N}$ nicht leer, so gibt es eine Element $b \in B$. Dann ist die Menge $\{1, 2, \ldots, b\}$ eine endliche Menge und wir finden unter diesen Elementen sicher ein kleinstes Element, das in B liegt. Es sollte bemerkt werden, dass dieser Beweis formal nicht ganz präzise ist. Ein formal wirklich ganz genauer Beweis würde eine bessere Axiomatisierung der Mengenlehre erfordern, die wir hier nicht geben können. Unter Verwendung dieser Wohlordnungseigenschaft kann jedoch die folgende wichtige Eigenschaft bewiesen werden:

Satz 1.8 *Sei A eine Teilmenge von $\mathbb{N}$ mit den folgenden Eigenschaften:*
a) $1 \in A$
b) Für jedes $a \in A$ ist auch $a + 1 \in A$
Dann gilt $A = \mathbb{N}$.

Beweis. Wir führen die Annahme, dass $A \neq \mathbb{N}$ ist zu einem Widerspruch. Aus $A \neq \mathbb{N}$ folgt nämlich, dass A^c nicht leer ist. Demzufolge hat A^c ein kleinstes Element, nennen wir es b. Es gilt $b \neq 1$, denn 1 ist nach a) in A und demzufolge

nicht in A^c. Da $b \neq 1$ ist, ist $b-1 \in \mathbb{N}$. $b-1$ kann jedoch nicht in A^c sein, da b das kleinste Element von A^c war. Demzufolge ist $b-1 \in A$. Nach der Eigenschaft b) ist dann $b = (b-1)+1 \in A$ im Widerspruch zu $b \in A^c$. ■

Der obige Satz führt zu einem äusserst wichtigen Beweisverfahren, der **vollständigen Induktion**.

Satz 1.9 *Gegeben sei für jede natürliche Zahl $n \in \mathbb{N}$ eine Aussage $\mathcal{E}(n)$, die entweder wahr oder falsch sein kann. Falls*
a) $\mathcal{E}(1)$ gilt (Induktionsverankerung)
b) $\mathcal{E}(n) \Longrightarrow \mathcal{E}(n+1)$ für alle $n \in \mathbb{N}$ (Induktionsschluss)
Dann gilt $\mathcal{E}(n)$ für alle $n \in \mathbb{N}$.

Beweis. Sei $A := \{n \in \mathbb{N} : \mathcal{E}(n) \text{ gilt}\}$. Nach a) folgt $1 \in A$ und nach b) folgt, dass mit jeder Zahl $n \in A$ auch $n+1 \in A$ ist. Nach dem vorangegangenen Satz folgt, dass $A = \mathbb{N}$ ist. Demzufolge gilt $\mathcal{E}(n)$ für alle $n \in \mathbb{N}$. ■

Wir geben ein Beispiel:

Satz 1.10 *Für jede natürliche Zahl n gilt*

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Beweis. Wir führen den Beweis mit vollständiger Induktion.

Induktionsverankerung: Die Aussage gilt für $n = 1$. Dies ist offensichtlich.

Induktionsschluss: Wir nehmen an, die Aussage gelte für n (*Induktionsvoraussetzung*). Wir zeigen nun, dass sie dann auch für $n+1$ gilt:

$$\begin{aligned}
\sum_{j=1}^{n+1} j^2 &= \sum_{j=1}^{n} j^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \text{ (nach Induktionsvoraussetzung)} \\
&= (n+1)\left[\frac{n(2n+1)}{6} + n + 1\right] = (n+1)\frac{(n+2)(2n+3)}{6} \\
&= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.
\end{aligned}$$

■

Dieser Beweis hat natürlich den Nachteil, dass man nicht sieht, wie die Formel zustande kommt.

Prinzip der rekursiven Konstruktion

Es kommt oft vor, dass man eine Funktion, eine Zahl oder eine Menge, die noch von $n \in \mathbb{N}$ abhängt, quasi per Induktion nach n, oder wie man sagt, rekursiv

konstruiert. Ein einfaches Beispiel ist die Fakultät $n!$, die rekursiv durch die beiden Vorschriften:

$$1! := 1$$
$$(n+1)! := (n+1) \cdot n!$$

festgelegt wird. Es ist dann klar, dass $n!$ für jedes n auf diese Weise definiert ist. Man konstruiert also zunächst das erste Element und beschreibt dann, wie man das $(n+1)$-te aus dem n-ten gewinnt. Wir wollen das nicht genau durchformalisieren; wir werden noch sehr viele Beispiele dazu kennen lernen. Hier noch ein einfaches:

Nehmen wir an, Sie können zählen aber noch nicht rechnen (addieren und multiplizieren). Sie wissen also nur, wie man zu jeder Zahl n den Nachfolger dieser Zahl gewinnt, den wir mit $\phi(n)$ bezeichnen. Nun definieren wir die Addition: Wir konstruieren für $m, n \in \mathbb{N}$ die Zahl $m+n$ rekursiv nach n :

$$m + 1 := \phi(m)$$
$$m + (n+1) := \phi(m+n).$$

Wenn Sie also zählen können und das Prinzip der rekursiven Konstruktion kennen, so können Sie auch addieren. Nun zur Multiplikation $m \cdot n$, ebenfalls rekursiv nach n — wir setzen hier voraus, dass die Addition schon bekannt ist:

$$m \cdot 1 := m$$
$$m \cdot (n+1) := m \cdot n + m.$$

2 Algebraische Grundstrukturen: Gruppen, Ringe, Körper

2.1 Zweistellige Verknüpfungen, Gruppen

Wir betrachten eine nicht leere Menge A. Eine Abbildung $A \times A \to A$ nennt man eine **zweistellige Verknüpfung.** Statt wie sonst üblich mit f, g, ϕ oder ähnlichen Buchstaben, bezeichnet man eine derartige Abbildung meist mit $+, \cdot$ oder $*$. Im Moment nehmen wir $*$. Wir schreiben dann auch $a * b$ anstelle von $*(a, b)$. Das Paar $(a, b) \in A \times A$ wird also unter der Verknüpfung auf das Element $a * b \in A$ abgebildet. Sie kennen schon viele derartige Verknüfpungen, z.B. die Addition auf $\mathbb{N}$, die Multiplikation auf $\mathbb{N}$ oder auf $\mathbb{R}$ etc.

Definition 2.1 *$*$ sei eine zweistellige Verknüpfung auf der Menge A.*
*a) $*$ heisst **assoziativ**, wenn für alle Element $a, b, c \in A$ die Gleichung*

$$(a * b) * c = a * (b * c)$$

gilt.
*b) $*$ heisst **kommutativ**, wenn für alle $a, b \in A$*

$$a * b = b * a$$

gilt.
*c) Ein Element $e \in A$ heisst **Neutralelement,** wenn für jedes $a \in A$*

$$a * e = a = e * a$$

gilt.

Bemerkung 2.1 *Ein Neutralelement ist, falls es existiert, eindeutig.*

Beweis. Es seien e und e' zwei Neutralelemente. Dann folgt aus der Definition

$$e = e' * e = e'.$$

■

Es sei eine zweistellige assoziative Verknüpfung $*$ auf der Menge A gegeben. Es ist dann ziemlich klar, dass man nach Belieben "umklammern" kann. Z.B. ist dann für Elemente $a_1, a_2, \ldots, a_n \in A$ ein Produkt $a_1 * a_2 * \ldots * a_n \in A$ eindeutig definiert. Eigentlich hat man nur festgelegt, wie man je zwei Elemente verknüpft, sodass man dieses Element durch sukzessive Multiplikation gewinnen muss. Wir machen das nun ganz formal und definieren $a_1 * a_2 * \ldots * a_n$ rekursiv wie folgt: Für $n = 1$ ist das einfach a_1. Rekursiv setzen wir

$$a_1 * a_2 * \ldots * a_n * a_{n+1} := (a_1 * a_2 * \ldots * a_n) * a_{n+1}.$$

Damit haben wir für beliebiges $n \in \mathbb{N}$ und beliebige Elemente $a_1, a_2, \ldots, a_n \in A$ das Element $a_1 * a_2 * \ldots * a_n \in A$ definiert. Diese Defininition hängt zunächst nicht von der Assoziativität ab und könnte mit einer beliebigen zweistelligen Verknüpfung so gemacht werden. Nun zeigen wir, dass man dann beliebig umklammern kann:

Satz 2.1 *Für $n \in \mathbb{N}$, $a_1, a_2, \ldots, a_n \in A$ und $1 \leq k \leq n-1$ gilt*

$$(a_1 * a_2 * \ldots * a_k) * (a_{k+1} \ldots * a_n) = a_1 * a_2 * \ldots * a_n \tag{2.1}$$

Beweis. Wir definieren die Aussage $\mathcal{E}(n)$, $n \in \mathbb{N}$ wie folgt: Für beliebige Elemente $a_1, a_2, \ldots, a_n \in A$ und jedes $k \in \mathbb{N}$ mit $1 \leq k \leq n-1$ gilt (2.1).

Wir zeigen nun, dass $\mathcal{E}(n)$ für alle $n \in \mathbb{N}$ gilt, was die Aussage des Satzes beweist. Der Beweis erfolgt mit Induktion nach n.

Induktionsverankerung: Für $n = 1$ ist die Aussage trivialerweise richtig, denn es gibt gar keine Zahl k mit $1 \leq k \leq n-1$.

Induktionsschluss: Wir zeigen $\mathcal{E}(n) \Longrightarrow \mathcal{E}(n+1)$.

Seien also $a_1, a_2, \ldots, a_{n+1} \in A$ und $1 \leq k \leq n$. Ist $k = n$, so ist (2.1) einfach die Gleichung

$$a_1 * a_2 * \ldots * a_n * a_{n+1} = (a_1 * a_2 * \ldots * a_n) * a_{n+1},$$

die durch die rekursive Definition abgedeckt ist. Ist $1 \leq k \leq n-1$ so schliessen wir wie folgt:

$$\begin{aligned}(a_1 * a_2 * \ldots * a_k) * (a_{k+1} * \ldots * a_{n+1}) &= (a_1 * \ldots * a_k) * ((a_{k+1} * \ldots * a_n) * a_{n+1}) \\ &= ((a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_n)) * a_{n+1} \\ &= (a_1 * \ldots * a_n) * a_{n+1} \\ &= a_1 * \ldots * a_{n+1}.\end{aligned}$$

Die erste und vierte Gleichung gilt nach der rekursiven Definition, die zweite wegen der Assoziativität und die dritte folgt aus der Induktionsvoraussetzung.

Damit ist $\mathcal{E}(n+1)$ gezeigt. ■

Definition 2.2 *Eine Menge A, versehen mit einer zweistelligen Operation $*$, die assoziativ ist und ein Neutralelement besitzt, nennt man eine **Halbgruppe**. Eine Halbgruppe heisst **abelsch**, wenn die Operation zusätzlich kommutativ ist.*

*Eine Halbgruppe heisst **Gruppe**, wenn sie zusätzlich die folgende Eigenschaft hat: Zu jedem Element $a \in A$ existiert ein Element $b \in A$ mit*

$$a * b = b * a = e. \tag{2.2}$$

*Man nennt ein $b \in A$ mit dieser Eigenschaft ein zu a **inverses Element**.*

Wir schreiben dann $(A, *)$ für die Halbgruppe bzw. die Gruppe. Für abelsche Halbgruppen und Gruppen bezeichnet man die Verknüpfung üblicherweise mit $+$. Oft verwendet man auch einfach (je nach Situation) $\cdot$ als Verknüpfungszeichen.

Lemma 2.1 *Sei $(A, *)$ eine Halbgruppe und sei $a \in A$. Existiert ein $b \in A$ mit (2.2), so ist dieses Element eindeutig.*

Beweis. b, b' seien zwei derartige Elemente. Dann gilt

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'.$$

■

Nach dem Lemma können wir also von *dem* Inversen eines Elementes einer Halbgruppe sprechen. Eine Gruppe ist also eine Halbgruppe in der jedes Element ein Inverses hat. Man bezeichnet dieses Inverse von a üblicherweise als a^{-1}, oder auch als $-a$ im abelschen Fall, sofern man die Verknüpfung mit $+$ bezeichnet.

Beispiel 2.1 *a)* $(\mathbb{N}_0, +)$ *ist eine abelsche Halbgruppe (*0 *ist das Neutralelement)*
b) $(\mathbb{Z}, +)$ *ist eine abelsche Gruppe.*
c) $\mathbb{Z}$ *mit der üblichen Multiplikation* $\cdot$ *ist eine abelsche Halbgruppe.*
d) $(\mathbb{R}\setminus\{0\}, \cdot)$ *ist eine abelsche Gruppe.*

Bisher haben wir nur Beispiele abelscher Gruppen oder Halbgruppen gesehen. Hier eine nicht abelsche Gruppe:

Beispiel 2.2 *M sei eine beliebige, nicht leere Menge. A sei die Menge der bijektiven Selbstabbildungen $f : M \to M$. Auf A ist die zweistellige Verknüpfung der Komposition definiert: Für $f, g \in A$ ist $g \circ f$ die Komposition. Dann ist $(A, \circ)$ eine Gruppe. Das Neutralelement ist id_M. Das Inverse von f ist einfach die inverse Abbildung f^{-1}. Wir hatten alle Gruppeneigenschaften schon im Abschnitt 1.2 gezeigt. Wie wir auch dort am Beispiel einer endlichen Menge M gezeigt hatten, ist die Verknüpfung $\circ$ nicht kommutativ. Ist M eine endliche Menge mit n Elementen, so bezeichnet man diese Gruppe als die* ***symmetrische Gruppe*** *oder die* ***Permutationsgruppe*** *von n Elementen.*

Wir kommen nun zu einer anderen wichtigen (abelschen) Gruppe: $(\mathbb{Z}_n, +)$. Zur Erinnerung: In Beispiel 1.7 hatten wir $\mathbb{Z}_n$ für $n \in \mathbb{N}$ beschrieben als die Menge der Äquivalenzklassen in $\mathbb{Z}$ unter der Äquivalenzrelation

$$a \sim b \Longleftrightarrow \exists k \,\mathrm{mit}\, a = b + kn. \tag{2.3}$$

Wir konnten $\mathbb{Z}_n$ auch einfach mit der Menge $\{0, 1, \ldots, n-1\}$ identifizieren. Wir definieren nun eine Addition $\dot{+}$ auf dieser Menge: Sind $a, b \in \{0, 1, \ldots, n-1\}$, so ist $a + b$, in den ganzen Zahlen addiert, in $\{0, 1, \ldots, n-1\}$ oder in $\{n, n+1, \ldots,$

$2n-1\}$. Im ersten Fall setzen wir $a\dot{+}b := a+b$ und im zweiten $a\dot{+}b := a+b-n$. In jedem Fall erhalten wir $a \dot{+} b \in \{0, 1, \ldots, n-1\}$. $\left(\mathbb{Z}_n, \dot{+}\right)$ ist dann eine abelsche Gruppe, wie man leicht nachprüft. Das Neutralelement ist natürlich 0.

Wir wollen nun dieselbe Addition auf etwas umständlichere Weise erklären, die jedoch später in sehr vielen Fällen wichtig sein wird. Wie oben erwähnt, kann $\mathbb{Z}_n$ auch also $\mathbb{Z}/\sim$ beschrieben werden, wobei $\sim$ durch (2.3) gegeben ist. $\mathbb{Z}_n$ ist also die Menge der Äquivalenzklassen unter dieser Äquivalenzrelation:

$$\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}.$$

Wir versuchen nun die Addition $\dot{+}$ auf $\mathbb{Z}_n$ einfach wie folgt zu beschreiben:

$$[a] \dot{+} [b] := [a+b]. \tag{2.4}$$

Ein Moment des Nachdenkens zeigt jedoch, dass es nicht ganz klar ist, ob die rechte Seite eine Verknüpfung von $[a]$ und $[b]$ überhaupt definiert. Man muss sich folgendes überlegen: Wenn a und $a' \in \mathbb{Z}$ dieselbe Äquivalenzklasse repräsentieren, d.h. wenn $[a] = [a']$ gilt und auch $[b] = [b']$, so gilt $[a+b] = [a'+b']$. Wäre dies nicht richtig, so wäre (2.4) eine unsinnige Festsetzung, die gar keine Verknüpfung auf $\mathbb{Z}_n$ definiert.

Lemma 2.2 *Sind $a, a', b, b' \in \mathbb{Z}$ mit $a \sim a'$ und $b \sim b'$, so gilt $a+b \sim a'+b'$.*

Beweis. Wegen $a \sim a'$ existiert $k \in \mathbb{Z}$ mit $a = a' + k\,n$. Dasselbe mit den b's: Es exisitiert $l \in \mathbb{Z}$ mit $b = b' + l\,n$. Daraus ergibt sich $a+b = a'+b'+(k+l)\,n$. Dies impliziert $a+b \sim a'+b'$. ■

Die Aussage dieses Lemmas impliziert, dass (2.4) eine Verknüpfung auf $\mathbb{Z}_n$ definiert. Was man mit dem Lemma zeigt, ist dass die gewünschte Festlegung durch (2.4) unabhängig von den Repräsentanten auf der linken Seite ist. Man sagt dann auch, dass durch (2.4) die Verknüpfung **wohldefiniert** sei. Dies ist sprachlich etwas unsinnig, denn wenn die Aussage des Lemmas nicht gelten würde, so würde (2.4) gar nichts definieren, auch nicht "unwohl".

Auf dieselbe Weise können wir auch eine Multiplikation auf $\mathbb{Z}_n$ festlegen. Dazu benötigen wir das folgende

Lemma 2.3 *Sind $a, a', b, b' \in \mathbb{Z}$ mit $a \sim a'$ und $b \sim b'$, so gilt $ab \sim a'b'$.*

Beweis. Wegen $a \sim a'$ existiert $k \in \mathbb{Z}$ mit $a = a' + k\,n$. Dasselbe mit den b's: Es exisitiert $l \in \mathbb{Z}$ mit $b = b' + l\,n$. Daraus folgt $ab = a'b' + knb' + lna' + lkn^2 = a'b' + (kb' + la' + lkn)\,n$. Dies impliziert $ab \sim a'b'$. ■

Mit Hilfe dieses Lemmas wird mit

$$[a] * [b] := [ab]$$

eine Verknüpfung auf $\mathbb{Z}_n$ definiert.

Es ist leicht zu sehen, dass diese Verknüpfung assoziativ und kommutativ ist. Ferner existiert ein Neutralelement, nämlich [1] (1, wenn wir $\mathbb{Z}_n$ mit $\{0, 1, 2, \ldots, n-1\}$ identifizieren). Somit gilt

Satz 2.2 *a)* $\left(\mathbb{Z}_n, \dot{+}\right)$ *ist eine abelsche Gruppe.*

b) $(\mathbb{Z}_n, *)$ *ist eine abelsche Halbgruppe. Das Neutralelement ist* [1]

Es stellt sich die naheliegende Frage, ob $(\mathbb{Z}_n, *)$ eine Gruppe ist. Es ist leicht ersichtlich, dass das nicht der Fall ist. $[0] * [a] = [0]$ für alle $[a] \in \mathbb{Z}_n$. Demzufolge kann [0] kein inverses Element haben, denn es gilt $[1] \neq [0]$ (sofern $n \geq 2$ ist). Eine interessantere Frage ist jedoch, ob $\mathbb{Z}_n$ unter der Multiplikation eine Gruppe ist, wenn man die Null weglässt. Wir setzen

$$\mathbb{Z}_n^* := \mathbb{Z}_n \setminus \{[0]\}.$$

Nun ergibt sich jedoch das Problem, dass $*$ auf $\mathbb{Z}_n^*$ gar nicht immer definiert ist, dann z.B. für $n = 6$ gilt $[2] * [3] = [6] = [0]$.

Lemma 2.4 *Ist* n *eine Primzahl, so ist* $[a] * [b] \neq [0]$ *für alle* $[a], [b] \in \mathbb{Z}_n^*$.

Beweis. Wir können annehmen, dass a und b in $\{1, 2, \ldots, n-1\}$ sind. Wäre $[a] * [b] = [0]$, so wäre ab ein Vielfaches von n. Also wäre n in der Primfaktorzerlegung von ab, was offensichtlich nicht möglich ist. ■

Satz 2.3 *Ist* n *eine Primzahl, so ist* $(\mathbb{Z}_n^*, *)$ *eine Gruppe.*

Beweis. Wir müssen nachweisen, dass jedes Element $[a] \in \mathbb{Z}_n^*$ ein multiplikatives Inverses hat. Dazu weisen wir einfach nach, dass die Elemente $[a] * [b]$ für $b = 1, 2, \ldots, n-1$ alle verschieden sind. Da $\mathbb{Z}_n^*$ genau $n-1$ Elemente enthält, folgt dann, dass ein b existiert mit $[a] * [b] = [1]$.

Wir können den Repräsentanten a in $\{1, 2, \ldots, n-1\}$ wählen. Der Rest des Beweises geht analog zu dem von Lemma 2.4. Wir führen ihn indirekt. Wir nehmen an, dass zwei verschiedene Elemente $b, b' \in \{1, 2, \ldots, n-1\}$ existieren mit $[a]*[b] = [a]*[b']$. Wir können annehmen, dass $b > b'$ gilt. Aus $[a]*[b] = [a]*[b']$ folgt, dass ein $k \in \mathbb{Z}$ existiert mit $ab = ab' + kn$, d.h. $a(b - b')$ ist ein Vielfaches von n. Das ist offensichtlich nicht möglich, wenn n eine Primzahl ist. ■

Wir werden von nun an $+$ anstelle von $\dot{+}$ und $\cdot$ anstelle von $*$ schreiben für die beiden Operationen auf $\mathbb{Z}_n$. Statt $[a] + [b] = [c]$ mit $a, b, c \in \{1, 2, \ldots, n-1\}$ schreibt man dann oft auch

$$a + b = c \bmod n$$

oder auch einfach $a + b = c$ wenn aus dem Kontext klar ist, dass es sich um die Addition in $\mathbb{Z}_n$ handelt, und entsprechend auch für die Multiplikation.

2.2 Ringe und Körper

Es gibt viele wichtige algebraische Strukturen, die zwei zweistellige Verknüpfungen besitzen. Das Paradebeispiel dafür ist $\mathbb{Z}$, auf dem man addieren und multiplizieren kann.

Definition 2.3 *Eine Menge A mit zwei zweistelligen Verknüpfungen $+$ und $\cdot$ heisst **Ring (mit Eins)**, wenn die folgenden Bedingungen erfüllt sind:*

a) $(A, +)$ ist eine abelsche Gruppe.

b) $(A, \cdot)$ ist eine Halbgruppe

*c) Es gelten die beiden **Distributivgesetze:** Für alle $a, b, c \in A$ gilt*

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

*Ist die Verknüpfung $\cdot$ kommutativ, d.h. ist $(A, \cdot)$ eine abelsche Halbgruppe, so heisst der Ring **kommutativ.***

Das Neutralelement der Addition bezeichnet man stets mit 0. Das zu $a \in A$ bezüglich der Addition inverse Element bezeichnet man mit $-a$. Das Neutralelement der Multiplikation wird mit 1 bezeichnet. Das mag unter Umständen etwas verwirren, denn mit 1 bezeichnen wir ja auch stets die natürliche Zahl "Eins". Aus dem Kontext sollte immer klar sein, um welche "Eins" es sich jeweilen handelt. Gewöhnen Sie sich jedoch an, sich das immer ganz genau zu überlegen.

Ist der Ring kommutativ, so braucht man natürlich nur eines der Distributivgesetzte zu fordern; das andere folgt dann wegen der Kommutativität.

Lemma 2.5 *Ist $(A, +, \cdot)$ ein Ring, so gilt*

$$a \cdot 0 = 0 \cdot a = 0$$

für alle $a \in A$.

Beweis.

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

Addiert man auf der linken und der rechten Seite dieser Gleichung $-(a \cdot 0)$, so folgt $0 = a \cdot 0$. Analog folgt $0 \cdot a = 0$. ∎

Eine einfach Folgerung aus dem Lemma ist, dass $1 \neq 0$ ist, sofern A mehr als ein Element enthält. Wäre nämlich $1 = 0$, so würde für jedes $a \in A$ die Gleichung $a = 1 \cdot a = 0 \cdot a = 0$ gelten. Der Ring, der nur die 0 enthält, ist natürlich völlig trivial. Wir setzen von nun an stets voraus, dass $1 \neq 0$ gilt.

Beispiel 2.3 *a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.*

b) $(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring mit Eins. Das Distributivgesetz folgt ganz leicht aus dem Distributivgesetz in $\mathbb{Z}$.

Wir werden noch viele wichtige Ringe kennenlernen. Zu den in der Mathematik wichtigsten gehören die sogenannten **Polynomringe**. Wir betrachten zunächst reelle Polynome; dies lässt sich jedoch später sehr leicht verallgemeinern.

Definition 2.4 *Ein **reelles Polynom** in einer Variablen x ist ein Ausdruck der Form*

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

*mit $a_0, a_1, \ldots, a_n \in \mathbb{R}$. Diese Zahlen heissen die **Koeffizienten** des Polynoms. Das Polynom mit allen Koeffizienten 0 heisst das **Nullpolynom.** Wir bezeichnen es auch einfach mit 0.*

Man setzt üblicherweise für ein Polynom, das nicht das Nullpolynom ist, voraus, dass $a_n \neq 0$ ist. Ist $a_n = 0$ so lässt man $a_n x^n$ einfach weg. Reduziert man das Polynom auf diese Weise, so gelangt man schliesslich zu einem Polynom mit höchstem Koeffizienten $\neq 0$. n heisst dann der **Grad** des Polynoms. Man kann jedoch ein Polynom vom Grad n für jedes $m \in \mathbb{N}$ auch mit Koeffizienten $a_{n+1} = 0, \ldots, a_{n+m} = 0$ ergänzen.

Polynome kann man addieren und multiplizieren. Sind $p(x)$ und $q(x)$ zwei Polynome, so definiert man die Addition $p(x) + q(x)$, indem man einfach die Koeffizienten addiert:

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)\, x + \ldots + (a_n + b_n)\, x^n.$$

In dieser Schreibweise haben wir das Polynom von eventuell niedrigerem Grad durch Nullen ergänzt. Die Multiplikation ist etwas komplizierter definiert. Die Multiplikation mit dem Nullpolynom ist stets das Nullpolynom. Sind $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ und $q(x) = b_0 + b_1 x + \ldots + b_m x^m$ zwei Polynome, beide $\neq 0$, so definiert man

$$p(x) \cdot q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + (a_0 b_2 + a_1 b_1 + a_2 b_0)\, x^2 + \ldots + a_n b_m x^{m+n}.$$

Es sollte aus dem Gymnasium bekannt sein, dass die Polynommultiplikation kommutativ und assoziativ ist. Das Neutralelement ist das Polynom $p(x) = 1$. Man bezeichnet mit $\mathbb{R}[x]$ die Menge aller Polynome (mit reellen Koeffizienten). $\mathbb{R}[x]$ versehen mit der Addition ist offenbar eine abelsche Gruppe. Das Neutralelement ist das Nullpolynom 0. Ferner ist $\mathbb{R}[x]$ versehen mit der Multiplikation $\cdot$ eine abelsche Halbgruppe. Es sollte ebenfalls bekannt sein, dass das Distributivgesetz gilt. Demzufolge gilt

Satz 2.4 $(\mathbb{R}[x], +, \cdot)$ *ist ein kommutativer Ring mit Eins.*

Bemerkung 2.2 *Eine Bemerkung, die etwas an Haarspalterei grenzt: Die "Variable" x spielt eigentlich in der obigen Diskussion keine richtige Rolle. Wir*

können ein Polynom auch einfach durch das $(n+1)$-Tupel seiner Koeffizienten $(a_0, a_1, \ldots, a_n)$ beschreiben. Dann ist

$$\mathbb{R}[x] := \{(a_0, a_1, \ldots, a_n) : n \in \mathbb{N}_0,\, a_i \in \mathbb{R} \,\text{für}\, 0 \leq i \leq n,\, a_n \neq 0 \,\text{falls}\, n \neq 0\}\,.$$

Die Addition und die Multiplikation kann dann aufgrund dieser Koeffizienten definiert werden. Eine "Variable" x kommt so gar nicht mehr vor.

Andererseits wissen Sie natürlich, dass ein Polynom eine Abbildung $\mathbb{R} \to \mathbb{R}$ definiert, einfach durch $\mathbb{R} \ni t \to a_0 + a_1 t + \ldots + a_n t^n$ und Addition und Multiplikation von Polynomen entspricht dann einfach der Addition und Multiplikation der Funktionswerte. Man sollte jedoch zwischen einem Polynom, aufgefasst als formales Tupel $(a_0, a_1, \ldots, a_n)$ der Koeffizienten, und aufgefasst als Abbildung $\mathbb{R} \to \mathbb{R}$ unterscheiden. Der Grund für diese Haarspalterei ist im Moment nicht richtig ersichtlich. Es wird sich jedoch später herausstellen, dass in allgemeineren Situation zwei verschiedene (formale) Polynome durchaus dieselbe Abbildung definieren können.

Ist $(A, +, \cdot)$ ein Ring mit Eins (kommutativ oder nicht), so kann man sich fragen, welche Elemente ein Inverses bezüglich der Multiplikation haben. 0 kann offenbar kein Inverses haben, denn wir hatten schon gesehen, dass $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in A$ gilt, und demzufolge kann es kein Element 0^{-1} geben mit $0^{-1} \cdot 0 = 0 \cdot 0^{-1} = 1$ (wegen $1 \neq 0$). Das Nächstbeste, was man haben kann, ist wenn jedes Element $\neq 0$ ein Inverses besitzt.

Definition 2.5 *a) Ein kommutativer Ringe mit Eins, in dem jedes Element $\neq 0$ ein multiplikatives Inverses besitzt, heisst* ***Körper.***

b) Ein nicht-kommutativer Ring (mit Eins), in dem jedes Element $\neq 0$ ein multiplikatives Inverses besitzt, heisst ***Schiefkörper.***

Die Namensgebung hat sich so eingebürgert, ist linguistisch aber ganz unsinnig. Nach üblichem Sprachverständnis wäre ein Schiefkörper ein Körper, der noch die zusätzliche Eigenschaft "Schiefe" hat. Das ist aber genau nicht der Fall: Eine zusätzliche Eigenschaft hat ein Körper, nämlich die Kommutativität. Schiefkörper machen sich übrigens ziemlich rar. Während wir gleich eine Reihe von Beispielen von Körpern kennen lernen werden, können wir im Moment kein Beispiel eines Schiefkörpers angeben. Das einzige (konkrete) Beispiele, das wir kennen lernen werden, ist der Quaternionen-Schiefkörper, den wir im nächsten Semester diskutieren werden.

Das multiplikative Inverse eines Elements a bezeichnet man üblicherweise mit a^{-1} oder $\frac{1}{a}$ (im Gegensatz zum additiven Inversen $-a$).

Beispiel 2.4 *a) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Beispiele von Körpern.*

b) Ist n eine Primzahl, so ist $(\mathbb{Z}_n, +, \cdot)$ ein Körper (wegen Satz 2.3).

Ist n keine Primzahl, so ist $(\mathbb{Z}_n, +, \cdot)$ kein Körper. Das können wir wie folgt einsehen. Ist n keine Primzahl, so existieren Zahlen $1 \leq p, q < n$ mit $pq = n$. Demzufolge gilt in $\mathbb{Z}_n$ die Gleichung $pq = 0$. Man sagt, dass $\mathbb{Z}_n$ **Nullteiler** hat. Dass $(\mathbb{Z}_n, +, \cdot)$ kein Körper sein kann, folgt dann aus

Lemma 2.6 *Ein Körper $(K, +, \cdot)$ hat keine Nullteiler, d.h. für $a, b \neq 0$, $a, b \in K$ gilt $a \cdot b \neq 0$.*

Beweis. Aus $a \cdot b = 0$ und $a \neq 0$ folgt

$$b = 1 \cdot b = \left(a^{-1} \cdot a\right) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

■

Die Umkehrung der Aussage des Lemmas gilt übrigens nicht: Ein kommutativer Ring (mit Eins), der keine Nullteiler besitzt, ist deswegen noch lange kein Körper. Ein Beispiel ist $\mathbb{R}[x]$. $\mathbb{R}[x]$ hat offensichtlich keine Nullteiler, das Polynom $p(x) = x$ hat jedoch kein Inverses, d.h. es gibt kein Polynom $q(x)$ mit $p(x) \cdot q(x) = 1$.

Wir werden im weiteren Verlauf der Vorlesung den Punkt $\cdot$ für die Multiplikation auch weglassen, wenn dies nicht zu Verwechslungen führen kann, so wie das auch in $\mathbb{R}$ üblich ist.

Körper haben also die Eigenschaft, dass man in ihnen "wie in $\mathbb{R}$" rechnen kann: Man kann addieren, subtrahieren, multiplizieren und durch Elemente $\neq 0$ dividieren. Es gibt jedoch durchaus grosse Unterschiede. Z.B. gilt im Körper $\mathbb{Z}_2$ die Eigenschaft $1+1 = 0$, was vielleicht etwas ungewohnt ist. Sei K ein beliebiger Körper. Wir definieren rekursiv für $n \in \mathbb{N}$ ein Element $\widehat{n} \in K$:

$$\begin{aligned} \widehat{1} &:= 1 \\ \widehat{(n+1)} &:= \widehat{n} + 1. \end{aligned}$$

Hier ist etwas Vorsicht geboten: Die 1 auf den rechten Seiten meint die Eins im Körper, also das Neutralelement der Multiplikation. Ebenfalls ist + die Addition im Körper. Hingegen ist die 1 auf der linken Seite die Eins in $\mathbb{N}$ und die Addition ist die Addition in $\mathbb{N}$.

Definition 2.6 *Gilt in einem Körper $\widehat{n} \neq 0$ für alle $n \in \mathbb{N}$, so sagt man, der Körper habe **Charakteristik** 0. Anderenfalls ist die Charakteristik definiert durch*

$$\operatorname{char}(K) := \min\{n \in \mathbb{N} : \widehat{n} = 0\}.$$

Satz 2.5 *Ist* $\operatorname{char}(K) \neq 0$, *so ist* $\operatorname{char}(K)$ *eine Primzahl.*

Beweis. Wir zeigen, dass für $m, n \in \mathbb{N}$ die Gleichung

$$\widehat{(mn)} = \widehat{m}\widehat{n} \tag{2.5}$$

gilt. Zunächst zeigen wir die Gleichung

$$\widehat{(m+n)} = \widehat{m} + \widehat{n}. \tag{2.6}$$

Dies folgt mit Induktion nach n : Für $n = 1$ ist es die Definition und der Induktionsschluss geht wie folgt:

$$\begin{aligned}(m + \widehat{(n+1)}) = (\widehat{(m+n)} + 1) &= \widehat{(m+n)} + 1 \\ &= \widehat{m} + \widehat{n} + 1 = \widehat{m} + \widehat{n+1}.\end{aligned}$$

(Übungsaufgabe: Überlegen Sie sich bei jeder der Gleichungen *ganz genau*, wieso sie gilt). Damit ist (2.6) bewiesen. Wir zeigen nun (2.5) ebenfalls mit Induktion nach n. Für $n = 1$ folgt die Aussage wegen $\widehat{1} = 1$. Nun wieder der Induktionsschritt:

$$\begin{aligned}(m\widehat{(n+1)}) &= (\widehat{mn+m}) \\ &= \widehat{mn} + \widehat{m} && \text{(nach (2.6))} \\ &= \widehat{m}\widehat{n} + \widehat{m} && \text{(nach Induktionsvoraussetzung)} \\ &= \widehat{m}\,(\widehat{n}+1) && \text{(Distributivgesetz in } K) \\ &= \widehat{m}\widehat{(n+1)} && \text{(nach Definition).}\end{aligned}$$

Damit ist (2.5) bewiesen.

Aus dieser Gleichung folgt nun sofort, dass die Charakteristik von K eine Primzahl ist (falls sie $\neq 0$ ist): Sei $n \in \mathbb{N}$ die Charakteristik. Zunächst ist wegen $1 \neq 0$ (im Körper) die Charakteristik $\neq 1$. Wir nehmen an, die Charakteristik sei keine Primzahl. Dann existieren Zahlen $p, q \in \mathbb{N}$, $p, q < n$ mit $n = pq$. Wegen (2.5) folgt

$$0 = \widehat{n} = \widehat{pq} = \widehat{p}\widehat{q}.$$

Da ein Körper keine Nullteiler hat, folgt dass $\widehat{p}$ oder $\widehat{q}$ gleich 0 ist. Dies steht jedoch im Widerspruch zur Definition der Charakteristik als die *kleinste* natürliche Zahl n mit $\widehat{n} = 0$. ■

Beispiel 2.5 *Der Körper $(\mathbb{Z}_p, +, \cdot)$ (p Primzahl) hat Charakteristik p.*

Bemerkung 2.3 *Es gibt viele andere Körper, die Charakteristik p haben. Es gibt jedoch nicht sehr viele Körper mit endlich vielen Elementen. Man weiss, dass es für jede Zahl $m \in \mathbb{N}$ und jede Primzahl p im Wesentlichen genau einen Körper mit p^m Elementen gibt. Diese Körper heissen Galois-Felder. Der Körper kann für $m \geq 2$ jedoch nicht $(\mathbb{Z}_{p^m}, +, \cdot)$ sein, da dieser Ring Nullteiler hat, wie wir gesehen hatten. Die Konstruktion der Galois-Felder ist nicht ganz einfach. Man kann jedoch leicht nachweisen, dass ein Körper mit p^m Elementen Charakteristik p hat. (Übungsaufgabe).*

3 Lineare Gleichungssysteme, Matrizen

3.1 Das Gaußsche Eliminationsverfahren

Die einfachste lineare Gleichung für die Unbekannte $x \in \mathbb{R}$ ist die Gleichung der Form

$$ax = b, \tag{3.1}$$

wobei a und $b \in \mathbb{R}$ sind. Schon für diese einfache Gleichung müssen wir einige Fallunterscheidungen machen. Der "Standardfall" ist $a \neq 0$. Dann hat die Gleichung die eindeutige Lösung $x = b/a$. Ist hingegen $a = 0$, so gibt es zwei Unterfälle: Ist auch $b = 0$, so ist jede Zahl eine Lösung dieser Gleichung. Ist aber $b \neq 0$ (aber immer noch $a = 0$), so hat die Gleichung keine Lösung. Bezeichnen wir mit L die Lösungsmenge

$$L := \{x \in \mathbb{R} : ax = b\}, \tag{3.2}$$

so gilt also

$$L = \begin{cases} \{b/a\}, & \text{falls } a \neq 0, \\ \mathbb{R}, & \text{falls } a = 0 \text{ und } b = 0, \\ \emptyset, & \text{falls } a = 0 \text{ und } b \neq 0. \end{cases}$$

Wir wollen diese Diskussion nun auf mehrere Gleichungen mit mehreren Unbekannten verallgemeinern. Das Endergebnis wird eine völlig analoge Fallunterscheidung sein. Zunächst sei jedoch bemerkt, dass wir, statt nur Gleichungen für Unbekannte in $\mathbb{R}$ zu betrachten, in jedem beliebigen Körper arbeiten können. K sei also ein Körper (z.B. $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{Z}_p$, p Primzahl). Wir betrachten dann die Gleichung (3.2) für Koeffizienten $a, b \in K$ und suchen Lösungen x in K. Alles geht natürlich genauso wie oben, denn wir können in K wie in $\mathbb{R}$ durch Zahlen $\neq 0$ dividieren.

Nun zu Systemen von Gleichungen. Wir betrachten m Gleichungen für die n Unbekannten $x_1, x_2, \ldots, x_n \in K$:

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & b_1, \\ a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n & = & b_2, \\ \vdots & & \vdots & & & & \vdots & \vdots & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n & = & b_m. \end{array} \tag{3.3}$$

Dabei sind die Koeffizienten $a_{ij} \in K$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ und $b_i \in K$ für $1 \leq i \leq m$. Man kann das Gleichungssystem auch kurz wie folgt schreiben:

$$\sum_{j=1}^{n} a_{ij}x_j = b_i,\ i = 1, \ldots, m.$$

Die Lösungsmenge ist definiert als

$$L := \left\{ (x_1, x_2, \ldots, x_n) \in K^n : \sum_{j=1}^{n} a_{ij}x_j = b_i \text{ für } i = 1, \ldots, m \right\}.$$

Dies ist eine Teilmenge der Menge aller n-Tupel von Elementen in K : $L \subset K^n$. L kann natürlich leer sein, wie wir schon gesehen haben. Wir gehen nun daran, das Gleichungssystem systematisch zu lösen. Die Methode heisst "Gauss-Elimination", nach dem berühmten Mathematiker Carl Friedrich Gauss, von ihm selbst "eliminatio vulgaris" genannt. Dazu führen wir Manipulationen des Systems durch, welche die Lösungsmenge nicht ändern. Ziel dieser Manipulationen ist es, das System auf ein anderes System zu reduzieren, bei dem die Lösungen unmittelbar abgelesen werden können. Die Operationen nennt man **elementare Zeilenoperationen (**die "Zeilen" sind einfach die einzelnen Gleichungen):

Z1 Vertauschen zweier Zeilen des Gleichungssystems.

Z2 Multiplikation einer Zeile mit einem Körperelement $\alpha \neq 0$. Hier werden alle Koeffizienten einer der Gleichungen mit α multipliziert, und natürlich auch das entsprechende b_i.

Z3 Addition des α-fachen einer Zeile zu einer anderen, $\alpha \in K$. Wird etwa das α-fache der l-ten Zeile zur k-ten addiert, so sieht das Gleichungssystem (3.3) wie folgt aus:

$$\begin{array}{ccccccc}
a_{11}x_1 & + & a_{12}x_2 & +\ldots+ & a_{1n}x_n & = & b_1, \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{k1}x_1 + \alpha a_{l1}x_1 & + & a_{k2}x_2 + \alpha a_{l2}x_2 & +\ldots+ & a_{kn}x_n + \alpha a_{ln}x_n & = & b_k + \alpha b_l, \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{m1}x_1 & + & a_{m2}x_2 & +\ldots+ & a_{mn}x_n & = & b_m.
\end{array}$$

Alle Gleichungen ausser der k-ten bleiben unangetastet. In kompakter Schreibweise sieht das Gleichungssystem nach dieser Zeilenoperation wie folgt aus:

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \quad \text{für } 1 \leq i \leq m,\ i \neq k, \tag{3.4}$$

$$\sum_{j=1}^{n} \left(a_{kj} + \alpha a_{lj}\right) x_j = b_k + \alpha b_l. \tag{3.5}$$

Satz 3.1 *Die elementaren Zeilenoperationen Z1-Z3 verändern die Lösungsmenge eines Gleichungssystems nicht.*

Beweis. Für Z1 und Z2 ist das offensichtlich. Wir diskutieren Z3: Sei L die Lösungsmenge von (3.3) und L' die Lösungsmenge von (3.4), (3.5). Ist $x = (x_1, x_2, \ldots, x_n) \in L$, so gilt natürlich (3.4) und ferner

$$\sum_{j=1}^{n} \left(a_{kj} + \alpha a_{lj}\right) x_j = \sum_{j=1}^{n} a_{kj}x_j + \sum_{j=1}^{n} \alpha a_{lj}x_j = b_k + \alpha b_l,$$

was nichts anderes als (3.5) ist. Demzufolge ist $x \in L'$, und wir haben somit gezeigt, dass $L \subset L'$ ist.

Zum Beweis von $L' \subset L$ beachte man, dass wir das "alte" Gleichungssystem (3.3) aus dem Gleichungssystem (3.4), (3.5) erhalten, indem wir zur k-ten Zeile das $(-\alpha)$-fache der l-ten addieren. Damit ergibt sich das "alte" Gleichungssystem aus dem "neuen" ebenfalls durch eine Zeilenoperation des Typs Z3. Die vorherige Überlegung zeigt also $L' \subset L$. Damit ist $L = L'$ bewiesen. ■

Für den weiteren Verlauf der Diskussion ist es überflüssig und eher beschwerlich, die x_i in der Notation immer mitzuschleppen. Wir betrachten deshalb einfach die sogenannte Koeffizientenmatrix

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

Eine solche Anordnung von Körperelementen nennt man eine $m \times n$-Matrix. Die obige Matrix hat m Zeilen und n Spalten. a_{ij} nennt man die ***ij*-te Komponente** der Matrix. Wir schreiben die Matrix auch als

$$A = (a_{ij})_{1 \le i \le m,\, 1 \le j \le n},$$

oder auch einfach kurz $A = (a_{ij})$, wenn klar ist, wieviele Zeilen und Spalten sie hat. Man bezeichnet die Zeilen und Spalten als "Vektoren" (später mehr zu diesem Begriff). Die Matrix hat also die m Zeilenvektoren

$$\begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix},\ 1 \le i \le m,$$

und die n Spaltenvektoren

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix},\ 1 \le j \le n.$$

Einen Zeilenvektor können wir natürlich auch als $1 \times n$-Matrix auffassen, und einen Spaltenvektor als $m \times 1$-Matrix. Einige zusätzliche Begriffe: **Nullvektoren** sind Vektoren, deren Komponenten *alle* gleich Null sind. Ebenfalls ist die **Nullmatrix** die Matrix mit allen $a_{ij} = 0$. Wir können unsere Matrix A durch den zusätzlichen Spaltenvektor

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \tag{3.6}$$

ergänzen und erhalten dann die $m \times (n+1)$-Matrix

$$(A,b) := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}.$$

Die oben beschriebenen elementaren Zeilenoperationen verändern dann einfach die Zeilenvektoren, indem bei Z1 zwei Zeilenvektoren vertauscht werden, bei Z2 eine Zeile in jeder Komponente mit einem Körperelement $\alpha \neq 0$ multipliziert wird und bei Z3 das α-fache einer Zeile zu einer anderen Zeile addiert wird.

Wir wollen die Matrix (A,b) nun mit Hilfe solcher Zeilenoperationen auf eine besonders einfache Form bringen, die sogenannte **Stufenform**. Wir suchen zunächst nach der ersten Spalte der Matrix A, die nicht gleich dem Nullvektor ist, d.h. deren Komponenten nicht alle gleich Null sind. Gibt es keine derartige Spalte, so ist A die Nullmatrix. In diesem Fall ist das Gleichungssystem (3.3) besonders einfach

$$\sum_{j=1}^{n} 0 \cdot x_j = b_i,\ 1 \leq i \leq m.$$

Die Lösungsmenge dieses Gleichungssystems L ist natürlich ganz einfach zu bestimmen: Gibt es mindestens ein $b_i \neq 0$, so ist $L = \emptyset$, d.h. es gibt gar keine Lösungen. Gilt hingegen $b_i = 0$ für alle i, so sind offensichtlich alle n-Tupel $(x_1, x_2, \dots, x_n)$ Lösungen, d.h. es gilt $L = \mathbb{R}^n$. In diesem Fall können wir die Lösungsmenge somit unmittelbar finden. Wir fahren daher fort mit dem Fall, wo A mindestens eine vom Nullvektor verschiedene Spalte hat. Nehmen wir (der notationellen Einfachheit halber) an, dies sei die erste Spalte. Dann können wir mit einer Vertauschung von Zeilen (was die Lösungsmenge nicht verändert), die Matrix (A,b) so verändern, dass die Komponente in der linken oberen Ecke $\neq 0$ ist. Wir gehen also nun weiter davon aus, dass $a_{11} \neq 0$ ist.

Nun zum eigentlichen Eliminationsschritt: Wir verändern die Matrix (A,b) mit Hilfe von Zeilenoperationen Z3, so dass die erste Spalte keine weitere Komponente $\neq 0$ hat; wir "eliminieren" also x_1 aus den Gleichungen Nummer 2 bis m. Dies geht sehr einfach: Wir addieren das $(-a_{21}/a_{11})$-fache der ersten Zeile zur zweiten. Damit erhalten wir für die zweite Zeile

$$\begin{pmatrix} 0 & a_{22} - \frac{a_{21}}{a_{11}} a_{12} & \dots & a_{2n} - \frac{a_{21}}{a_{11}} a_{1n} & b_2 - \frac{a_{21}}{a_{11}} b_1 \end{pmatrix}.$$

Nun fahren wir entsprechend weiter mit der dritten, vierten bis zur letzten Zeile und erhalten die Matrix

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ 0 & a_{22} - \frac{a_{21}}{a_{11}} a_{12} & \dots & a_{2n} - \frac{a_{21}}{a_{11}} a_{1n} & b_2 - \frac{a_{21}}{a_{11}} b_1 \\ 0 & \vdots & & \vdots & \vdots \\ 0 & a_{m2} - \frac{a_{m1}}{a_{11}} a_{12} & \dots & a_{mn} - \frac{a_{m1}}{a_{11}} a_{1n} & b_m - \frac{a_{m1}}{a_{11}} b_1 \end{pmatrix}.$$

Wir betrachten nun die $(m-1) \times (n-1)$-Matrix

$$A^* := \begin{pmatrix} a_{22} - \frac{a_{21}}{a_{11}} a_{12} & \dots & a_{2n} - \frac{a_{21}}{a_{11}} a_{1n} \\ \vdots & & \vdots \\ a_{m2} - \frac{a_{m1}}{a_{11}} a_{12} & \dots & a_{mn} - \frac{a_{m1}}{a_{11}} a_{1n} \end{pmatrix}$$

und den Spaltenvektor

$$b^* := \begin{pmatrix} b_2 - \frac{a_{21}}{a_{11}} b_1 \\ \vdots \\ b_m - \frac{a_{m1}}{a_{11}} b_1 \end{pmatrix}.$$

Ist A^* die Nullmatrix, so ist das Eliminationsverfahren zu Ende, und sonst verfahren wir mit der Matrix (A^*, b^*) in gleicher Weise wie vorher mit der Matrix (A, b). Es ist offensichtlich, dass das Verfahren nach endlich vielen Schritten abbricht, wobei wir dann bei einer Matrix $\left(\overline{A}, \overline{b}\right)$ der folgenden Form angelangt sind:

$$\begin{pmatrix} 0 & \dots & 0 & \overline{a}_{1n_1} & \overline{a}_{1,n_1+1} & \dots & \dots & \dots & \dots & \dots & \overline{a}_{1n} & \overline{b}_1 \\ 0 & \dots & \dots & \dots & \dots & 0 & \overline{a}_{2n_2} & \dots & \dots & \dots & \overline{a}_{2n} & \overline{b}_2 \\ \vdots & & & & & & \ddots & \ddots & & & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \overline{a}_{k,n_k} & \dots & \overline{a}_{kn} & \overline{b}_k \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \overline{b}_{k+1} \\ \vdots & & & & & & & & & & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \overline{b}_m \end{pmatrix}$$

Die formale Beschreibung sieht wie folgt aus: Es ist $0 \le k \le n$, und $1 \le n_1 < \dots < n_k \le n$. Ist $k = 0$, so ist $\overline{A}$ die Nullmatrix. Ist $k \ge 1$, so ist für $1 \le j \le k$ die Komponente $\overline{a}_{j,n_j}$ die erste von Null verschiedene Komponente der j-ten Zeile. Für $j > k$ ist die j-te Zeile der Matrix $\overline{A}$ der Nullvektor. Es können jedoch durchaus einzelne oder alle der $\overline{b}_j$ für $j > k$ verschieden von 0 sein.

Wir können die Matrix noch etwas vereinfachen, was die nachfolgende Diskussion erleichtert: Durch Multiplikation von Zeilen mit Körperelementen $\neq 0$ (Operation Z2) können wir erreichen, dass für $1 \le j \le k$ die Komponenten $\overline{a}_{j,n_j} = 1$ sind. Ferner können wir durch nochmalige Anwendung von Z3 erreichen, dass für $2 \le j \le k$ in der n_j-ten Spalte oberhalb von $\overline{a}_{j,n_j} = 1$ nur Nullen stehen. Die Matrix sieht dann wie folgt aus:

$$\begin{pmatrix} 0 & \dots & 0 & 1 & \overline{a}_{1,n_1+1} & \dots & \overline{a}_{1,n_2-1} & 0 & \overline{a}_{1,n_2+1} & \dots & 0 & \dots & \overline{a}_{1n} & \overline{b}_1 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 & \overline{a}_{2,n_2+1} & \dots & 0 & \dots & \overline{a}_{2n} & \overline{b}_2 \\ \vdots & & & & & & & & & & \vdots & & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & \dots & \overline{a}_{kn} & \overline{b}_k \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \overline{b}_{k+1} \\ \vdots & & & & & & & & & & & & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \overline{b}_m \end{pmatrix}.$$

Wenn wir das Gleichungssystem auf diese Form gebracht haben

$$\sum_{j=1}^{n} \overline{a}_{ij} x_j = \overline{b}_i,\ 1 \leq i \leq m,$$

so lässt sich die Lösungsmenge einfach ablesen:

Fall 1: Es gilt $k < m$ und mindestens eine der Zahlen $\overline{b}_{k+1}, \ldots, \overline{b}_m$ ist $\neq 0$.

In diesem Fall hat das System offenbar keine Lösung. Es gilt also $L = \emptyset$, denn wenn $j \in \{k+1, \ldots, m\}$ ein Zeilenindex ist mit $\overline{b}_j \neq 0$, so ist die j-te Gleichung auf keine Weise erfüllbar.

Fall 2: Es gilt $k = m$ oder $\overline{b}_{k+1} = \ldots = \overline{b}_m = 0$.

In letzterem Fall können wir die Gleichungen Nr. $k+1$ bis Nr. m einfach weglassen, denn sie sind automatisch bei jeder Wahl der x-Werte erfüllt. Wir teilen unseren Fall nun in zwei Unterfälle auf:

Fall 2a: Es gilt $k = n$.

In diesem Fall muss $\overline{A}$ in der obigen Matrix nach dem Weglassen eventueller Zeilen $k+1$ bis m die sogenannte $n \times n$ **Einheitsmatrix** E_n sein:

$$\overline{a}_{ij} = \delta_{ij} := \begin{cases} 1, & \text{falls } i = j, \\ 0, & \text{falls } i \neq j, \end{cases} \tag{3.7}$$

oder als Matrix geschrieben

$$E_n \overset{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & & \vdots \\ 0 & 0 & \ddots & & \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}. \tag{3.8}$$

Wir haben oben das sogenannte Kronecker Deltasymbol δ_{ij} verwendet, das durch die zweite Gleichung in (3.7) definiert ist. Das Gleichungssystem ist damit ganz einfach geworden:

$$x_i = \overline{b}_i \text{ für } i = 1, 2, \ldots, k\,(= n)\,.$$

Es gibt also in diesem Fall *genau eine* Lösung, d.h.

$$L = \left\{ \left(\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_k \right) \right\}.$$

Fall 2b: $k < n$. In diesem Fall können die Variablen x_j mit $j \notin \{n_1, n_2, \ldots, n_k\}$ frei gewählt werden, und $x_{n_1}, x_{n_2}, \ldots, x_{n_k}$ ergeben sich daraus durch die Gleichungen

$$x_{n_i} = \overline{b}_i - \sum_{\substack{j=n_i+1 \\ j \notin \{n_{i+1}, \ldots, n_k\}}}^{n} \overline{a}_{ij} x_j.$$

Es gibt in diesem Fall unendlich viele Lösungen (falls K unendlich ist, wie z.B. $K = \mathbb{R}$), denn $n - k$ der x-Variablen, nämlich x_j mit $j \notin \{n_1, n_2, \ldots, n_k\}$ können nach Belieben gewählt werden. Auch im Fall, wo K endlich ist (z.B. $K = \mathbb{Z}_2$) gibt es mehr als eine Lösung. Wir sehen also, dass in diesem Fall das Gleichungssystem zwar lösbar, aber nicht eindeutig lösbar ist.

Wir machen ein Zahlenbeispiel (mit $K = \mathbb{R}$):

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 1, \\ 2x_1 + x_2 + x_3 &= 0, \\ 3x_1 + 2x_3 &= 4. \end{aligned}$$

Nach Elimination der x_1-Variablen aus der zweiten und der dritten Gleichung ergibt sich

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 1, \\ -3x_2 + 3x_3 &= -2, \\ -6x_2 + 5x_3 &= 1. \end{aligned}$$

Nun eliminieren wir x_2 aus der dritten Gleichung:

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 1, \\ -3x_2 + 3x_3 &= -2, \\ -x_3 &= 5. \end{aligned}$$

Auf die weitere Reduktion können wir verzichten: Die eindeutige Lösung lässt sich nun sofort ablesen: $x_3 = -5$, $x_2 = -13/3$, $x_1 = 14/3$. Wir modifizieren das erste Gleichungssystem nun ein wenig:

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 1, \\ 2x_1 + x_2 + x_3 &= 0, \\ 3x_1 + 3x_3 &= -1. \end{aligned}$$

Nach der Elimination von x_1 haben wir

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 1, \\ -3x_2 + 3x_3 &= -2, \\ -6x_2 + 6x_3 &= -4. \end{aligned}$$

Nun sieht man, dass die dritte Gleichung das zweifache der zweiten Gleichung ist. Nach Elimination von x_2 aus der dritten Gleichung fällt die letzte Gleichung daher einfach weg und wir erhalten:

$$\begin{aligned} x_1 + 2x_2 - x_3 &= 1, \\ -3x_2 + 3x_3 &= -2. \end{aligned}$$

Nun dividieren wir die zweite Gleichung noch durch -3 und eliminieren x_2 aus der ersten Gleichung. Wir erhalten dann

$$\begin{aligned} x_1 + 0x_2 + x_3 &= -1/3, \\ x_2 - x_3 &= 2/3. \end{aligned}$$

Wir sind damit im Fall 2a und erhalten als Lösungsmenge

$$L = \{(-1/3 - t, 2/3 + t, t) : t \in \mathbb{R}\}.$$

Man beachte, dass der Fall 2a nicht auftreten kann, wenn das System weniger Gleichungen als Unbekannte hat. Wir erhalten daher den folgenden

Satz 3.2 *Hat ein Gleichungssystem (3.3) weniger Gleichungen als Unbekannte, d.h. gilt $m < n$, so hat das System entweder gar keine Lösung oder mehr als eine Lösung.*

Wir betrachten noch etwas genauer den besonders wichtigen Spezialfall von gleich vielen Gleichungen wie Unbekannten, also $m = n$. In diesem Fall ist die Matrix A, wie man sagt, **quadratisch**, d.h. sie hat gleich viele Zeilen wie Spalten. Im Fall 2a lässt sich diese Matrix durch elementare Zeilenoperationen auf die Einheitsmatrix E_n transformieren, und das Gleichungssystem hat für jede Wahl der b_i genau eine Lösung. Diese Situation ist wichtig genug für eine Definition:

Definition 3.1 *Eine quadratische $n \times n$-Matrix A heisst **regulär**, falls sie sich durch elementare Zeilenoperationen auf die Einheitsmatrix E_n transformieren lässt. Ist A nicht regulär, so heisst sie **singulär.***

Aus der obigen Diskussion ergibt sich der folgende

Satz 3.3 *Wir betrachten das Gleichungssystem (3.3) mit $m = n$. Ist A regulär, so hat das Gleichungssystem für jede Wahl der b_i, $1 \leq i \leq n$ genau eine Lösung. Ist A singulär, so hat das System entweder gar keine Lösung oder mehr als eine Lösung.*

Der Satz hat die folgende interessante Konsequenz:

Korollar 3.1 *Hat das Gleichungssystem (3.3) mit $m = n$ für irgend eine spezielle Wahl der b_i genau eine Lösung, so ist A regulär und demzufolge hat das System für **jede** Wahl der b_i genau eine Lösung.*

Ein wichtiger Spezialfall ist $b_i = 0$, $\forall i$.

Definition 3.2 *Ein Gleichungssystem der Form*

$$\sum_{j=1}^{n} a_{ij}x_j = 0,\ i = 1, \ldots, m \tag{3.9}$$

heisst ***homogen.*** *Ist (3.3) ein Gleichungssystem mit beliebigen b_i, so heisst (3.9) das zu (3.3) gehörende homogene System.*

Ein homogenes Gleichungssystem hat offensichtlich immer mindestens eine Lösung, nämlich die sogenannte *triviale Lösung* $x_j = 0$, $1 \leq j \leq n$. Als Korollar aus Satz 3.2 erhalten wir im Fall von weniger Gleichungen als Unbekannte:

Korollar 3.2 *Ein homogenes Gleichungssystem mit $m < n$ hat mehr als eine Lösung.*

Beweis. Nach Satz 3.2 tritt der Fall einer eindeutigen Lösung nicht auf. Da aber ein homogenes System immer mindestens eine Lösung hat, nämlich die triviale, so bleibt nur der Fall übrig, dass das System mehr also eine Lösung hat (natürlich dann unendlich viele, wenn K unendlich ist). ■

Betrachten wir nochmals den Fall $m = n$, also gleich viele Gleichungen wie Unbekannte. Ein Spezialfall von Korollar 3.1 ist:

Korollar 3.3 *Wir betrachten das System (3.3) mit $m = n$. Dieses Gleichungssystem ist dann und nur dann eindeutig lösbar, wenn das zugehörige homogene System nur die triviale Lösung hat.*

Falls das zugehörige homogene System nicht nur die Triviallösung hat, so weiss man, dass (3.3) nicht eindeutig lösbar ist. Es sind dann aber immer noch zwei Fälle möglich, nämlich, dass es gar keine Lösung hat, oder dass es mehr als eine Lösung hat.

Es ist interessant, dass man von der Tatsache, dass das homogene System *höchstens* eine Lösung hat (nämlich die Triviallö sung), auf die (eindeutige) *Existenz* einer Lösung des inhomogenen Systems schliessen kann. Es gibt viele wichtige Beispiele von linearen Gleichungssystemen, bei denen man für das homogene System nachweisen kann, dass es nur die triviale Lösung besitzt, *ohne* dass man die Gauss-Elimination durchführt. In diesem Fall hat man also die *Existenz* einer Lösung des inhomogenen Systems nachgewiesen *ohne* deren explizite Berechnung. Mehr dazu in den Übungen.

3.2 Matrizenrechnung

Für das Rechnen mit Gleichungssystemen ist es bequem, eine Addition und eine Multiplikation von zwei Matrizen einzuführen. Wir betrachten hier Matrizen, deren Komponenten aus einem beliebigen aber fest gewählten Körper K sind.

Beide Operationen sind jedoch nur erklärt, wenn die beiden Matrizen, die zu addieren bzw. zu multiplizieren sind, gewissen Bedingungen genügen. Zunächst die **Addition**. Sie ist nur für zwei Matrizen des gleichen Typs erklärt, d.h. wenn die Anzahl der Zeilen und die Anzahl der Spalten bei beiden Matrizen die gleiche ist.

Definition 3.3 *$A = (a_{ij})$ und $B = (b_{ij})$ seien zwei $m \times n$-Matrizen. Dann ist die Summe $A + B$ wieder eine $m \times n$-Matrix:*

$$A + B = (a_{ij} + b_{ij})_{1 \leq i \leq m,\, 1 \leq j \leq n}\,.$$

Die Addition definiert man also einfach, indem man die Komponenten der Matrizen addiert.

Es gibt gute Gründe dafür, dass man bei der **Multiplikation** anders vorgeht. Zunächst ist sie nur definiert, wenn die Anzahl der Spalten der ersten Matrix gleich der Anzahl der Zeilen der zweiten Matrix ist:

Definition 3.4 *$A = (a_{ij})$ sei eine $m \times n$-Matrix und $B = (b_{ij})$ sei eine $n \times k$-Matrix. Dann ist die $m \times k$-Matrix $C = A \cdot B = (c_{ij})$ wie folgt definiert:*

$$c_{ij} := \sum_{t=1}^{n} a_{it} b_{tj},\ 1 \leq i \leq m,\ 1 \leq j \leq k.$$

Die Komponente i, j von $A \cdot B$ ergibt sich also, indem man die *Zeile* Nummer i der A-Matrix

$$\begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix}$$

und die *Spalte* Nummer j der B-Matrix

$$\begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix}$$

nimmt und die Komponenten dieser Vektoren sukzessive paarweise miteinander multipliziert und diese Produkte dann aufsummiert.

Hier ein Beispiel

$$A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 3 & -5 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 2 & 2 \\ 1 & -1 & 2 \end{pmatrix}.$$

$A \cdot B$ ist dann eine 2×3-Matrix:

$$A \cdot B = \begin{pmatrix} 8 & 1 & 11 \\ 0 & 11 & -5 \end{pmatrix}.$$

Man beachte, dass $B \cdot A$ nicht definiert ist, denn die Anzahl der Spalten von B ist nicht gleich der Anzahl der Zeilen von A. Im nachfolgenden Satz formulieren wir ein Reihe von elementaren Eigenschaften dieser Multiplikation. Wir lassen üblicherweise den $\cdot$ weg. Ferner verwenden wir die Konvention, dass "mal" stärker bindet als "plus".

Satz 3.4 *a) Ist A eine $m \times n$-, B eine $n \times k$- und C eine $k \times l$-Matrix, so gilt*

$$(AB)\,C = A\,(BC)\,.$$

b) Ist A eine $m \times n$-, und sind B, C $n \times k$- Matrizen, so gilt

$$A\,(B + C) = AB + AC.$$

c) Sind A, B zwei $m \times n$-Matrizen, und ist C eine $n \times k$- Matrix, so gilt

$$(A + B)\,C = AC + BC.$$

d) Ist A eine $m \times n$-Matrix, und sind E_m und E_n die durch (3.8) definierten Einheitsmatrizen, so gilt

$$E_m A = AE_n = A.$$

Beweis. Die Beweise folgen sofort aus den entsprechenden Assoziativ- und Distributivgesetzen der Multiplikation in K. Wir beweisen a). Die Beweise der anderen Aussagen seien dem Leser überlassen.

Wir betrachten die Komponente d_{ij} von $D := (AB)\,C$. Per Definition erhalten wir sie als

$$d_{ij} = \sum_{t=1}^{k} f_{it} c_{tj},$$

wobei f_{it} die entsprechende Komponente von AB ist, also

$$f_{it} = \sum_{s=1}^{n} a_{is} b_{st}.$$

Zusammen ergibt das

$$d_{ij} = \sum_{t=1}^{k} \left(\sum_{s=1}^{n} a_{is} b_{st} \right) c_{tj} = \sum_{s=1}^{n} a_{is} \left(\sum_{t=1}^{k} b_{st} c_{tj} \right)$$

nach den Assoziativ- und Distributivgesetzen in K. Die rechte Seite ist aber nichts anderes als die Komponente Nummer i, j von $A\,(BC)\,$. ■

Ein Spezialfall sind die quadratischen Matrizen. Wir bezeichnen die Menge der $n \times n$-Matrizen mit Komponenten aus K mit $M(n, K)$. Elemente in $M(n, K)$ können wir also stets addieren und multiplizieren.

Satz 3.5 *$M(n,K)$ versehen mit der Addition $+$ und der Matrizenmultiplikation $\cdot$ ist ein Ring mit Eins. Das Neutralelement der Addition ist die Nullmatrix (mit allen Komponenten 0) und das Neutralelement der Multiplikation ist die Einheitsmatrix E_n.*

Beweis. Das folgt sofort aus dem vorangegangen Satz. ■

Bemerkung 3.1 *Es ist sehr wichtig zu bemerken, dass der Ring $(M(n,K),+,\cdot)$* nicht *kommutativ ist (ausser natürlich für $n=1$). Dazu ein Beispiel*

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 7 & 10 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 4 & 11 \end{pmatrix}.$$

Es kann natürlich durchaus (auch für $n \geq 2$) für zwei Matrizen A und $B \in M(n,K)$ vorkommen, dass $AB = BA$ gilt. Ein triviales Beispiel ist $A = E_n$. Man sagt dann, dass A und B vertauschen. "In der Regel" vertauschen jedoch zwei Matrizen nicht. Wenn Sie zwei Matrizen "zufällig" auswählen, so werden diese typischerweise nicht vertauschen. (Der letzte Satz macht natürlich keinen mathematisch präzisen Sinn).

Wir bezeichnen die Nullmatrix auch einfach mit 0. Es sollte aus dem Kontext stets klar sein, ob mit 0 die Null im Körper oder die Nullmatrix gemeint ist.

Von besonderem Interesse in einem Ring sind die bezüglich der Multiplikation invertierbaren Elemente.

Definition 3.5 *Eine Matrix $A \in M(n,K)$ heisst **invertierbar**, wenn eine Matrix $B \in M(n,K)$ existiert mit*

$$AB = BA = E_n. \tag{3.10}$$

Diese zu A inverse Matrix wird dann meist mit A^{-1} bezeichnet. Die Menge aller invertierbaren $n \times n$-Matrizen wird mit $GL(n,K)$ bezeichnet. (GL steht für "general linear").

Bemerkung 3.2 *Die obige Definition setzt implizit voraus, dass die Inverse A^{-1} eindeutig ist. Hier das Argument: Sind B, B' zwei Matrizen, die (3.10) erfüllen, so gilt*

$$B = BE_n = B\left(AB'\right) = \left(BA\right)B' = E_nB' = B'.$$

Es ist keinesfalls so, dass alle von 0 verschiedenen Matrizen $A \in M(n,K)$ invertierbar sind. Betrachten wir etwa

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

Dann ist

$$A \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} b_{21} & b_{22} \\ 0 & 0 \end{pmatrix},$$

was natürlich unmöglich die Einheitsmatrix ist. Demzufolge ist A nicht invertierbar, obwohl es nicht die Nullmatrix ist.

E_n ist trivialerweise invertierbar, und es gilt $E_n^{-1} = E_n$.

Satz 3.6 *a)* $(GL(n,k),\cdot)$ *ist eine Gruppe. (Man nennt sie die allgemeine lineare Gruppe).*

b) Für $A, B \in GL(n,K)$ *gilt* $(AB)^{-1} = B^{-1}A^{-1}$.

c) Für $A \in GL(n,K)$ *ist* $A^{-1} \in GL(n,K)$ *und es gilt* $(A^{-1})^{-1} = A$.

Beweis. Wir müssen zeigen, dass $\cdot$ auf $GL(n,k)$ überhaupt definiert ist, denn bisher hatten wir nur gesehen, dass für $A, B \in M(n,K)$ das Produkt AB wieder eine $n \times n$-Matrix ist. Wir müssen also zeigen, dass für $A, B \in GL(n,K)$, das Produkt AB wieder invertierbar ist. Das ist jedoch sehr einfach: Wir weisen nach, dass $B^{-1}A^{-1}$ das Inverse davon ist (dann haben wir auch gleich b) bewiesen):

$$\begin{aligned} \left(B^{-1}A^{-1}\right)(AB) &= \left(B^{-1}\left(A^{-1}A\right)\right)B = \left(B^{-1}E_n\right)B \\ &= B^{-1}B = E_n, \end{aligned}$$

und

$$(AB)\left(B^{-1}A^{-1}\right) = E_n$$

geht genau gleich.

Damit ist zunächst gezeigt, dass $\cdot$ eine zweistellige Verknüpfung auf $GL(n,K)$ ist. Damit folgt jedoch nun sofort, dass $(GL(n,k),\cdot)$ eine Gruppe ist. Das Assoziativgesetz überträgt sich einfach von $M(n,K)$ her, E_n ist das Neutralelement, und jedes Element hat per Definition ein Inverses. Teil b) ist damit auch bewiesen und c) ist evident. ■

Ein sehr einfacher Spezialfall von quadratischen Matrizen sind **Diagonalmatrizen.** Dies sind Matrizen, die höchstens in der Diagonalen $i = j$ von Null verschiedene Elemente haben.

$$D = \begin{pmatrix} d_1 & 0 & \dots & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ 0 & 0 & d_3 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & d_n \end{pmatrix},$$

oder kurz mit dem Kronecker-Symbol.

$$D = (d_i \delta_{ij}).$$

Eine derartige Diagonalmatrix ist genau dann invertierbar, wenn alle Diagonalelement d_i von Null verschieden sind, und es ist dann

$$D^{-1} = \left(\frac{1}{d_i}\delta_{ij}\right).$$

Die Einheitsmatrix E_n ist die Diagonalmatrix mit $d_i = 1$.

Wir betrachten nun die Diskussion des Gleichungssystems (3.3) unter diesen Gesichtspunkten. Zunächst können wir es etwas kompakter schreiben. Dazu fassen wir das n-Tupel der Unbekannten x_i als Spaltenvektor auf

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

Wir können das natürlich auch als $n \times 1$-Matrix auffassen. Das Gleichungssystem (3.3) hat dann einfach die Form

$$Ax = b. \tag{3.11}$$

b ist hier der Spaltenvektor (3.6), den wir als $m \times 1$-Matrix auffassen. Das sieht nun genau wie der triviale Fall (3.1) aus, nur dass $a \in K$ durch die Matrix A ersetzt wird, und b wie auch die Unbekannten zu je einem Spaltenvektor zusammegefasst werden.

Wir können unsere im letzten Abschnitt eingeführten Zeilenoperationen ebenfalls als Matrizenmultiplikationen interpretieren. Zunächst Z1: Betrachten wir die $m \times m$-Matrix $Z^{i,j}$ die wie folgt gebildet ist: Sei e^k der Zeilenvektor, dessen k-te Komponente 1 ist und sonst 0

$$e^k := \begin{array}{ccccccccc} (0 & \dots & 0 & 1 & 0 & \dots & 0) \\ & & & \uparrow & & & \\ & & & k & & & \end{array}.$$

Die i-te Zeile der Matrix $Z^{i,j}$ ist e^j, die j-te ist e^i und für $k \neq i, j$ ist die k-te Zeile e^k. $Z^{i,j}$ ist also "fast" die Einheitsmatrix, nur steht in den Zeilen i und j die Eins jeweils an der vertauschten Stelle. Multiplizieren wir die Matrix A von links mit $Z^{i,j}$, so wird einfach die i-te Zeile von A mit der j-ten ausgetauscht. $Z^{i,j}b$ ist einfach der Spaltenvektor, dessen i-te mit der j-ten Komponente ausgetauscht sind. Man beachte, dass $Z^{i,j}$ invertierbar ist: Es gilt

$$Z^{i,j} \cdot Z^{i,j} = E_m,$$

d.h. $Z^{i,j}$ ist sein eigenes Inverses. Das Gleichungssystem (3.11) hat deshalb die gleiche Lösungsmenge wie das System

$$\left(Z^{i,j}A\right)x = Z^{i,j}b.$$

Die Zeilenoperation Z1 ist also nichts anderes als die Multiplikation des Systems von links mit einer dieser Z-Matrizen.

Nun zur Zeilenoperation Z2: Diese ist noch einfacher zu bewerkstelligen. Wir betrachten die $m \times m$-Diagonalmatrix $D^{i,\alpha}$ deren i-tes Diagonalelement die Zahl α ist und die anderen 1. Die Multiplikation des Gleichungssystems (3.11) von links mit $D^{i,\alpha}$,

$$D^{i,\alpha} A x = D^{i,\alpha} b,$$

ist dann nichts anderes, als dass die i-te Gleichung mit α multipliziert wird. Wiederum ist für $\alpha \neq 0$ die Matrix $D^{i,\alpha}$ invertierbar mit

$$\left(D^{i,\alpha}\right)^{-1} = D^{i,1/\alpha}.$$

Nun noch zur Zeilenoperation Z3: Addieren wir das α-fache der l-ten Zeile zur k-ten, so ist das einfach die Multiplikation von links mit der Matrix $M^{l,k,\alpha}$, die bis auf die k-te Zeile die Zeilen der Einheitsmatrix hat und deren k-te Zeile gleich

$$\begin{array}{cccccccccc} (0 & \dots & 0 & \alpha & 0 & \dots & 1 & & 0)\,. \\ & & & \uparrow & & & \uparrow & & \\ & & & l & & & k & & \end{array}$$

ist. Wiederum ist $M^{l,k,\alpha}$ invertierbar: Das Inverse ist einfach $M^{l,k,-\alpha}$.

Wir können nun die Definition 3.1 wie folgt in Matrizensprechweise übersetzen: Eine quadratische Matrix ist regulär (im Sinne dieser Definition), wenn sie durch Multiplikation von links mit Z-, D- oder M-Matrizen der obigen Form in die Einheitsmatrix überführt werden kann. Damit ergibt sich nun ziemlich einfach der folgende

Satz 3.7 *Eine quadratische Matrix A ist genau dann invertierbar, wenn sie regulär ist.*

Beweis. I) Wir setzen zunächst voraus, dass die Matrix A invertierbar ist. Dann hat das Gleichungssystem (3.11) die eindeutige Lösung $x = A^{-1}b$. Nach Satz 3.3 ist die Matrix A also regulär.

II) Wir setzen nun voraus, dass die Matrix A regulär ist. Gemäss der Diskussion vor der Formulierung des Satzes gibt es eine Matrix B, die als Produkt von Z-, D- oder M-Matrizen dargestellt werden kann, mit

$$BA = E_n.$$

Wegen Satz 3.6 ist B invertierbar. Daraus folgt

$$A = \left(B^{-1}B\right) A = B^{-1}\left(BA\right) = B^{-1},$$

also

$$AB = B^{-1}B = E_n.$$

Somit ist A invertierbar und die Inverse davon ist B. ■

Die Identifikation der Inversen einer quadratischen Matrix A mit der Matrix B des obigen Beweises führt auf ein bequemes Schema, um die Inverse "von Hand" auszurechnen. Ist A eine $n \times n$-Matrix, so bilden wir die $n \times 2n$-Matrix, indem wir die Einheitsmatrix E_n rechts an die Matrix anfügen:

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \dots & a_{1n} & 1 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \ddots & 0 \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & \dots & 0 & 1 \end{array}\right).$$

Nun führen wir elementare Zeilenoperationen durch, bis die linke Hälfte die Einheitsmatrix ist (oder bis das Verfahren vorher abbricht, in welchem Fall die Matrix A singulär ist). Dann steht in der rechten Hälfte die Inverse von A (falls man sich nicht verrechnet hat).

Zum Schluss noch eine Begriffsbildung, die später wichtig werden wird.

Definition 3.6 *a) Sei A eine $m \times n$-Matrix: $A = (a_{ij})$. Dann nennt man die $n \times m$-Matrix, die man durch Vetauschung der Zeilen und Spalten aus A erhält, die* ***transponierte Matrix*** *A^T von A: $A^T = \left(a'_{ij}\right)$, mit $a'_{ij} \stackrel{\text{def}}{=} a_{ji}$.*

b) Eine quadratische Matrix A heisst ***symmetrisch,*** *wenn $A^T = A$ gilt.*

Hier ein paar einfache Eigenschaften:

Satz 3.8 *a) Seien A eine $m \times n$-Matrix und B eine $n \times k$-Matrix, so gilt*

$$(AB)^T = B^T A^T.$$

b) Ist $A \in GL(n, K)$, so ist $A^T \in GL(n, K)$ und es gilt

$$\left(A^T\right)^{-1} = \left(A^{-1}\right)^T.$$

Beweis. a) B^T ist eine $k \times n$-Matrix und A^T eine $n \times m$-Matrix. Somit ist $B^T A^T$ definiert. Sei $D = (d_{ij}) \stackrel{\text{def}}{=} AB$ und $D^T = \left(d'_{ij}\right)$. Dann gilt

$$d'_{ij} = d_{ji} = \sum_k a_{jk} b_{ki} = \sum_k b'_{ik} a'_{kj},$$

mit der Notation $A^T = \left(a'_{ij}\right)$, $B^T = \left(b'_{ij}\right)$. Die rechte Seite der obigen Gleichung ist genau die ij-te Komponente von $B^T A^T$.

b) Nach a) gilt

$$\left(A^{-1}\right)^T A^T = \left(AA^{-1}\right)^T = E_n^T = E_n,$$

$$A^T \left(A^{-1}\right)^T = \left(A^{-1}A\right)^T = E_n^T = E_n.$$

Daraus folgt, dass $\left(A^{-1}\right)^T$ die Inverse von A^T ist. Insbesondere folgt auch, dass A^T invertierbar ist. ■

4 Vektorräume und lineare Abbildungen

4.1 Vektorräume

Dreidimensionale Vektoren können bekanntlich addiert werden (Parallelogrammregel) und mit reellen Zahlen ("Skalaren") gestreckt werden. Wir betrachten in diesem Kapitel Verallgemeinerungen dieser Situation. Zunächst können die reellen Zahlen durch Elemente eines beliebigen Körpers K ersetzt werden, z.B. $\mathbb{C}$, $\mathbb{Z}_2$. Wir nennen die Elemente des Körpers manchmal auch "Skalare".

Definition 4.1 *Eine nichtleere Menge V, versehen mit zwei zweistelligen Verknüpfungen*

$$V \times V \ni (v, w) \to v + w \in V,$$
$$K \times V \ni (\alpha, v) \to \alpha v \in V,$$

heisst ***K*-Vektorraum** *(oder einfach Vektorraum, falls klar ist, mit was für einem Körper man arbeitet), wenn die folgenden Vektorraumaxiome (V1)-(V5) erfüllt sind:*

V1 $(V, +)$ *ist eine abelsche Gruppe,*

V2
$$1v = v, \forall v \in V,$$

V3
$$\alpha(\beta v) = (\alpha\beta) v, \forall \alpha, \beta \in K, \forall v \in V,$$

V4
$$(\alpha + \beta) v = \alpha v + \beta v, \forall \alpha, \beta \in K, \forall v \in V,$$

V5
$$\alpha(v + w) = \alpha v + \alpha w, \forall \alpha \in K, \forall v, w \in V.$$

Die Elemente von V bezeichnet man üblicherweise als "Vektoren". Die Operation $+$ nennt man Vektoraddition, die von der Addition im Körper zu unterscheiden ist. Wir bezeichnen mit $-v$ das bezüglich der Addition inverse Element von $v \in V$. Die Axiome bedürfen einiger Erläuterungen. Zunächst bezeichnen wir jeweils mit 0 das Neutralelement der Addition in V, das existiert, da $(V, +)$ eine abelsche Gruppe ist. Dies sollte jedoch nicht mit dem Nullelement des Körpers verwechselt werden. In vielen Büchern werden Vektoren generell in der Notation besonders hervorgehoben, z.B. indem man $\overrightarrow{v}$, oder $\underline{v}$ für Elemente aus V schreibt. Der Nullvektor wäre entsprechend dann $\overrightarrow{0}$ oder $\underline{0}$. Dies führt jedoch zu einer Inflation von Notationen. Es ist aus dem Kontext *immer* klar, was für

eine Null in einer Formel steht. Der Leser sollte sich das jeweils genau überlegen. Entsprechende Unterscheidungen sind auch in (V2)-(V5) notwendig. Man muss insbesondere zwischen + als Verknüpfung der Körperelemente und + als Verknüpfung der Vektoren unterscheiden. So ist das Plus auf der linken Seite von (V4) die Addition in K und auf der rechten Seite die in V. In (V5) ist das Plus auf beiden Seiten die Verknüpfung in V. Ein Ausdruck der Form $\alpha + v$ mit $\alpha \in K$ und $v \in V$ ist hingegen nicht definiert. Ähnliche Unterscheidungen gibt es bei der Multiplikation. In (V2) wird auf der linken Seite zweimal die Multiplikation von Vektoren mit Skalaren verwendet, während auf der rechten Seite $\alpha\beta$ natürlich die Multiplikation in K ist. Das resultierende Körperelement wird anschliessend mit einem Vektor verknüpft. Eine Multiplikation von zwei Vektoren ist ebenfalls nicht definiert.

Einige einfache Folgerungen aus den Axiomen:

Proposition 4.1 *a)*

$$0v = 0,\ \forall v \in V.$$

Hier ist die Null auf der linken Seite die "Körper-Null" und auf der rechten Seite die "Vektorraum-Null"

b)

$$\alpha 0 = 0,\ \forall \alpha \in K.$$

(Hier ist die Null auf beiden Seiten natürlich die "Vektorraum-Null")

c)

$$(-1)\, v = -v,\ \forall v \in V.$$

Auf der linken Seite wird mit der -1 des Körpers multipliziert und auf der rechten Seite steht das inverse Element bezüglich der Addition in V.

d) Falls $\alpha v = 0$ gilt, so folgt $\alpha = 0$ oder $v = 0$.

Beweis. a)

$$\begin{aligned} 0v &= (0+0)\, v && \text{(Eigenschaft der Null in } K) \\ &= 0v + 0v && \text{(V4).} \end{aligned}$$

Addiert man auf beiden Seiten $-(0v)$, das inverse Element von $0v$ in V bezüglich der Vektorraumaddition, so folgt $0v = 0$.

b) geht analog.

c)

$$\begin{aligned} (-1)\, v + v &= (-1)\, v + 1v && \text{(V2)} \\ &= (-1+1)\, v && \text{(V4)} \\ &= 0v \\ &= 0 && \text{nach a).} \end{aligned}$$

d) Ist $\alpha \neq 0$ so folgt

$$v = 1v = \left(\frac{1}{\alpha}\alpha\right) v = \frac{1}{\alpha}(\alpha v) = \frac{1}{\alpha}0 = 0.$$

Die erste Gleichung gilt nach (V2), die zweite ist die Eigenschaft eines Inversen in K, die dritte folgt aus (V3), die vierte folgt aus der Voraussetzung und die letzte folgt aus b). ■

Sind $v_1, v_2, \ldots, v_n \in V$ und $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ so ist rekursiv

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = \sum_{i=1}^{n} \alpha_i v_i$$

definiert. Man nennt dies eine **Linearkombination** der v_i.

Beispiel 4.1 *Der einfachste Vektorraum ist der sogenannte* **0-*dimensionale Vektorraum***. *Er enthält nur ein Element, den* 0*-Vektor:* $V = \{0\}$.

Beispiel 4.2 *Sei* $n \in \mathbb{N}$ *und* K *sei ein beliebiger Körper. Dann ist der Raum der* n*-Tupel von Elementen von* K :

$$K^n := \{x = (x_1, x_2, \ldots, x_n) : x_i \in K\}$$

ein K*-Vektorraum. Wir definieren die Addition durch*

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) := (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

und die Multiplikation mit Skalaren durch

$$\alpha(x_1, x_2, \ldots, x_n) := (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

Man prüft sofort nach, dass die Vektorraumaxiome erfüllt sind.

K selbst wird auf diese Weise zu einem K-Vektorraum.

Beispiel 4.3 *Wir verallgemeinern das vorangegangene Beispiel: Sei M eine beliebige Menge. Dann definieren wir K^M als die Menge aller Funktionen $M \to K$:*

$$K^M := \{f : f : M \to K\}.$$

Wir definieren die Addition zweier Funktionen $f, g \in K^M$ durch

$$(f + g)(m) := f(m) + g(m)$$

und die Multiplikation mit Skalaren durch

$$(\alpha f)(m) := \alpha f(m).$$

Das Beispiel 4.2 ist der Spezialfall $M = \{1, \ldots, m\}$. Ein weiterer Spezialfall ist $M := \mathbb{N}$. Eine Funktion $\mathbb{N} \to K$ ist nichts anderes als eine Folge $(\alpha_i)_{i \in \mathbb{N}}$ von Elementen in K.

Beispiel 4.4 *Wir können uns auch auf spezielle Funktionen einschränken:*

$$V := \{f : f ist\ stetige\ Funktion\ \mathbb{R} \to \mathbb{R}\}$$

ist ebenfalls ein Vektorraum.

Beispiel 4.5 *Seien K, L zwei Körper mit $K \subset L$, wobei die Addition und die Multiplikation in K von Elementen in K mit den entsprechenden in L übereinstimmen. L heisst dann eine* ***Körpererweiterung*** *von K. Z.B. ist $\mathbb{R}$ eine Körpererweiterung von $\mathbb{Q}$ und $\mathbb{C}$ ist eine Körpererweiterung von $\mathbb{R}$ (und von $\mathbb{Q}$). In einem solchen Fall ist L ein K-Vektorraum: Die Addition ist die Addition in L und die Multiplikation von Elementen $x \in L$ mit "Skalaren" $\alpha \in K$ ist natürlich einfach die Multiplikation in L. Man prüft sofort nach, dass die Vektorraumaxiome gelten.*

Man muss jedoch aufpassen: $\mathbb{Z}_5$, das wir mit $\{0, 1, \ldots, 4\}$ identifizieren können, ist keine Körpererweiterung von $\mathbb{Z}_2$. $1 + 1 = 0$ gilt in $\mathbb{Z}_2$, aber nicht in $\mathbb{Z}_5$. Somit ist die obige Voraussetzung verletzt, dass die Verknüpfungen auf der kleineren Menge übereinstimmen.

Beispiel 4.6 *Sei $M(m, n, K)$ die Menge der $m \times n$-Matrizen mit Komponenten in K. (Zur Erinnerung: Wir hatten mit $M(n, K)$ die Menge der quadratischen $n \times n$-Matrizen bezeichnet). $M(m, n, K)$ ist ein K-Vektorraum. Addition und Multiplikation mit Skalaren sind auf die natürliche Weise definiert. Wir können die Komponenten einer Matrix natürlich einfach "der Reihe nach" aufschreiben. Dann ist eine $m \times n$-Matrix natürlich nichts anderes als ein Element in K^{nm}. In dieser Schreibweise gehen jedoch alle Aspekte, die mit der Multiplikation von Matrizen zusammenhängen, unter.*

Bemerkung 4.1 *Die folgende Bemerkung ist im Moment nicht allzu wichtig: Wie schon oben erwähnt, wird in einem K-Vektorraum nicht verlangt, dass Vektoren miteinander multipliziert werden können. Dennoch gibt es natürlich Vektorräume, wo eine Multiplikation der Vektoren definiert und wichtig ist. Beispiele sind etwa der $\mathbb{R}^3$ mit dem Ihnen wahrscheinlich bekannten Vektorprodukt, oder $M(n, K)$ mit dem Matrizenprodukt. Die Minimalforderung an ein solches Produkt, nennen wir es $*$, ist üblicherweise die sogenannte Bilinearität: Für $\alpha, \beta \in K$ und $u, v, w \in V$ soll*

$$(\alpha u + \beta v) * w = \alpha (u * w) + \beta (v * w)$$

gelten, und dasselbe im zweiten Argument des Produkts. Man prüft sofort nach, dass diese Eigenschaft in den beiden eben erwähnten Produkten erfüllt sind. Man nennt einen K-Vektorraum mit einem Produkt, das diese Eigenschaft erfüllt, eine ***K-Algebra.***

Das Vektorprodukt in $\mathbb{R}^3$ ist jedoch nicht assoziativ, erfüllt aber

$$u * v + v * u = 0$$

und die sogenannte ***Jacobi-Identität****:*

$$u * (v * w) + v * (w * u) + w * (u * v) = 0.$$

Eine K-Algebra mit diesen Eigenschaften nennt man eine ***Lie-Algebra****. Eine K-Algebra, deren Verknüpfung $*$ assoziativ ist, bezeichnet man als* ***assoziative K-Algebra.*** *Da nicht assoziative Algebren sehr wichtig sind, betont man die Assoziativität, falls sie vorliegt. $M(n, K)$ ist eine assoziative Algebra.*

Übung 4.1 *Zeigen Sie, dass $M(n, K)$ mit der Verknüpfung*

$$[A, B] := AB - BA$$

eine Lie-Algebra ist.

4.2 Unterräume

Definition 4.2 *V sei ein K-Vektorraum. Eine nichtleere Teilmenge $U \subset V$ heisst* ***Unterraum*** *(oder linearer Teilraum, oder auch linearer Unterraum), wenn die folgenden Axiome erfüllt sind:*

U1 *Für $u, v \in U$ gilt $u + v \in U$.*

U2 *Für $u \in U$ und $\alpha \in K$ gilt $\alpha u \in U$.*

Bemerkung 4.2 *Wir können die beiden Bedingungen in eine zusammenfassen:*

$$\alpha u + \beta v \in U, \text{ für } \forall \alpha, \beta \in K, \ \forall u, v \in U.$$

Beispiel 4.7 *Die beiden Koordinatenachsen $\{(x, 0) : x \in \mathbb{R}\}$ und $\{(0, y) : y \in \mathbb{R}\}$ sind Unterräume des $\mathbb{R}$-Vektorraums $\mathbb{R}^2$.*

Wir können dieses Beispiel noch weitgehend verallgemeinern.

Beispiel 4.8 *Wir betrachten ein homogenes lineares Gleichungssystem*

$$Ax = 0,$$

wobei A eine $m \times n$-Matrix ist. Dann ist der Lösungsraum

$$L := \{x \in K^n : Ax = 0\}$$

ein Unterraum von K^n. Das ist ganz einfach zu sehen: Sind x, y Lösungen des Systems und sind $\alpha, \beta \in K$, so ist $\alpha x + \beta y$ wegen

$$A(\alpha x + \beta y) = \alpha Ax + \beta Ay = 0$$

ebenfalls eine Lösung des Systems.

Es ist wichtig zu bemerken, dass die Lösungsmenge eines inhomogenen Systems kein Unterraum ist. Sind x, y Lösungen des Systems

$$Ax = b,$$

so gilt

$$A(\alpha x + \beta y) = (\alpha + \beta) b$$

und die rechte Seite ist natürlich im Allgemeinen ungleich b.

Satz 4.1 *Ist U ein Unterraum eines K-Vektorraums V, so ist U selbst ein K-Vektorraum.*

Beweis. Wir überzeugen uns zunächst davon, dass der Nullvektor von V ebenfalls in U liegt: Wir haben vorausgesetzt, dass U mindestens ein Element enthält, nennen wir es u. Dann ist wegen (U2) und Proposition 4.1 a)

$$0 = 0v \in U.$$

Zu $v \in U$ ist wegen (U2)

$$-v = (-1) v \in U,$$

die erste Gleichung nach 4.1 c).

Damit folgt nun, dass $(U, +)$ eine abelsche Gruppe ist, mit der von V übernommenen Addition. Die anderen der Vektorraumaxiome folgen nun sofort aus den entsprechenden in V. ■

Satz 4.2 *Sind U_1 und U_2 zwei Unterräume des Vektorraums V, so ist $U_1 \cap U_2$ ein Unterraum.*

Beweis. Es gilt

$$0 \in U_1 \cap U_2.$$

Somit ist $U_1 \cap U_2$ nicht leer.

Sind $\alpha, \beta \in K$ und $u, v \in U_1 \cap U_2$, so sind u, v sowohl aus U_1 wie aus U_2. Wegen der Unterraumeigenschaft dieser Mengen ist $\alpha u + \beta v$ sowohl in U_1 wie in U_2, und damit auch in $U_1 \cap U_2$. Damit ist der Satz bewiesen. ■

Im Gegensatz zum Durchschnitt ist die Vereinigung zweier Unterräume i.A. kein Unterraum. Ein einfaches Beispiel: Sei $U_1 := \mathbb{R} \times \{0\} \subset \mathbb{R}^2$, $U_2 := \{0\} \times \mathbb{R} \subset \mathbb{R}^2$. U_1 und U_2 sind natürlich Unterräume von $\mathbb{R}^2$, aber $U_1 \cup U_2$ ist kein Unterraum: $(1, 0)$ und $(0, 1)$ sind beide in $U_1 \cup U_2$, aber $(1, 1) = (1, 0) + (0, 1)$ ist es nicht.

Definition 4.3 *Seien $U_1, U_2, \ldots, U_n$ Unterräume des K-Vektorraums V. Dann ist die **Summe** dieser Unterräume definiert durch*

$$U_1 + U_2 + \ldots + U_n := \{u_1 + u_2 + \ldots + u_n : u_i \in U_i \; \forall i\}.$$

Satz 4.3 *Sind $U_1, U_2, \ldots, U_n$ Unterräume von V, so ist $U_1 + U_2 + \ldots + U_n$ ein Unterraum.*

Der ganz einfache Beweis sei dem Leser als Übungsaufgabe überlassen.

Ist U ein Unterraum von V, so können wir auf V die folgende Äquivalenzrelation definieren:

$$v_1 \sim v_2 \Longleftrightarrow v_2 - v_1 \in U.$$

Nach den Unterraumeigenschaften folgt sofort, dass dies eine Äquivalenzrelation ist. Wir können daher die Quotientenmenge $V/\sim$, d.h. die Menge der Äquivalenzklassen bezüglich dieser Äquivalenzrelation bilden. Die Äquivalenzrelation hat die folgende Eigenschaft: Sind $v_1, v_2, v_1', v_2' \in V$ mit $v_1 \sim v_2$, und $v_1' \sim v_2'$, und sind $\alpha, \beta \in K$, so gilt

$$\alpha v_1 + \beta v_2 \sim \alpha v_1' + \beta v_2'.$$

In der Tat ist

$$(\alpha v_1' + \beta v_2') - (\alpha v_1 + \beta v_2) = \alpha\,(v_1' - v_1) + \beta\,(v_2' - v_2) \in U$$

nach den Unterraumeigenschaften (U1) und (U2). Damit wird mit

$$[v_1] + [v_2] := [v_1 + v_2]$$

eine zweistellige Verknüpfung auf $V/\sim$ und mit

$$\alpha\,[v] := [\alpha v]$$

eine Verknüpfung von Skalaren mit Elementen von $V/\sim$ definiert.

Übung 4.2 *Prüfen Sie nach, dass $V/\sim$ mit diesen Verknüpfungen zu einem K-Vektorraum wird. Man nennt diesen K-Vektorraum den Quotientenraum und bezeichnet ihn üblicherweise mit V/U.*

4.3 Basis eines Vektorraums, Erzeugendensysteme, lineare Unabhängigkeit

Definition 4.4 *Sei V ein K-Vektorraum. Eine (endliche) **Basis** des Vektorraums ist ein n-Tupel $\mathcal{V} = (v_1, v_2, \ldots, v_n)$ von **Vektoren**, das die Eigenschaft hat, dass sich jeder Vektor $v \in V$ **eindeutig** als Linearkombination der v_i darstellen lässt, d.h. dass es zu jedem $v \in V$ genau ein n-Tupel $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K^n$ gibt mit*

$$v = \sum_{i=1}^{n} \alpha_i v_i.$$

*Hat ein Vektorraum eine (endliche) Basis, so heisst er **endlichdimensional.***

Eine Spitzfindigkeit: Wir achten bei einer Basis $\mathcal{V} = (v_1, v_2, \ldots, v_n)$ auf die Reihenfolge der Basiselemente v_i. Ist $\mathcal{V}$ eine Basis, so ist offensichtlich auch $(v_2, v_1, v_3, \ldots, v_n)$ eine Basis. Wir betrachten das aber als eine andere Basis. Dennoch sprechen wir manchmal etwas salopp davon, dass die Vektoren v_1, v_2, $\ldots$, v_n "eine Basis bilden". Das ist formal nicht ganz korrekt: Es ist das geordnete n-Tupel, das eine Basis ist.

Die Vektoren einer Basis müssen immer ungleich dem Nullvektor sein, denn mit dem Nullvektor in dem Satz von Vektoren kann natürlich eine Darstellung nicht eindeutig sein. Der einfachste Vektorraum, nämlich der Vektorraum $\{0\}$ enthält kein vom Nullvektor verschiedenes Element. Man sagt dann auch, dass dieser Vektorraum die Basis $\emptyset$ habe. Das ist aber nur eine (vernünftige) Konvention.

Im Rahmen dieser Vorlesung werden wir uns hauptsächlich mit endlichdimensionalen Vektorräumen beschäftigen. Zunächst ein wichtiges Beispiel: Wir betrachten den K-Vektorraum $V = K^n$. Für $1 \leq i \leq n$ betrachten wir die Vektoren $e_i := (\delta_{i1}, \delta_{i2}, \ldots, \delta_{in})$. Dieser Vektor hat also genau eine 1 an der i-ten Stelle und sonst Nullen. Dann ist $\mathcal{E} := (e_1, e_2, \ldots, e_n)$ eine Basis. In der Tat hat jeder Vektor $x = (x_1, x_2, \ldots, x_n) \in V = K^n$ die eindeutige Darstellung als

$$x = \sum_{i=1}^{n} x_i e_i.$$

Definition 4.5 $(e_1, e_2, \ldots, e_n)$ *heisst die* ***Standardbasis*** *von* K^n.

Es ist *sehr wichtig* zu bemerken, dass K^n nicht nur diese eine Basis hat, sondern *sehr viele* andere. Betrachten wir den einfachsten nichttrivialen Fall $\mathbb{R}^2$. Die Standardbasis besteht aus den Vektoren $(1, 0)$ und $(0, 1)$. Ich behaupte, dass z.B. auch die Vektoren $(1, 1)$, $(2, 3)$ eine Basis bilden. Um dies nachzuprüfen, müssen wir nur nachweisen, dass jeder Vektor $b = (b_1, b_2) \in \mathbb{R}^2$ eine eindeutige Darstellung als

$$b = \alpha_1 (1, 1) + \alpha_2 (2, 3)$$

hat. Das ist aber nichts anderes als ein Gleichungssystem für α_1, α_2. In der uns aus dem vorletzten Kapitel vertrauten Form können wir es sie folgt darstellen: Wir nehmen die Vektoren $(1, 1)$, $(2, 3)$ als Spaltenvektoren einer Matrix:

$$\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

Dann erhalten wir das Gleichungssystem für α_1, α_2 :

$$\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}.$$

Nun ist aber die Matrix $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ regulär, wie man sofort mit Gauss-Elimination nachprüft. Daher hat das obige Gleichungssystem für jede Wahl von b_1, b_2 genau eine Lösung. Dies ist aber nichts anderes als die Basiseigenschaft des Paars von Vektoren (als Spaltenvektoren geschrieben): $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

Es ist nun ziemlich offensichtlich, wie sich das verallgemeinert:

Satz 4.4 *Es seien $u_1, u_2, \ldots, u_n$ Vektoren in K^n. Wir schreiben sie als Spaltenvektoren*

$$u_j = \begin{pmatrix} u_{1j} \\ u_{2j} \\ \vdots \\ u_{nj} \end{pmatrix}.$$

$(u_1, u_2, \ldots, u_n)$ ist genau dann eine Basis von K^n wenn die Matrix $U := (u_{ij})$ regulär ist.

Beweis. $(u_1, u_2, \ldots, u_n)$ ist per Definition genau dann eine Basis von K^n, wenn jeder Vektor $b \in K^n$ (den wir als Spaltenvektor schreiben), eine eindeutige Darstellung als

$$b = \sum_{j=1}^{n} \alpha_j u_j$$

hat. Dies ist aber nichts anderes, als das folgende Gleichungssystem für die "Unbekannten" α_i

$$U \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = b.$$

Dieses Gleichungssystem hat nach Satz 3.3 genau dann eine eindeutige Lösung, wenn die Matrix regulär ist. ∎

Wir zeigen nun ganz allgemein, dass jede Basis eines Vektorraums V gleich viele Vektoren enthält:

Satz 4.5 *Sei V ein K-Vektorraum. Besitzt V eine Basis mit n Vektoren, so hat* jede *Basis von V n Vektoren.*

Beweis. Es seien $\mathcal{V} = (v_1, v_2, \ldots, v_m)$ und $\mathcal{U} = (u_1, u_2, \ldots, u_n)$ Basen von V. Wir zeigen zunächst $m \geq n$. Da wir die Rollen der Basen im untenstehenden Beweis vertauschen können, folgt dann auch $n \geq m$, was $m = n$ impliziert.

Aus der Basiseigenschaft von $\mathcal{V}$ folgt, dass jeder der Vektoren u_j eine Darstellung durch die v's hat:

$$u_j = \sum_{i=1}^{m} a_{ij} v_i, \quad 1 \leq j \leq n, \quad a_{ij} \in K \tag{4.1}$$

Sei $(x_1, x_2, \ldots, x_n) \in K^n$. Dann gilt

$$\sum_{j=1}^{n} x_j u_j = \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij} v_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} x_j \right) v_i. \tag{4.2}$$

Nach der Basiseigenschaft von $\mathcal{U}$ ist die einzige Möglichkeit, wie die linke Seite gleich dem Nullvektor ist, die Wahl $x_1 = x_2 = \ldots = x_n = 0$. Andererseits würde aus $m < n$ und Korollar 3.2 folgen, dass das homogene lineare Gleichungssystem

$$\sum_{j=1}^{n} a_{ij} x_j = 0, \quad \forall i. \tag{4.3}$$

eine nichttriviale Lösung hat, was implizieren würde, dass die rechte Seite von (4.2) mit einer nichttrivialen Wahl der x_i (d.h. nicht alle gleich Null) zu Null gemacht werden könnte. Da dies nicht möglich ist folgt $m \geq n$. ■

Ein endlichdimensionaler Vektorraum hat zwar keine eindeutige Basis; der Satz besagt jedoch, dass die Anzahl der Vektoren in einer Basis unabhängig von der speziellen Basis ist. Diese Anzahl ist also eine Grösse, die nur vom Vektorraum selbst abhängt.

Definition 4.6 *Für einen endlichdimensionalen Vektorraum V ist die Anzahl der für eine Basis benötigten Vektoren die* ***Dimension*** $\dim(V)$ *des Vektorraums. Ist der Vektorraum nicht endlichdimensional, so setzt man* $\dim(V) := \infty$. *Die Dimension des trivialen Vektorraum* $\{0\}$ *(der die Basis* $\emptyset$ *hat) ist* 0.

Beispiel 4.9 *Der K-Vektorraum K^n hat die Dimension n.*

Beispiel 4.10 ***Polynome****: In Verallgemeinerung der (formalen) Polynome, die in Kapitel 2 eingeführt wurden, können wir Polynome*

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

betrachten $a_i \in K$, mit der Konvention, dass $a_n \neq 0$ ist, falls $n \geq 1$ ist. n bezeichnet man dann als den ***Grad*** $\operatorname{grad}(p(x))$ *des Polynoms. Mit $K[x]$ bezeichnen wir die Menge aller Polynome, und mit $K_n[x]$ die Menge der Polynome vom Grad $\leq n$. $K[x]$ und $K_n[x]$ sind mit der üblichen Addition und Multiplikation durch Skalare beides K-Vektorräume. Eine Basis von $K_n[x]$ ist $(1, x, x^2, x^3, \ldots, x^n)$. Deshalb gilt* $\dim(K_n[x]) = n + 1$.

Zur weiteren Diskussion benötigen wir einige neue Begriffsbildungen.

Definition 4.7 *Sei V ein Vektorraum und $v_1, \ldots, v_n \in V$. Dann ist*

$$L[v_1, \ldots, v_n] := \left\{ \sum_{i=1}^{n} \alpha_i v_i : \alpha_1, \ldots, \alpha_n \in K \right\}$$

die ***lineare Hülle*** *der $v_1, \ldots, v_n$. Die lineare Hülle ist also einfach die Menge der Vektoren, die sich als Linearkombinationen der v_i's darstellen lassen. Per Konvention setzt man $L[\emptyset] := \{0\}$.*

Lemma 4.1 *$L[v_1, \ldots, v_n]$ ist ein Unterraum von V.*

Beweis. Seien $v = \sum_{i=1}^n \alpha_i v_i$ und $u = \sum_{i=1}^n \beta_i v_i$ zwei beliebige Elemente in $L[v_1, \ldots, v_n]$. Dann ist

$$v + u = \sum_{i=1}^{n} (\alpha_i + \beta_i) v_i \in L[v_1, \ldots, v_n]$$

und für $\lambda \in K$ ist

$$\lambda v = \sum_{i=1}^{n} (\lambda \alpha_i) v_i \in L[v_1, \ldots, v_n].$$

■

Definition 4.8 *$\mathcal{V} = (v_1, \ldots, v_n)$ heisst ein* ***Erzeugendensystem*** *von V, wenn $V = L[v_1, \ldots, v_n]$ gilt.*

$v_1, \ldots, v_n$ ist per Definition stets ein Erzeugendensystem von $L[v_1, \ldots, v_n]$. Jede Basis von V ist ein Erzeugendensystem von V. Für ein Erzeugendensystem wird jedoch nicht verlangt, dass die Darstellung als Linearkombination eindeutig ist. So ist z.B. $((1,0), (0,1), (1,1))$ ein Erzeugendensystem von $\mathbb{R}^2$, aber natürlich keine Basis. Die andere "Hälfte" der Basiseigenschaft wird mit dem folgenden *wichtigen* Begriff ausgedrückt:

Definition 4.9 *n Vektoren $v_1, \ldots, v_n \in V$ heissen* ***linear unabhängig****, wenn der Nullvektor $0 \in V$ keine nichttriviale Darstellung als Linearkombination der v_i hat, d.h. wenn*

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \Longrightarrow \alpha_i = 0 \text{ für alle } i \tag{4.4}$$

gilt. Sind die Vektoren nicht linear unabhängig, so heissen sie ***linear abhängig.***

Eine unendliche Teilmenge $(v_i)_{i \in I}$ von V heisst linear unabhängig, wenn jede endliche Teilmenge linear unabhängig ist, d.h. wenn für jedes $n \in \mathbb{N}$ und jede Auswahl $i_1, \ldots, i_n \in I$, die Vektoren $v_{i_1}, \ldots, v_{i_n}$ linear unabhängig sind.

Hier einige ganz einfache Folgerungen aus der Definition:

Proposition 4.2 *a) Ist einer der Vektoren v_i der Nullvektor, so sind $v_1, \ldots, v_n$ linear abhängig.*

b) Sind in $v_1, \ldots, v_n$ zwei Vektoren gleich, so sind $v_1, \ldots, v_n$ linear abhängig.

c) Jede Teilmenge einer linear unabhängigen Menge von Vektoren ist wieder linear unabhängig. (Per Konvention deklariert man auch die leere Menge als linear unabhängig.)

d) Ist $v \in V$ nicht der Nullvektor, so ist die Menge bestehend aus diesem einen Vektor linear unabhängig.

Beweis. a)-c) sind einfache Folgerungen aus der Definition. (Überprüfen Sie das!). d) folgt aus Proposition 4.1 d). ■

Satz 4.6 *$\mathcal{V} = (v_1, \ldots, v_n)$ ist genau dann eine Basis von V, wenn $\mathcal{V}$ ein Erzeugendensystem von V ist, und wenn die Vektoren $v_1, \ldots, v_n$ linear unabhängig sind.*

Beweis. Wir hatten schon gesehen, dass eine Basis ein Erzeugendensystem ist. Die lineare Unabhängigkeit folgt aus der geforderten *Eindeutigkeit* der Darstellung, was insbesondere (4.4) impliziert.

Wir zeigen nun umgekehrt, dass ein linear unabhängiges Erzeugendsystem $\mathcal{V}$ eine Basis ist. Sei $v \in V$ beliebig. Da $\mathcal{V}$ ein Erzeugendensystem ist, existieren $\alpha_1, \ldots, \alpha_n \in K$ mit

$$\sum_{i=1}^{n} \alpha_i v_i = v.$$

Wir müssen noch zeigen, dass diese Darstellung eindeutig ist. Sei also

$$\sum_{i=1}^{n} \alpha_i' v_i = v$$

eine zweite derartige Darstellung. Dann folgt

$$\sum_{i=1}^{n} (\alpha_i' - \alpha_i)\, v_i = 0.$$

Nach (4.4) ergibt sich $\alpha_i' - \alpha_i = 0$, $\forall i$, also $\alpha_i = \alpha_i'$ $\forall i$. Das ist die gewünschte Eindeutigkeit. ■

Satz 4.7 *Ist $\mathcal{V} = (v_1, \ldots, v_n)$ ein Erzeugendensystem des K-Vektorraums V, so ist V endlichdimensional und es existiert eine Basis von V, die aus einer Teilmenge dieser Vektoren besteht.*

Beweis. Sind $v_1, \ldots, v_n$ linear unabhängig, so ist $\mathcal{V}$ eine Basis und $\dim(V) = n$. Sind diese Vektoren nicht linear unabhängig, so existieren $\alpha_1, \ldots, \alpha_n$, nicht alle Null, mit $\sum_{i=1}^{n} \alpha_i v_i = 0$. Sei etwa $\alpha_n \neq 0$. (Wir nehmen den n-ten nur

der notationellen Bequemlichkeit halber, mit allen anderen geht das Argument genauso). Dann lässt sich v_n aus den anderen kombinieren:

$$v_n = \sum_{i=1}^{n-1} (-\alpha_i/\alpha_n)\, v_i.$$

Daraus folgt aber, dass auch $v_1, \ldots, v_{n-1}$ ein Erzeugendensystem von V ist: Ist w ein beliebiger Vektor in V, so lässt er sich, da $v_1, \ldots, v_n$ ein Erzeugendensystem ist, als

$$\begin{aligned} w &= \sum_{i=1}^{n} \beta_i v_i = \sum_{i=1}^{n-1} \beta_i v_i + \sum_{i=1}^{n-1} \frac{-\beta_n \alpha_i}{\alpha_n} v_i \\ &= \sum_{i=1}^{n-1} \left(\beta_i - \frac{\beta_n \alpha_i}{\alpha_n} \right) v_i \end{aligned}$$

darstellen. Das ist eine Darstellung von w als Linearkombination der $v_1, \ldots, v_{n-1}$.

Wir können in gleicher Weise mit dem Erzeugendensystem $(v_1, \ldots, v_{n-1})$ weiterfahren. Entweder ist dieser Satz von Vektoren linear unabhängig und damit eine Basis, oder wir können einen weiteren Vektor wegstreichen. In dieser Weise kann man weiterfahren, bis man zu einer Basis gelangt. ■

Lemma 4.2 *Seien $u_1, \ldots, u_m$ linear unabhängige Vektoren in einem Vektorraum V, die keine Basis bilden. Dann gibt es einen Vektor $v \in V$, sodass $u_1, \ldots, u_m, v$ linear unabhängig sind.*

Beweis. Wir betrachten den Unterraum $L[u_1, \ldots, u_m] \subset V$ ($L[\emptyset] = \{0\}$, falls $m = 0$). Da nach Voraussetzung, $u_1, \ldots, u_m$ keine Basis ist, folgt $L[u_1, \ldots, u_m] \neq V$. Demzufolge existiert $v \notin L[u_1, \ldots, u_m]$. Wir zeigen, dass $u_1, \ldots, u_m, v$ linear unabhängig sind. Sei $\sum_{i=1}^{m} \alpha_i u_i + \alpha_{m+1} v = 0$. Wäre $\alpha_{m+1} \neq 0$, so liesse v sich als Linearkombination der u's darstellen: $u_{m+1} = -\sum_{i=1}^{m} \frac{\alpha_i}{\alpha_{m+1}} u_i$, was aber wegen $v \notin L[u_1, \ldots, u_m]$ nicht möglich ist. Somit folgt $\alpha_{m+1} = 0$ und dann folgt wegen der angenommenen linearen Unabhängigkeit von $u_1, \ldots, u_m$, dass auch $\alpha_1 = \ldots = \alpha_m = 0$ gilt. Somit ist gezeigt, dass die $u_1, \ldots, u_m, v$ linear unabhängig sind. ■

Satz 4.8 *Seien $u_1, \ldots, u_m$ linear unabhängige Vektoren in einem Vektorraum V. Ist V endlichdimensional, so lassen sich diese Vektoren zu einer Basis ergänzen. Ist V unendlichdimensional, so lassen sie sich zu einer unendlichen Folge $u_1, \ldots, u_m, u_{m+1}, u_{m+2}, \ldots$ von linear unabhängigen Vektoren ergänzen.*

Beweis. Nach dem vorangegangenen Lemma können wir die Folge ergänzen. Entweder stossen wir nach einer endlichen Anzahl von Repetitionen der Konstruktion des Lemmas auf eine Basis oder die Konstruktion führt auf eine unendliche

Folge $(u_i)_{i\in\mathbb{N}}$ von Vektoren, die die Eigenschaft hat, dass $u_1, \ldots, u_n$ für jedes $n \in \mathbb{N}$ unabhängig sind. Damit folgt aber auch, dass jede endliche Teilmenge $u_{i_1}, \ldots, u_{i_m}$ linear unabhängig ist, denn zu diesen $i_1, \ldots, i_m$ existiert $n \in \mathbb{N}$ mit $i_1, \ldots, i_m \leq n$. Da eine Teilmenge eines Satzes von linear unabhängigen Vektoren wieder linear unabhängig ist (Proposition 4.2 c)), folgt, dass $u_{i_1}, \ldots, u_{i_m}$ linear unabhängig sind. ■

Als Folgerung aus den Sätzen 4.7 und 4.8 ergeben sich die folgenden drei Korollare:

Korollar 4.1 *Sei V ein Vektorraum, sei $\mathcal{V} = (v_1, \ldots, v_n)$ ein Erzeugendensystem von V und seien $u_1, \ldots, u_m$ linear unabhängig. Dann ist V endlichdimensional und es gilt*

$$n \geq \dim(V) \geq m.$$

Beweis. Die Aussage folgt unmittelbar aus den Sätzen 4.7 und 4.8. ■

Korollar 4.2 *Sei V ein K-Vektorraum mit $\dim V = n$.*
a) n linear unabhängige Vektoren in V bilden eine Basis.
b) Ein Erzeugendensystem mit n Vektoren bildet eine Basis.

Beweis. a): Wären die n Vektoren keine Basis, so könnten sie nach Satz 4.8 zu einer Basis mit mehr als n Vektoren ergänzt werden, was $\dim V = n$ widerspricht. b) folgt analog. ■

Korollar 4.3 *Sei U ein Unterraum des endlichdimensionalen K-Vektorraums V. Dann gilt:*
a) U ist endlichdimensional und es gilt $\dim(U) \leq \dim(V)$.
b) $\dim(U) = \dim(V)$ gilt genau dann, wenn $U = V$ ist.

Beweis. a) Dass U endlichdimensional ist, folgt sofort aus Satz 4.8, denn sonst würde eine unendliche Folge von linear unabhängigen Vektoren in U existieren, die auch linear unabhängig in V wären. Jede Basis in U ist auch linear unabhängig als Menge von Vektoren in V und lässt sich daher nach Satz 4.8 zu einer Basis in V ergänzen. Daraus folgt $\dim(U) \leq \dim(V)$.

b) Gilt $\dim(U) = \dim(V)$, so ist nach dem vorangegangen Korollar jede Basis in U auch eine Basis in V. ■

Als weitere Anwendung von Satz 4.8 erhalten wir den folgenden Satz über die Dimension von Unterräumen:

Satz 4.9 *Seien U_1 und U_2 zwei Unterräume des endlichdimensionalen K-Vektorraums V. Dann gilt*

$$\dim U_1 + \dim U_2 = \dim(U_1 \cap U_2) + \dim(U_1 + U_2).$$

Beweis. Sei $k := \dim(U_1 \cap U_2)$ und $m_i := \dim U_i$. Natürlich gilt $m_1, m_2 \geq k$. Wir beginnen mit einer Basis von $U_1 \cap U_2$, bestehend aus Vektoren $v_1, \ldots, v_k$. Nach Satz 4.8 können wir diese Basis zu einer Basis in U_1 ergänzen: $v_1, \ldots, v_k$, $v_{k+1}, \ldots, v_{m_1}$, und natürlich genausogut zu einer Basis in U_2 : $v_1, \ldots, v_k$, w_{k+1}, $\ldots, w_{m_2}$.

Wir zeigen nun, dass $v_1, \ldots, v_k, v_{k+1}, \ldots, v_{m_1}, w_{k+1}, \ldots, w_{m_2}$ eine Basis von $U_1 + U_2$ ist. Offensichtlich ist es ein Erzeugendensystem dieses Vektorraums. Wir müssen nur noch zeigen, dass diese Vektoren linear unabhängig sind. Betrachten wir also eine Linearkombination des Nullvektors mit diesen Vektoren:

$$0 = \sum_{i=1}^{m_1} \alpha_i v_i + \sum_{i=k+1}^{m_2} \beta_i w_i.$$

Anders geschrieben ist das

$$\sum_{i=k+1}^{m_2} \beta_i w_i = -\sum_{i=1}^{m_1} \alpha_i v_i.$$

Die linke Seite ist somit ein Vektor in U_1. Andererseits ist es aber auch ein Vektor in U_2 und somit ist es ein Vektor in $U_1 \cap U_2$. Er lässt sich also als Linearkombination der Vektoren $v_1, \ldots, v_k$ darstellen. Damit folgt $\alpha_{k+1} = \ldots = \alpha_{m_1} = 0$ und somit gilt

$$0 = \sum_{i=1}^{k} \alpha_i v_i + \sum_{i=k+1}^{m_2} \beta_i w_i$$

und wegen der linearen Unabhängigkeit von $v_1, \ldots, v_k, w_{k+1}, \ldots, w_{m_2}$ folgt, das auch die restlichen α's und die β's alle gleich 0 sind. ∎

4.4 Basiswechsel, Koordinaten

Wir schauen uns den Beweis des Satzes 4.5 noch unter einem etwas anderen Gesichtspunkt an. Es seien zwei Basen $\mathcal{V}$ und $\mathcal{U}$ eines Vektorraums V gegeben. Nach dem Beweis dieses Satzes lässt sich eine der Basen, sagen wir $\mathcal{U}$, durch die andere $\mathcal{V}$ wie folgt ausdrücken: Nach (4.1) mit $m = n$ ist

$$u_j = \sum_{i=1}^{n} a_{ij} v_i, \quad 1 \leq j \leq n. \tag{4.5}$$

Die Matrix $A = (a_{ij})$, eine quadratische Matrix, nennt man die **Matrix des Basiswechsels von $\mathcal{V}$ nach $\mathcal{U}$**. Etwas Vorsicht ist mit der Notation geboten: Die v_i und u_j sind hier Vektoren.

Beispiel 4.11 *Betrachten wir die Standardbasis* $\mathcal{V} = (e_1, \ldots, e_n)$ *in* K^n *und eine "neue" Basis* $\mathcal{U} = (u_1, \ldots, u_n)$, *mit den Vektoren*

$$u_i = \begin{pmatrix} u_{1i} \\ u_{2i} \\ \vdots \\ u_{ni} \end{pmatrix},$$

wie in Satz 4.4. Dann ist die (nach diesem Satz reguläre) Matrix U, *die die* u_i *als Spalten hat, die Matrix des Basiswechsels von der Standardbasis* $\mathcal{V}$ *nach der Basis* $\mathcal{U}$.

Der folgende Satz ist eine leichte Verallgemeinerung von Satz 4.4 in einer etwas abstrakteren Situation.

Satz 4.10 *Sind zwei Basen eines endlichdimensionalen Vektorraums gegeben, so ist die durch (4.5) definierte quadratische Matrix des Basiswechsels regulär. Ist umgekehrt* $\mathcal{V}$ *eine Basis und ist eine reguläre Matrix* $A = (a_{ij})$ *gegeben, so definiert (4.5) eine neue Basis* $\mathcal{U}$.

Beweis. Die Diskussion im Beweis des Satzes 4.5 zeigt, dass das homogene Gleichungssystem (4.3) genau dann nur die triviale Lösung hat, wenn die Vektoren $u_1, \ldots, u_n$ linear unabhängig sind, wenn sie also nach Korollar 4.2 eine Basis bilden. ■

Die Gleichung (4.5) drückt die Basis $\mathcal{U}$ durch die Basis $\mathcal{V}$ aus. Natürlich drückt sich dann die Basis $\mathcal{V}$ durch die Basis $\mathcal{U}$ mit der zu A inversen Matrix aus:

$$v_j = \sum_{i=1}^{n} a_{ij}^{(-1)} u_i,$$

$\left(a_{ij}^{(-1)}\right) = A^{-1}$. ($a_{ij}^{(-1)}$ ist die ij-te Komponente der Matrix A^{-1} und natürlich nicht $1/a_{ij}$).

Eine Basis $\mathcal{V}$ in einem Vektorraum V kann man auch als ein **Koordinatensystem** betrachten: Jeder Vektor $v \in V$ hat ja eine eindeutige Darstellung als

$$v = \sum_{i=1}^{n} x_i v_i.$$

Definition 4.10 *Die* $x_i \in K$ *in der obigen Darstellung heissen die* ***Koordinaten*** *des Vektors* v *bezüglich der Basis* $\mathcal{V}$.

Das n-Tupel der Koordinaten $x = (x_1, x_2, \ldots, x_n)$ ist also ein Element von K^n. Man bezeichnet dieses n-Tupel als den Koordinatenvektor (in K^n) von v

bezüglich der Basis $\mathcal{V}$. Wir erhalten also eine Abbildung $\phi_{\mathcal{V}} : V \to K^n$, die jedem Vektor seine Koordinaten zuweist. Diese Abbildung ist natürlich bijektiv: Jedem n-Tupel von Elementen in K kann man umgekehrt vermöge $\sum_{i=1}^{n} x_i v_i$ auch einen Vektor in V zuordnen, der gerade die Koordinaten $(x_1, x_2, \ldots, x_n)$ hat. Wir können den "abstrakten" Vektorraum V also via die Bijektion $\phi_{\mathcal{V}}$ mit dem "konkreten" Vektorraum K^n identifizieren. Es ist *äusserst wichtig* zu bemerken, dass diese Abbildung von der Wahl der Basis abhängig ist. Man soll sich daher davor hüten, sich jeden endlichdimensionalen Vektorraum gleich als K^n vorzustellen, denn diese Identifikation hängt von der Wahl der Basis ab und ist nicht — wie man sagt — *natürlich* gegeben.

Man beachte, dass in der Matrix A für den Basiswechsel von der Basis $\mathcal{V}$ nach der Basis $\mathcal{U}$, die *Spalten* der Matrix genau die Koordinaten der Vektoren der $\mathcal{U}$-Basis bezüglich der $\mathcal{V}$-Basis sind.

Wir untersuchen nun, in welcher Beziehung die Koordinaten *eines* festen Vektors bezüglich zweier verschiedener Basen stehen. Wir betrachten zwei Basen $\mathcal{U}$ und $\mathcal{V}$ wie oben, wobei sich die Basis $\mathcal{U}$ mit Hilfe der Matrix A und (4.5) durch die Basis $\mathcal{V}$ ausdrückt. Wir nennen $\mathcal{U}$ die "neue" Basis und $\mathcal{V}$ die "alte" (diese Bezeichnung hat natürlich keinerlei mathematische Bedeutung). Sei v ein beliebiger Vektor in V mit Koordinaten x_i bezüglich der alten Basis $\mathcal{V}$ und Koordinaten y_i bezüglich der neuen Basis $\mathcal{U}$. Es gilt also

$$v = \sum_{i=1}^{n} x_i v_i = \sum_{j=1}^{n} y_j u_j.$$

Nun ersetzen wir die neue Basis durch die alte gemäss (4.5) und erhalten

$$\sum_{i=1}^{n} x_i v_i = \sum_{j=1}^{n} y_j \sum_{i=1}^{n} a_{ij} v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} y_j \right) v_i.$$

Wegen der Eindeutigkeit der Darstellung eines Vektors als Linearkombination von Basisvektoren ergibt sich

$$x_i = \sum_{j=1}^{n} a_{ij} y_j, \quad i = 1, \ldots, n. \tag{4.6}$$

Die alten Koordinaten drücken sich also durch die neuen Koordinaten mit Hilfe der Matrix A aus. Wegen dieser Beziehung ist es übrigens besser, man stellt die Koordinaten als Spaltenvektor dar:

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^n.$$

Dann gilt in alter Matrizenschreibweise

$$x = Ay.$$

Satz 4.11 *Drückt sich eine Basis $\mathcal{U}$ durch eine Basis $\mathcal{V}$ mit (4.5) aus, so transformieren sich die Koordinaten gemäss $x = Ay$, wobei x die Koordinaten eines Vektors bezüglich der Basis $\mathcal{V}$ sind und y die bezüglich der Basis $\mathcal{U}$.*

Will man die Koordinaten der neuen Basis $\mathcal{U}$ aus denen der alten Basis $\mathcal{V}$ berechnen, so muss man die Matrix A invertieren: $y = A^{-1}x$.

Beispiel 4.12 *$V = K^n$ und $\mathcal{V}$ die Standardbasis. Ein Vektor*

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$$

hat bezüglich der Standardbasis (Definition 4.5) natürlich die Koordinaten $x_1, \ldots, x_n$. Bezüglich einer anderen Basis sind die Koordinaten jedoch ganz andere. Nehmen wir z.B. $\mathcal{U} = ((1,1),(2,3))$ in $\mathbb{R}^2$. $x = (2,1)$ hat bezüglich der Standardbasis die Koordinaten 2 und 1. In unserer anderen Basis gilt jedoch die Darstellung

$$(2,1) = 4\,(1,1) - (2,3)\,.$$

Demzufolge hat derselbe Vektor die Koordinaten 4 und -1 bezüglich $\mathcal{U}$.

Sei $\mathcal{U}$ eine beliebige Basis in K^n bestehend aus den (Spalten)Vektoren

$$u_i = \begin{pmatrix} u_{1i} \\ u_{2i} \\ \vdots \\ u_{ni} \end{pmatrix}.$$

Die Koordinaten eines beliebigen Vektors $x \in K^n$

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

bezüglich der Standardbasis, also die x_i selbst, ergeben sich aus den "neuen" Koordinaten $y_1, \ldots, y_n$ desselben Vektors x bezüglich der Basis $\mathcal{U}$ durch $x_i = \sum_{j=1}^{n} u_{ij} y_j$. Will man die neuen Koordinaten aus den alten berechnen, so muss man die Matrix U invertieren und erhält die Darstellung:

$$y_i = \sum_{j=1}^{n} u_{ij}^{(-1)} x_j.$$

Die Wahl einer speziellen Basis wird oft von konkreten Problemstellung abhängig gemacht und ist in der Regel nicht "natürlich" gegeben. Als Beispiel betrachten wir die Menge der Polynome $K_{n-1}[x]$ vom Grad $\leq n-1$. Der Einfachheit halber nehmen wir an, dass der Körper K unendlich ist. $K_{n-1}[x]$ ist ein K-Vektorraum der Dimension n, und eine Basis ist $(1, x, x^2, \ldots, x^{n-1})$. Eine für viele Zwecke "natürlichere" Basis kann wie folgt konstruiert werden. Seien $a_1, a_2, \ldots, a_n \in K$ fest gewählte und verschiedene Elemente. Man steht oft vor dem Problem, ein Polynom vom Grade $n-1$ zu finden, das auf diesen Körperelementen fest vorgegebene Werte annimmt. Um diese Aufgabe anzugehen, betrachten wir die sogenannten Interpolationspolynome

$$q_i(x) := \prod_{j:j\neq i} \frac{x - a_j}{a_i - a_j}.$$

Man beachte, dass diese Polynome alle vom Grad $n-1$ sind, denn das Produkt hat $n-1$ Faktoren.

Satz 4.12 *$(q_1(x), \ldots, q_n(x))$ ist eine Basis von $K_{n-1}[x]$. Ist $p(x)$ ein beliebiges Polynom in $K_{n-1}[x]$, so hat es die eindeutige Darstellung*

$$p(x) = \sum_{i=1}^{n} p(a_i)\, q_i(x).$$

(Hier ist $p(a_i) \in K$ der Wert des Polynoms an der Stelle a_i).

Beweis. Wir zeigen zunächst, dass die $q_i(x)$ linear unabhängig sind. Sei

$$\sum_{i=1}^{n} \alpha_i q_i(x) = 0,\ \alpha_i \in K$$

eine Darstellung des Nullpolynoms als Linearkombination der $q_i(x)$. Man beachte nun, dass $q_i(a_j) = \delta_{ij}$ gilt. Demzufolge gilt $\sum_{i=1}^{n} \alpha_i q_i(a_j) = \alpha_j$. Die obige Darstellung kann also nur gelten, wenn alle α_j gleich Null sind. Damit ist die lineare Unabhängigkeit gezeigt. Andererseits wissen wir, dass $K_{n-1}[x]$ die Dimension n hat. Aus Korollar 4.2 folgt also, dass $(q_1(x), \ldots, q_n(x))$ eine Basis ist. Wir wissen daher, dass jedes Polynom $p(x)$ genau eine Darstellung als

$$p(x) = \sum_{i=1}^{n} y_i q_i(x),\ y_i \in K,$$

hat. Einsetzen der a_j auf beiden Seiten ergibt $y_j = p(a_j),\ j = 1, \ldots, n.$ ■

$K_{n-1}[x]$ hat übrigens noch viele andere "natürliche" Basen, von denen die meisten spezielle Namen tragen, wie z.B. "Hermite-Polynome", "Tschebyscheff-Polynome" etc. Einige dieser Basen werden Ihnen im Laufe Ihres Studiums noch begegnen.

4.5 Anwendungen auf Matrizen und lineare Gleichungssysteme

Wir kommen nun zu einigen wichtigen Beispielen von Unterräumen von K^n. Es sei A eine $m \times n$-Matrix. Wir bezeichnen mit z_i die m Zeilenvektoren $\in K^n$ dieser Matrix:

$$z_i = (a_{i1}, \ldots, a_{in}) .$$

$L[z_1, \ldots, z_m]$ ist dann ein Unterraum von K^n.

Definition 4.11 *$L[z_1, \ldots, z_m]$ heisst der **Zeilenraum der Matrix.** Die Zahl* $\operatorname{rang}(A) := \dim(L[z_1, \ldots, z_m])$ *nennt man den **Rang** der Matrix A.*

Proposition 4.3 *a) Sei B eine $m \times m$-Matrix. Dann ist der Zeilenraum von BA ein Unterraum des Zeilenraumes von A. Insbesondere gilt*

$$\operatorname{rang}(BA) \leq \operatorname{rang}(A) .$$

b) Ist B regulär, so ist der Zeilenraum von A gleich dem Zeilenraum von BA. Insbesondere gilt

$$\operatorname{rang}(BA) = \operatorname{rang}(A) .$$

Beweis. a) Wir bezeichnen mit $\widetilde{z}_i$, $1 \leq i \leq m$, die Zeilen von BA. Diese Zeilenvektoren ergeben sich wie folgt:

$$\widetilde{z}_i = \sum_{j=1}^{m} b_{ij} z_j .$$

Somit lässt sich jeder Vektor, der sich als Linearkombination der Zeilen von BA schreiben lässt, $\sum_{i=1}^{m} \alpha_i \widetilde{z}_i$, $\alpha_i \in K$, auch als Linearkombination der Zeilen von A schreiben:

$$\sum_{i=1}^{m} \alpha_i \widetilde{z}_i = \sum_{i=1}^{m} \alpha_i \sum_{j=1}^{m} b_{ij} z_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{m} \alpha_i b_{ij} \right) z_j .$$

Somit folgt

$$L[\widetilde{z}_1, \ldots, \widetilde{z}_m] \subset L[z_1, \ldots, z_m] ,$$

woraus sich auch $\operatorname{rang}(BA) \leq \operatorname{rang}(A)$ ergibt.

b) folgt sofort aus a): $A = B^{-1}(BA)$ und Teil a). ∎

Mit Hilfe des Satzes 4.7 können wir den Rang einer Matrix noch etwas anders interpretieren:

Proposition 4.4 *Der Rang einer Matrix ist die maximale Anzahl linear unabhängiger Zeilenvektoren der Matrix.*

Beweis. Die Zeilen der Matrix A bilden natürlich ein Erzeugendensystem des Zeilenraums. Nach Satz 4.7 können wir durch eventuelles Weglassen von Zeilen zu einer Basis des Zeilenraums gelangen. Es gibt also $r = \operatorname{rang}(A)$ unabhängige Zeilen unter allen Zeilen der Matrix. Andererseits kann es auch nicht mehr geben, sonst wäre die Dimension des Zeilenraums $> r$. ■

Wir diskutieren nun einige Aspekte von linearen Gleichungssystemen unter den oben entwickelten Gesichtspunkten. Wir kommen zunächst auf die Gauss-Elimination aus dem letzten Kapitel zurück. Wir haben dort mit Hilfe von elementaren Zeilenoperationen eine beliebige $m \times n$-Matrix A auf die folgende Form gebracht:

$$\overline{A} = \begin{pmatrix}
0 & \dots & 0 & 1 & \overline{a}_{1,n_1+1} & \dots & 0 & \overline{a}_{1,n_2+1} & \dots & 0 & \dots & \dots \\
0 & \dots & 0 & 0 & \dots & \dots & 1 & \overline{a}_{2,n_2+1} & \dots & 0 & & \\
 & & & & & & 0 & & & \vdots & & \\
 & & & & & & \vdots & & & 0 & & \\
0 & \dots & & & & & & & 0 & 1 & \overline{a}_{k,n_k+1} & \dots \\
0 & 0 & \dots & \dots & \dots & \dots & \dots & & & 0 & \dots & 0 \\
\vdots & & & & & & & & & & & \vdots \\
0 & 0 & \dots & & & & & & & & & 0
\end{pmatrix}.$$

Die letzte von 0 verschiedene Zeile ist die k-te. Ich behaupte, dass die ersten k Zeilen dieser Matrix linear unabhängig sind. Um dies einzusehen, betrachten wir eine Linearkombination des Nullvektors (als Zeilenvektor) durch die ersten k Zeilen der obigen Matrix, nennen wir diese $\overline{z}_1, \dots, \overline{z}_k$:

$$\sum_{i=1}^{k} \alpha_i \overline{z}_i = (0, 0, \dots, 0)\,.$$

Die erste Zeile $\overline{z}_1$ hat die n_1-te Komponente 1. Alle anderen Zeilen haben diese Komponente gleich 0. Deshalb ist die n_1-te Komponente von $\sum_{i=1}^{k} \alpha_i \overline{z}_i$ einfach α_1. Analog ist die n_j-te Komponente von $\sum_{i=1}^{k} \alpha_i \overline{z}_i$ der Skalar α_j. Die obige Gleichung kann daher nur gelten, wenn $\alpha_1 = \dots = \alpha_k = 0$ ist. Wir haben somit gezeigt, dass die Zeilen $\overline{z}_1, \dots, \overline{z}_k$ linear unabhängig sind. Mehr unabhängige Zeilen kann es in der Matrix $\overline{A}$ jedoch nicht geben, denn die anderen Zeilen sind alle der Nullvektor. Demzufolge ist $\operatorname{rang}\left(\overline{A}\right) = k$. Wir wissen jedoch, dass sich $\overline{A}$ aus A durch Multiplikation von rechts mit einer regulären $m \times m$-Matrix B ergibt: $\overline{A} = BA$. Nach Proposition 4.3 folgt also:

Satz 4.13 *Für eine $m \times n$-Matrix A ist* $\operatorname{rang}(A)$ *gleich der vom Nullvektor verschiedenen Zeilen der Stufenmatrix nach einer Gauss-Elimination.*

Korollar 4.4 *Eine quadratische $n \times n$-Matrix A ist genau dann regulär, wenn* $\operatorname{rang}(A) = n$ *gilt.*

Bemerkung 4.3 *Wie wir schon aus dem letzten Kapitel wissen, ist eine quadratische Matrix genau dann regulär, wenn ihre Transponierte regulär ist. Das lässt sich verallgemeinern: Der Rang einer $m \times n$-Matrix ist gleich dem Rang ihrer Transponierten. Da Transponieren einfach Zeilen mit Spalten vertauscht sagt man auch, dass der Zeilenrang gleich dem Spaltenrang ist. Man kann das beweisen, indem man zeigt, dass die elementaren Zeilenoperationen den Spaltenrang nicht verändern. Das Resultat ergibt sich aber auch ganz einfach aus einer Überlegung im nächsten Abschnitt, sodass wir den Beweis besser noch etwas verschieben.*

Ein weiterer wichtiger Unterraum von K^n ist die Lösungsmenge eines *homogenen* Gleichungssystems

$$L = \{x \in K^n : Ax = 0\}, \tag{4.7}$$

wobei $A = (a_{ij})$ wieder eine $m \times n$-Matrix ist. Wir hatten im Beispiel 4.8 schon gesehen, dass das ein Unterraum von K^n ist. Wir wollen nun eine Basis dieses Unterraums finden. Dazu wenden wir wieder die Gauss-Elimination aus dem letzten Kapitel an und bringen das Gleichungssystem auf die Stufenform mit der obigen Matrix $\overline{A}$:

$$L = \left\{x \in K^n : \overline{A}x = 0\right\}$$

Die letzten $m - k$ Zeilen von $\overline{A}$ sind alle gleich dem Nullvektor. Die entsprechenden Gleichungen entfallen deshalb. Wie wir schon wissen, existiert im Falle $k = n$ nur die triviale Lösung. Der Lösungsraum ist also $L = \{0\}$ und die Dimension des Lösungsraums in 0. Ist $k < n$, so gibt es auch nichttriviale Lösungen. Der notationellen Einfachheit halber nehmen wir an, dass die Matrix A nach Durchführung der Gauss-Elimination (und nach Weglassen der letzten $m - k$ Zeilen, falls vorhanden) wie folgt aussieht:

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & \overline{a}_{1,k+1} & \dots & \overline{a}_{1,n} \\ 0 & 1 & 0 & & \vdots & \overline{a}_{2,k+1} & \dots & \overline{a}_{2,n} \\ 0 & 0 & 1 & & & \vdots & & \\ & & & & \vdots & & & \\ 0 & \dots & & \dots & 1 & \overline{a}_{k,k+1} & \dots & \overline{a}_{k,n} \end{pmatrix}.$$

Die Lösungsmenge des homogenen Gleichungssystems ist dann sehr einfach zu bestimmen: Wir können $x_{k+1}, \dots, x_n$ frei wählen und $x_1, \dots, x_k$ daraus ausrechnen:

$$x_i = \sum_{j=k+1}^{n} (-\overline{a}_{ij})\, x_j.$$

Wählen wir z.B. $x_{k+1} = 1$ und $x_j = 0$ für $j \geq k+2$, so erhalten wir den Lösungsvektor

$$x^{(k+1)} := \begin{pmatrix} -\overline{a}_{1,k+1} \\ \vdots \\ -\overline{a}_{k,k+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Analog erhalten wir für jedes $l \in \{k+1, \ldots, n\}$ Lösungsvektoren mit genau einer Eins für die Komponenten $k+1$ bis n und sonst 0 (für diese Komponenten).

$$x^{(l)} := \begin{pmatrix} -\overline{a}_{1,l} \\ \vdots \\ -\overline{a}_{k,l} \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \leftarrow l \\ \\ \\ \end{matrix} . \tag{4.8}$$

Aus der Diskussion des homogenen Gleichungssystems ergibt sich, dass der Lösungsraum L des Gleichungssystems die lineare Hülle der Vektoren $x^{(k+1)}$, …, $x^{(n)}$ ist:

$$L = L\left[x^{(k+1)}, \ldots, x^{(n)}\right].$$

Man sieht jedoch auch sehr leicht, dass die Vektoren $x^{(k+1)}, \ldots, x^{(n)}$ linear unabhängig sind: Eine Linearkombination der Form

$$\sum_{i=k+1}^{n} \alpha_i x^{(i)}, \quad \alpha_{k+1}, \ldots, \alpha_n \in K$$

hat nämlich einfach $\alpha_{k+1}, \ldots, \alpha_n$ als die Komponenten $k+1$ bis n (die anderen Komponenten sind natürlich komplizierter, was uns nicht zu interessieren braucht). Gilt daher $\sum_{i=k+1}^{n} \alpha_i x^{(i)} = 0$, so folgt $\alpha_{k+1} = \ldots = \alpha_n = 0$. Somit sind die Vektoren $x^{(k+1)}, \ldots, x^{(n)}$ linear unabhängig. Die Vektoren $x^{(l)}$, $k+1 \leq l \leq n$, bilden eine Basis des Lösungsraums (4.7) des homogenen Gleichungssystems. Da wir im vorangegangen Satz schon gesehen haben, dass k der Rang der Matrix A ist, erhalten wir:

Satz 4.14 *Die Dimension des Lösungsraums des homogenen Gleichungssystems $Ax = 0$ mit der $m \times n$-Matrix A ist $n - \operatorname{rang}(A)$.*

4.6 Lineare Abbildungen

Definition 4.12 *V und W seien zwei K-Vektorräume (es ist wichtig, dass der Grundkörper bei beiden derselbe ist). Eine Abbildung $f : V \to W$ heisst* ***linear,*** *wenn die folgende Eigenschaft gilt:*

Für alle Vektoren $u, v \in V$ und beliebige Skalare $\alpha, \beta \in K$ gilt

$$f(\alpha u + \beta v) = \alpha f(u) + \beta f(v).$$

Jede lineare Abbildung bildet den Nullvektor auf den Nullvektor ab. Das folgt sehr einfach:

$$f(0) = f(0 + 0) = f(0) + f(0).$$

Daraus folgt $f(0) = 0$.

Mit Induktion zeigt man auch sehr einfach, dass für $u_1, u_2, \ldots, u_n \in V$ und $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$

$$f\left(\sum_{i=1}^{n} \alpha_i u_i\right) = \sum_{i=1}^{n} \alpha_i f(u_i)$$

gilt.

Ist $\mathcal{U} = (u_1, \ldots, u_n)$ eine Basis von V so wird eine lineare Abbildung $f : V \to W$ durch die Funktionswerte $f(u_i) \in W$, $1 \leq i \leq n$ vollständig festgelegt: Da jeder Vektor $v \in V$ eine eindeutige Darstellung als Linearkombination der u_i hat, $v = \sum_{i=1}^{n} \alpha_i u_i$, so ergibt sich der Funktionswert $f(v)$ einfach als

$$f(v) = \sum_{i=1}^{n} \alpha_i f(u_i). \tag{4.9}$$

Umgekehrt kann man eine lineare Abbildung f dadurch definieren, dass man die Funktionswerte auf einer Basis vorgibt. Sind nämlich $w_1, \ldots, w_n$ beliebige Vektoren in W (nicht notwendigerweise linear unabhängig), so gibt es genau eine lineare Abbildung f mit $f(u_i) = w_i$, $1 \leq i \leq n$. Durch (4.9) wird nämlich eindeutig eine Abbildung $f : V \to W$ festgelegt. Man zeigt dann sehr leicht, dass diese Abbildung linear ist.

Beispiel 4.13 *Die Abbildung $f : \mathbb{R} \to \mathbb{R}$ gegeben durch $f(x) := ax$, $a \in \mathbb{R}$, ist linear. Die Abbildung f definiert durch $f(x) = ax + 1$ ist jedoch nicht linear.*

Beispiel 4.14 ***Lineare Abbildungen $K^n \to K^m$:*** *Sei A eine $m \times n$-Matrix mit Koeffizienten in einem Körper K. Dann wird durch $x \to Ax$ eine lineare Abbildung $K^n \to K^m$ definiert (x als Spaltenvektor geschrieben). Jede lineare Abbildung $K^n \to K^m$ entsteht auf diese Weise. Ist nämlich $f : K^n \to K^m$ eine beliebige lineare Abbildung, so ist sie durch ihre Werte auf der Standardbasis $(e_1, \ldots, e_n)$ in K^n vollständig bestimmt. Definieren wir die $m \times n$-Matrix A nun*

indem wir $f(e_j) \in K^m$ in die j-te Spalte schreiben, so erhalten wir für einen beliebigen Vektor $x \in K^n$ (als Spaltenvektor geschrieben):

$$f(x) = f\left(\sum_{i=1}^{n} x_j e_j\right) = \sum_{j=1}^{n} x_j f(e_j)$$
$$= \begin{pmatrix} \sum_{j=1}^{n} a_{1j} x_j \\ \sum_{j=1}^{n} a_{2j} x_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj} x_j \end{pmatrix} = Ax.$$

Beispiel 4.15 *Sie V der $\mathbb{R}$-Vektorraum der stetigen linearen Abbildungen $\phi : \mathbb{R} \to \mathbb{R}$. Dann ist*

$$V \ni \phi \to \int_0^1 \phi(x)\, dx \in \mathbb{R}$$

eine lineare Abbildung von V in den $\mathbb{R}$-Vektorraum $\mathbb{R}$.

Beispiel 4.16 *Sei V eine beliebiger endlichdimensionaler Vektorraum und $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis in V. Wir definieren die Abbildung $\phi_{\mathcal{V}} : V \to K^n$ indem wir jedem Vektor v seine Koordinaten bezüglich dieser Basis zuweisen (siehe die Diskussion nach der Definition 4.10). Diese Abbildung ist linear. Um dies einzusehen, betrachten wir zwei Vektoren $u, v \in V$ mit Koordinatenvektoren*

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \text{ bzw. } y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

bezüglich dieser Basis. Dann ist für $\alpha, \beta \in K$

$$\alpha u + \beta v = \alpha \left(\sum_{i=1}^{n} x_i u_i\right) + \beta \left(\sum_{i=1}^{n} y_i u_i\right)$$
$$= \sum_{i=1}^{n} (\alpha x_i + \beta y_i)\, u_i.$$

Somit ist der Koordinatenvektor von $\alpha u + \beta v$ gleich

$$\begin{pmatrix} \alpha x_1 + \beta y_1 \\ \vdots \\ \alpha x_n + \beta y_n \end{pmatrix} = \alpha x + \beta y.$$

Dies beweist die Behauptung.

Satz 4.15 *Sind $f : V \to W$ und $g : W \to X$ lineare Abbildungen zwischen den K-Vektorräumen V, W, X, so ist auch $g \circ f : V \to X$ eine lineare Abbildung.*

Beweis. Seien $\alpha, \beta \in K$, $u, v \in V$. Dann gilt

$$\begin{aligned}(g \circ f)(\alpha u + \beta v) &= g(f(\alpha u + \beta v)) = g(\alpha f(u) + \beta f(v)) \\ &= \alpha g(f(u)) + \beta g(f(v)) \\ &= \alpha (g \circ f)(u) + \beta (g \circ f)(v).\end{aligned}$$

■

Wir betrachten den Spezialfall $V = K^n$, $W = K^m$, $X = K^r$. Lineare Abbildungen $f : V \to W$ und $g : W \to X$ werden durch Matrizen A, B beschrieben: $f(x) = Ax$, $g(y) = By$ (x, y als Spaltenvektoren geschrieben). Dann wird die Komposition der Abbildungen einfach durch das Produkt der Matrizen beschrieben:

$$(g \circ f)(x) = BAx.$$

Lemma 4.3 *Sei $f : V \to W$ eine lineare Abbildung.*

a) Ist U ein Unterraum von V, so ist

$$f(U) := \{f(u) : u \in U\}$$

ein Unterraum von W.

b) Ist X ein Unterraum von W, so ist

$$f^{-1}(X) := \{v \in V : f(v) \in X\}$$

ein Unterraum von V. (Vorsicht: Wir setzen nicht voraus, dass eine Abbildung f^{-1} existiert. $f^{-1}(X)$ ist bloss eine Notation.)

Beweis. Wir beweisen b); a) geht genauso.

Seien $u, v \in f^{-1}(X)$ und $\alpha, \beta \in K$. Dann gilt

$$f(\alpha u + \beta v) = \alpha f(u) + \beta f(v) \in X,$$

weil $f(u)$, $f(v)$ in X sind und X ein Unterraum ist. ■

Definition 4.13 *Eine bijektive lineare Abbildung von V nach W heisst **(linearer) Isomorphismus**. Zwei Vektorräume heissen **isomorph**, wenn ein Isomorphismus zwischen ihnen existiert.*

Lemma 4.4 *a) Ist $f : V \to W$ ein Isomorphismus, so ist auch die Umkehrabbildung f^{-1} linear (und damit ebenfalls ein Isomorphismus).*

b) Sind $f : V \to W$ und $g : W \to X$ Isomorphismen, so ist auch $g \circ f$ ein Isomorphismus.

c) Ist $f : V \to W$ ein Isomorphismus und ist U ein Unterraum von V, so sind U und $f(U)$ isomorph. (Für die Definition von $f(U)$ siehe Lemma 4.3.)

d) Sei $f : V \to W$ eine lineare Abbildung und $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V. Ferner sei $w_i := f(v_i)$. f ist genau dann ein Isomorphismus, wenn $\mathcal{W} = (w_1, \ldots, w_n)$ eine Basis von W ist.

Beweis. a) Seien $u, w \in W$ und $\alpha, \beta \in K$. Dann ist

$$\begin{aligned} f\left(\alpha f^{-1}(u) + \beta f^{-1}(w)\right) &= \alpha f\left(f^{-1}(u)\right) + \beta f\left(f^{-1}(w)\right) \\ &= \alpha u + \beta w. \end{aligned}$$

Daraus folgt

$$\alpha f^{-1}(u) + \beta f^{-1}(w) = f^{-1}(\alpha u + \beta w).$$

b) $g \circ f$ ist eine Bijektion und linear und damit ein Isomorphismus.

c) Wir definieren die Restriktion $f|_U : U \to f(U)$ durch die Festsetzung $f|_U(u) := f(u)$ für $u \in U$. ($f|_U$ ist formal eine andere Abbildung als f, da sie auf einem anderen Vektorraum definiert ist, nämlich einem Unterraum von V). $f|_U$ ist offensichtlich linear und bildet U bijektiv auf $f(U)$ ab. Damit ist diese Abbildung ein Isomorphismus.

d) Ist $\mathcal{W}$ eine Basis, so definieren wir eine lineare Abbildung $g : W \to V$ durch $g(w_i) = v_i$. Dann ist $g \circ f$ eine lineare Abbildung $V \to V$ mit $(g \circ f)(v_i) = v_i$ für $1 \leq i \leq n$. Daraus folgt $g \circ f = \mathrm{id}_V$. Analog folgt $f \circ g = \mathrm{id}_W$.

Ist umgekehrt f ein Isomorphismus, so muss $\mathcal{W}$ ein Erzeugendensystem sein, denn jeder Vektor $w \in W$ lässt sich als $w = f(\sum_{i=1}^n \alpha_i v_i) = \sum_{i=1}^n \alpha_i w_i$ darstellen. Ferner sind die Vektoren in $\mathcal{W}$ linear unabhängig, denn aus $\sum_{i=1}^n \alpha_i w_i = \sum_{i=1}^n \alpha_i f(v_i) = f(\sum_{i=1}^n \alpha_i v_i) = 0$ folgt aus der Bijektivität von f die Gleichung $\sum_{i=1}^n \alpha_i v_i = 0$ und daraus wegen der Unabhängigkeit der v_i : $\alpha_1 = \ldots = \alpha_n = 0$. Damit ist gezeigt, dass $\mathcal{W}$ eine Basis ist. ■

Satz 4.16 *a) Ist V ein endlichdimensionaler K-Vektorraum mit Basis $\mathcal{V}$, so ist die Koordinatenabbildung $\phi_{\mathcal{V}}$ ein Isomorphismus.*

b) Zwei endlichdimensionale Vektorräume V, W derselben Dimension sind isomorph.

Beweis. a) $\phi_{\mathcal{V}}$ ist linear und bijektiv, wie wir schon gesehen haben, und damit ein Isomorphismus.

b) folgt aus Lemma 4.4 d): Ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis in V und $\mathcal{W} = (w_1, \ldots, w_n)$ eine Basis in W, so definieren wir die lineare Abbildung $f : V \to W$ durch $f(v_i) = w_i$. Nach Lemma 4.4 ist f ein Isomorphismus. ■

Es muss jedoch betont werden, dass dieser Isomorphismus *basisabhängig* definiert ist und nicht *natürlich* gegeben ist.

Bemerkung 4.4 *Wir können die Matrix einer Basistransformation, die wir in Abschnitt 4.4 eingeführt hatten, noch etwas anders interpretieren. Sind $\mathcal{V}$ und $\mathcal{U}$ zwei Basen desselben Vektorraums V der Dimension n, so definiert $\phi_{\mathcal{V}} \circ \phi_{\mathcal{U}}^{-1}$ einen Isomorphismus $K^n \to K^n$, der gemäss Beispiel 4.16 durch eine Matrix A beschrieben ist. Diese Matrix ist als darstellende Matrix eines Isomorphismus regulär — und natürlich nichts anderes als die Matrix der Basistransformation von $\mathcal{V}$ nach $\mathcal{U}$. Um dies einzusehen betrachten wir den i-ten Vektor e_i der Standardbasis von K^n. Ae_i ist dann einfach die i-te Spalte der Matrix A. Ferner ist*

$\phi_{\mathcal{U}}^{-1}(e_i) = u_i$, *der i-te Vektor der Basis* $\mathcal{U}$. *Demzufolge ist* $\phi_{\mathcal{V}} \circ \phi_{\mathcal{U}}^{-1}(e_i) = \phi_{\mathcal{V}}(u_i)$ *der Koordinatenvektor von* u_i *bezüglich der* $\mathcal{V}$*-Basis. Somit ist der i-te Spaltenvektor von A der Koordinatenvektor von* u_i *bezüglich der* $\mathcal{V}$*-Basis, was nichts anderes bedeutet als*

$$u_i = \sum_{j=1}^{n} a_{ji} v_j.$$

Sind V und W zwei K-Vektorräume, so bezeichnet wir mit $\hom(V, W)$ die Menge aller linearen Abbildungen $f : V \to W$. $\hom(V, W)$ ist dann selbst ein K-Vektorraum: Sind f und $g \in \hom(V, W)$, so definieren wir die Abbildung $f + g : V \to W$ durch $(f + g)(v) := f(v) + g(v)$. Um nachzuweisen, dass $f + g \in \hom(V, W)$ gilt, müssen wir die Linearität nachweisen: Seien $u, v \in V$ und $\alpha, \beta \in K$. Dann gilt

$$\begin{aligned}(f+g)(\alpha u + \beta v) &= f(\alpha u + \beta v) + g(\alpha u + \beta v) \\ &= \alpha f(u) + \beta f(v) + \alpha g(u) + \beta g(v) \\ &= \alpha (f+g)(u) + \beta (f+g)(v).\end{aligned}$$

Somit ist $\alpha f + \beta g$ tatsächlich linear und damit in $\hom(V, W)$. Der Nullvektor in $\hom(V, W)$ ist einfach die Nullabbildung $V \to W$, die jeden Vektor aus V auf den Nullvektor in W abbildet.

Lineare Abbildungen eines K-Vektorraums V auf sich selbst bezeichnet man manchmal auch als **Endomorphismen.** Wir schreiben $\hom(V)$ für den Vektorraum der Endomorphismen $f : V \to V$.

Ein anderer Spezialfall verdient besondere Beachtung, nämlich der Fall $W = K$.

Definition 4.14 $V^* := \hom(V, K)$ *ist der* ***Dualraum*** *des Vektorraums V.*

Der Dualraum von V ist also einfach der Vektorraum aller linearen Abbildungen $V \to K$. Ist V endlichdimensional mit einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$, so können wir sehr einfach eine Basis von V^* finden: Wir definieren für jedes i, $1 \leq i \leq n$ das Element $v_i^* \in V^*$ durch die Festlegung

$$v_i^*(v_j) = \delta_{ij}.$$

Vermittels

$$v_i^*\left(\sum\nolimits_{j=1}^{n} \alpha_j v_j\right) = \sum_{j=1}^{n} \alpha_j v_i^*(v_j) = \sum_{j=1}^{n} \alpha_j \delta_{ij} = \alpha_i$$

wird dadurch eine lineare Abbildung $V \to K$ definiert. Anders ausgedrückt: v_i^* ordnet jedem Vektor seine i-te Koordinate bezüglich der Basis $\mathcal{V}$ zu.

Satz 4.17 $\mathcal{V}^* = (v_1^*, \ldots, v_n^*)$ *ist eine Basis von* V^*. *Insbesondere gilt* $\dim(V^*) = \dim(V)$.

Beweis. Wir schreiben einen beliebigen Vektor $v \in V$ in seinen Koordinaten bezüglich $\mathcal{V}$:

$$v = \sum_{i=1}^{n} v_i^*(v) v_i.$$

Damit ist für jedes $f \in V^*$

$$f(v) = \sum_{i=1}^{n} v_i^*(v) f(v_i),$$

oder anders ausgedrückt:

$$f = \sum_{i=1}^{n} f(v_i)\, v_i^*.$$

Somit ist gezeigt, dass sich jedes Element in V^* als Linearkombination der v_i^* ausdrücken lässt, d.h. $(v_1^*, \ldots, v_n^*)$ ist ein Erzeugendensystem von V^*.

Wir müssen nun noch nachweisen, dass die $v_1^*, \ldots, v_n^*$ linear unabhängig sind. Sei also $0 = \sum_{i=1}^{n} \alpha_i v_i^*$, $\alpha_i \in K$, wobei auf der linken Seite der Nullvektor in V^*, also die Nullabbildung $V \to K$ steht. Insbesondere gilt für jedes $j \in \{1, \ldots, n\}$:

$$0 = \sum_{i=1}^{n} \alpha_i v_i^*(v_j) = \alpha_j.$$

Damit ist die lineare Unabhängigkeit gezeigt, und es folgt also, dass $(v_1^*, \ldots, v_n^*)$ eine Basis von V^* ist. ■

Der Satz 4.16 impliziert, dass ein endlichdimensionaler Vektorraum V isomorph zu V^* ist. Um einen Isomorphismus $V \to V^*$ zu konstruieren, wählen wir eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$ in V und die dazu duale Basis $\mathcal{V}^* = (v_1^*, \ldots, v_n^*)$ in V^*. Die Festlegung $f(v_i) = v_i^*$ definiert dann einen Isomorphismus. Dieser Isomorphismus ist jedoch *basisabhängig* konstruiert und nicht, wie man sagt, "natürlich" gegeben. Bei Wahl einer anderen Basis erhält man einen anderen Isomorphismus, wie man wie folgt sieht: Betrachten wir eine andere Basis $\mathcal{U} = (u_1, \ldots, u_n)$ von V mit der dazugehörigen Dualbasis $\mathcal{U}^* = (u_1^*, \ldots, u_n^*)$. Ferner sei dann ein Isomorphismus $g : V \to V^*$ durch $g(u_i) = u_i^*$ festgelegt. Wir stellen uns nun die Frage, ob $f = g$ ist. Dazu betrachten wir die reguläre Matrix der Basistransformation

$$u_i = \sum_{j=1}^{n} a_{ji} v_j.$$

Wie transfomieren sich die Dualbasen? Aus der obigen Basistransformation ergibt sich

$$v_k^*(u_i) = \sum_{j=1}^{n} a_{ji} v_k^*(v_j) = a_{ki}$$

und somit folgt

$$v_k^* = \sum_{i=1}^{n} a_{ki}\, u_i^*.$$

Kehren wir zur obigen Frage zurück, ob $f = g$ gilt, so sehen wir das folgende:

$$\begin{aligned}
f = g &\Longleftrightarrow f(u_i) = g(u_i) \quad \forall i \\
&\Longleftrightarrow \sum_{j=1}^{n} a_{ji}\, f(v_j) = \sum_{j=1}^{n} a_{ji} v_j^* = g(u_i) = u_i^* \quad \forall i \\
&\Longleftrightarrow \sum_{j=1}^{n} a_{ji} \sum_{l=1}^{n} a_{jl}\, u_l^* = \sum_{l=1}^{n} \left(\sum_{j=1}^{n} a_{ji} a_{jl} \right) u_l^* = u_i^* \quad \forall i \\
&\Longleftrightarrow \sum_{j=1}^{n} a_{ji} a_{jl} = \delta_{il} \quad \forall i, l \\
&\Longleftrightarrow A^T A = E_n.
\end{aligned}$$

Wir sehen also, dass $f = g$ nur bei ganz speziellen Basistransformation gilt. Im Allgemeinen gilt nämlich für eine reguläre Matrix $A^T A \neq E_n$. Reguläre Matrizen, für die $A^T A = E_n$ gilt, sind sehr speziell. Wir sehen also, dass der oben konstruierte Isomorphismus zwischen V und V^* von der gewählten Basis abhängt.

Matrizen, die die Bedingung $A^T A = E_n$ erfüllen, sind jedoch wichtig genug für eine spezielle Definition. Die Bedeutung solcher Matrizen (und der Zusammenhang mit der obigen Diskussion) wird erst viel später klar werden.

Definition 4.15 *Eine reguläre Matrix A heisst **orthogonal,** wenn $A^T A = E_n$ gilt. Die Menge aller orthogonalen $n \times n$-Matrizen (mit Komponenten aus K) bezeichnen wir mit $O(n, K)$.*

Bemerkung 4.5 *Die Bedingung impliziert natürlich, dass $A^{-1} = A^T$ ist. Man beachte, dass das Produkt zweier orthogonaler Matrizen A und B wieder orthogonal ist:*

$$(AB)^T (AB) = B^T A^T A B = B^T E_n B = B^T B = E_n.$$

*Ferner ist mit A auch A^{-1} orthogonal und E_n ist selbstverständlich orthogonal. $O(n, K)$ ist somit mit der Matrizenmultiplikation eine Gruppe (wie man sagt, eine **Untergruppe** der allgemeinen linearen Gruppe $GL(n, K)$).*

Ein Beispiel einer orthogonalen 2×2-Matrix (mit $K = \mathbb{R}$)

$$A = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}, \quad \phi \in [0, 2\pi].$$

Dann ist

$$\begin{aligned} A^T A &= \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\phi + \sin^2\phi & \cos\phi\sin\phi - \cos\phi\sin\phi \\ \cos\phi\sin\phi - \cos\phi\sin\phi & \cos^2\phi + \sin^2\phi \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Bemerkung 4.6 *Im Gegensatz zu der Situation mit V und V^* sind die V und der doppelduale Raum V^{**} in natürlicher Weise isomorph (sofern V endlichdimensional ist). Die Elemente von V^{**} sind die linearen Abbildungen $V^* \to K$. Wir können nämlich basisunabhängig eine Abbildung $\Phi : V \to V^{**}$ wie folgt definieren:*

$$\Phi(v)(f) := f(v),$$

für $v \in V$ und $f \in V^*$. $\Phi(v)$ ist offensichtlich eine Abbildung $V^* \to K$. Man muss jedoch einige Dinge nachweisen, was dem Leser als Übungsaufgabe überlassen sei:

- *Für jedes $v \in V$ ist $\Phi(v)$ eine **lineare** Abbildung $V^* \to K$. Ist dies gezeigt, so ist nachgewiesen, dass $\Phi(v)$ für jedes $v \in V$ ein Element in V^{**} ist. D.h. es ist nachgewiesen, dass Φ überhaupt eine Abbildung $V \to V^{**}$ definiert.*
- *Φ ist ein lineare Abbildung $V \to V^{**}$*
- *Φ ist bijektiv.*

Definition 4.16 *Sei $f : V \to W$ eine lineare Abbildung des K-Vektorraums V nach dem K-Vektorraum W.*

*a) Der **Kern** von f ist definiert durch*

$$\ker(f) := \{v \in V : f(v) = 0\}.$$

*b) Das **Bild** von f ist definiert durch*

$$\operatorname{im}(f) := \{f(v) : v \in V\} \subset W.$$

*c) $\dim(\operatorname{im}(f))$ bezeichnet man als den **Rang** von f.*

Beispiel 4.17 *Wir betrachten die Abbildung $f : K^n \to K^m$ aus Beispiel 4.14. Dann ist $\ker(f)$ einfach die Lösungsmenge des homogenen Gleichungssystems $Ax = 0$.*

Lemma 4.5 *a) $\ker(f)$ ist ein Unterraum von V.*

b) $\operatorname{im}(f)$ ist ein Unterraum von W.

Beweis. a) Seien $u, v \in \ker(f)$ und $\alpha, \beta \in K$. Dann gilt

$$f(\alpha u + \beta v) = \alpha f(u) + \beta f(v) = \alpha 0 + \beta 0 = 0.$$

b) Seien $w_1, w_2 \in \operatorname{im}(f)$. Dann existieren $v_1, v_2 \in V$ mit $w_i = f(v_i)$, $i = 1, 2$. Dann ist für $\alpha, \beta \in K$

$$\begin{aligned} \alpha w_1 + \beta w_2 &= \alpha f(v_1) + \beta f(w_2) \\ &= f(\alpha v_1 + \beta v_2) \in \operatorname{im}(f). \end{aligned}$$

■

Lemma 4.6 *Ein lineare Abbildung $f : V \to W$ ist genau dann injektiv, wenn* $\ker(f) = \{0\}$ *gilt. f ist genau dann surjektiv, wenn* $\operatorname{im}(f) = W$ *ist.*

Beweis. Die zweite Aussage ist trivial. Wir beweisen die erste: Ist f injektiv, so gilt natürlich $\ker(f) = \{0\}$. Wir beweisen die Umkehrung. Sei $\ker(f) = \{0\}$. Sind $u, v \in V$ mit $f(u) = f(v)$, so folgt wegen der Linearität

$$f(u - v) = f(u) - f(v) = 0,$$

und wegen $\ker(f) = \{0\}$ folgt dann $u = v$. Damit ist gezeigt, dass f injektiv ist.
■

Korollar 4.5 *Ein lineare Abbildung $f : V \to W$ ist genau dann ein Isomorphismus, wenn* $\ker(f) = \{0\}$ *und* $\operatorname{im}(f) = W$ *gelten.*

Satz 4.18 *Sei V ein endlichdimensionaler K-Vektorraum,* $\dim V = n$, *und $f : V \to W$ sei eine lineare Abbildung. Dann gilt*

$$n = \dim(\ker(f)) + \dim(\operatorname{im}(f)).$$

Beweis. Sei $d := \dim(\ker(f))$, und $(u_1, \ldots, u_d)$ eine Basis von $\ker(f)$. Nach dem Basisergänzungssatz 4.8 können wir dies zu einer Basis in V ergänzen: $(u_1, \ldots, u_d, u_{d+1}, \ldots, u_n)$. Wir betrachten die $n - d$ Vektoren $f(u_{d+1}), \ldots, f(u_n)$.

1. Schritt: $(f(u_{d+1}), \ldots, f(u_n))$ ist ein Erzeugendensystem von $\operatorname{im}(f)$: Jeder Vektor $w \in \operatorname{im}(f)$ hat eine Darstellung $w = f(u)$, $u \in V$. Jeder Vektor $u \in V$ lässt sich aber als Linearkombination der u_i darstellen: $u = \sum_{i=1}^{n} \alpha_i u_i$. Damit folgt

$$\begin{aligned} w = f\left(\sum_{i=1}^{n} \alpha_i u_i\right) &= \sum_{i=1}^{n} \alpha_i f(u_i) \\ &= \sum_{i=d+1}^{n} \alpha_i f(u_i). \end{aligned}$$

2. Schritt: Die Vektoren $f(u_{d+1}), \ldots, f(u_n)$ sind linear unabhängig: Sei $\sum_{i=d+1}^{n} \alpha_i f(u_i) = 0$. Daraus folgt $f\left(\sum_{i=d+1}^{n} \alpha_i u_i\right) = 0$. Somit ist $\sum_{i=d+1}^{n} \alpha_i u_i \in \ker f$. Wegen der Basiseigenschaft von $(u_1, \ldots, u_d, u_{d+1}, \ldots, u_n)$ und der Voraussetzung, dass $(u_1, \ldots, u_d)$ eine Basis von $\ker f$ ist, folgt $\alpha_{d+1} = \ldots = \alpha_n = 0$. ■

Wir kommen nun nochmals auf Matrizen und ihren Rang zurück, den wir mit Hilfe des obigen Satzes neu interpretieren können. Sei also A eine $m \times n$-Matrix. Wie wir schon gesehen haben, können wir diese Matrix als lineare Abbildung $K^n \to K^m$ interpretieren. $\mathrm{im}(A)$ ist dann einfach der von den Spaltenvektoren von A aufgespannte Unterraum. Nach Satz 4.18 und Satz 4.14 folgt dann

$$\begin{aligned} \dim(\mathrm{im}(A)) &= n - \dim(\ker(A)) \\ &= \mathrm{rang}(A). \end{aligned}$$

Wir haben also den folgenden Satz bewiesen:

Satz 4.19 *Ist A eine $m \times n$-Matrix, so ist der Rang der Matrix gleich der Dimension des von den Spalten aufgespannten Unterraums von K^m. ("Zeilenrang=Spaltenrang")*

Eine andere einfache Aussage über den Rang ist

Lemma 4.7 *Sei A eine $m \times n$-Matrix und B ein $n \times k$-Matrix. Dann gilt*

$$\mathrm{rang}(AB) \leq \min(\mathrm{rang}(A), \mathrm{rang}(B)).$$

Beweis. Offensichtlich ist $\mathrm{im}(AB)$ ein Unterraum von $\mathrm{im}A$ und somit folgt

$$\mathrm{rang}(AB) \leq \mathrm{rang}(A).$$

Andererseits ist $\ker B$ ein Unterraum von $\ker(AB)$, woraus $\dim(\ker B) \leq \dim(\ker(AB))$ folgt, was nach Satz 4.14

$$\mathrm{rang}(AB) \leq \mathrm{rang}(B)$$

impliziert. Damit ist das Lemma bewiesen. ■

Dieses Lemma hat die folgende etwas überraschende Konsequenz.

Proposition 4.5 *Sie A eine quadratische $n \times n$-Matrix, die ein Rechtsinverses hat. D.h. es existiert eine $n \times n$-Matrix B mit $AB = E_n$. Dann ist A invertierbar und es gilt $B = A^{-1}$. Die gleiche Aussage gilt, wenn A ein Linksinverses besitzt.*

Beweis. Aus dem vorangegangen Lemma folgt

$$\min\left(\operatorname{rang}\left(A\right),\operatorname{rang}\left(B\right)\right)\geq n,$$

was aber nur möglich ist, wenn A und B Rang n haben. Somit ist A invertierbar und es folgt

$$\begin{aligned} B &= E_nB = \left(A^{-1}A\right)B = \\ &= A^{-1}\left(AB\right) = A^{-1}E_n = A^{-1}. \end{aligned}$$

Wenn A ein Linksinverses besitzt, so geht der Beweis genau analog. ■

Die Aussage der Proposition ist insofern etwas erstaunlich, als allgemein in Ringen keinesfalls richtig ist, dass die Existenz eines Rechtsinversen für ein Element des Ringes impliziert, dass dieses Element invertierbar ist.

Ein wichtiges Anliegen in der Mathematik ist oft die Klassifikation von Objekten nach "Verwandtschaftsverhältnissen". Betrachten wir etwa zwei vorgegebene K-Vektorräume V und W. Wir möchten wissen, wieviele "substantiell verschiedene" lineare Abbildungen $V\to W$ es gibt. Ein naheliegendes Verfahren ist das folgende: Wir definieren eine Äquivalenzrelation auf $\hom\left(V,W\right)$. Sind $f,g\in\hom\left(V,W\right)$, d.h. lineare Abbildungen $V\to W$, so setzen wir $f\sim g$ falls Isomorphismen $\psi:V\to V$ und $\sigma:W\to W$ existieren mit

$$\sigma\circ f=g\circ\psi, \tag{4.10}$$

oder

$$f=\sigma^{-1}\circ g\circ\psi$$

Übung 4.3 *Überzeugen Sie sich davon, dass dies eine Äquivalenzrelation auf* $\hom\left(V,W\right)$ *definiert.*

Wir deklarieren nun zwei Elemente von $\hom\left(V,W\right)$ als "wesentlich verschieden", wenn sie nicht äquivalent sind, wenn sie also nicht zur gleichen Äquivalenzklassen gehören. Wieviele Äquivalenzklassen gibt es? Nicht sehr viele:

Satz 4.20 *Zwei lineare Abbildungen* $f,g\in\hom\left(V,W\right)$ *sind genau dann äquivalent, wenn sie denselben Rang haben.*

Beweis. Wir setzen zunächst voraus, dass (4.10) gilt. Da ψ ein Isomorphismus ist und insbesondere bijektiv, folgt

$$\operatorname{im}\left(f\right)=\left\{\sigma^{-1}\left(v\right):v\in\operatorname{im}\left(g\right)\right\}=\sigma^{-1}\left(\operatorname{im}\left(g\right)\right),$$

in der Notation von Lemma 4.3. Nach Lemma 4.4 c) folgt, dass $\operatorname{im}\left(f\right)$ und $\operatorname{im}\left(g\right)$ isomorph sind und damit dieselbe Dimension haben.

Wir beweisen nun umgekehrt, dass aus

$$\dim(\operatorname{im}(f)) = \dim(\operatorname{im}(g))$$

folgt, dass Isomorphismen σ und ψ existieren, sodass (4.10) gilt. Zunächst folgt mit Hilfe von Satz 4.18, dass auch die Dimensionen d der Kerne übereinstimmen. Wir wählen zunächst eine Basis $(u_1, \ldots, u_d)$ in $\ker(f)$ und eine Basis $(v_1, \ldots, v_d)$ in $\ker(g)$. Diese Basen können wir zu Basen in ganz V ergänzen: $(u_1, \ldots, u_d, u_{d+1}, \ldots, u_n)$ und $(v_1, \ldots, v_d, v_{d+1}, \ldots, v_n)$. Wir definieren $w_i := f(u_{d+i})$, $1 \leq i \leq n-d$ und $x_i := g(v_{d+i})$, $1 \leq i \leq n-d$. Nach dem Beweis von Satz 4.18 ist $(w_1, \ldots, w_{n-d})$ eine Basis von $\operatorname{im}(f)$ und $(x_1, \ldots, x_{n-d})$ ist eine Basis von $\operatorname{im}(g)$. Wir können diese Basen zu Basen in W ergänzen: $(w_1, \ldots, w_{n-d}, w_{n-d+1}, \ldots, w_m)$ und $(x_1, \ldots, x_{n-d}, x_{n-d+1}, \ldots, x_m)$. Wir definieren nun einen Isomorphismus $\psi : V \to V$ durch $\psi(u_i) = v_i$ für $i = 1, \ldots, n$ und einen Isomorphismus $\sigma : W \to W$ durch $\sigma(w_i) = x_i$ für $i = 1, \ldots, m$. Dass dies Isomorphismen sind, folgt aus Lemma 4.4 d). Dann gilt

$$\begin{aligned}(g \circ \psi)(u_i) &= g(v_i) = 0 \\ &= (\sigma \circ f)(u_i), \quad 1 \leq i \leq d,\end{aligned}$$

und

$$\begin{aligned}(g \circ \psi)(u_i) &= g(v_i) = x_i \\ &= \sigma(w_i) = (\sigma \circ f)(u_i), \quad d+1 \leq i \leq n.\end{aligned}$$

Demzufolge stimmen $g \circ \psi$ und $\sigma \circ f$ auf allen Basisvektoren u_i überein, und somit gilt (4.10). ■

Es muss hier schon im Hinblick auf spätere Diskussionen bemerkt werden, dass die Situation für Endomorphismen $V \to V$ sich anders darstellt. Zwei Endomophismen $f, g \in \hom(V)$ definiert man als "im wesentlichen gleich", falls **ein** Isomorphismus $\psi : V \to V$ existiert mit

$$f \circ \psi = \psi \circ g.$$

Dies definiert ebenfalls eine Äquivalenzrelation auf $\hom(V)$. Die Äquivalenzklassen sind jedoch hier *sehr* viel schwieriger zu diskutieren. Dieses Problem wird uns noch detailliert beschäftigen.

4.7 Darstellende Matrix einer linearen Abbildung

Wir hatten schon im letzten Abschnitt gesehen, dass eine lineare Abbildung $f : V \to W$ vollständig durch die Funktionswerte auf einer Basis von V festgelegt sind. Betrachten wir eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$ von V und eine Basis $\mathcal{W} =$

$(w_1, \ldots, w_m)$ von W. Die Funktionswerte $f(v_i)$ sind dann Vektoren in W, und wir können daher die Koordinaten dieser Vektoren bezüglich der Basis $\mathcal{W}$ berechnen:

$$f(v_i) = \sum_{j=1}^{m} a_{ji} w_j. \tag{4.11}$$

Die $m \times n$-Matrix A erhalten wir also, indem wir den Koordinatenvektor von $f(v_i)$ bezüglich der Basis $\mathcal{W}$ in die i-te Spalte von A setzen.

Definition 4.17 *A heisst die **darstellende Matrix** von f bezüglich der Basen $\mathcal{V}$ und $\mathcal{W}$.*

Wir schreiben auch manchmal A_f. Es muss jedoch immer im Auge behalten werden, dass diese Matrix von der Wahl der Basen abhängt. Wir können also bei fest vorliegenden Basen $\mathcal{V}$ und $\mathcal{W}$ jeder linearen Abbildung $f \in \hom(V, W)$ eine $m \times n$-Matrix zuordnen. Umgekehrt definiert auch jede $m \times n$-Matrix A via (4.11) eine lineare Abbildung. Die Zuordnung $\hom(V, W) \ni f \to A_f \in M(n, m, K)$ ist, wie man leicht nachprüft, linear ($M(n, m, K)$ ist ein K-Vektorraum, siehe Beispiel 4.6) und damit ein Isomorphismus. Dieser Isomophismus ist jedoch nicht *natürlich* gegeben, sondern hängt von der Wahl der Basen ab.

Wir betrachten kurz den Spezialfall $V = K^n$, $W = K^m$. Eine lineare Abbildung $V \to W$ wird einfach durch eine $m \times n$-Matrix A beschrieben: $K^n \ni x \to Ax \in K^m$. A ist dann einfach die darstellende Matrix bezüglich der Standardbasen in K^n bzw. K^m : Ist e_j der j-te (Spalten)Vektor der Standardbasis, so ist Ae_j einfach die j-te Spalte von A, was natürlich gleich $\sum_{i=1}^{m} a_{ij} e_i$ ist.

Wir können die darstellende Matrix einer linearen Abbildung $f : V \to W$ bezüglich zweier Basen $\mathcal{V}$ und $\mathcal{W}$ noch etwas anderes interpretieren. Wie wir im letzten Abschnitt gelernt haben, führt die Wahl einer Basis $\mathcal{V}$ in V zum Isomorphismus $\phi_{\mathcal{V}} : V \to K^n$, der jedem Vektor seine Koordinaten bezüglich dieser Basis zuordnet. Dann ist die darstellende Matrix von f bezüglich Basen $\mathcal{V}$ in V und $\mathcal{W}$ in W einfach durch die lineare Abbildung $\phi_{\mathcal{W}} \circ f \circ \phi_{\mathcal{V}}^{-1} : K^n \to K^m$ gegeben. Ist nämlich $(e_1, \ldots, e_n)$ die Standardbasis in K^n, so gilt $v_j = \phi_{\mathcal{V}}^{-1}(e_j)$ und $\left(\phi_{\mathcal{W}} \circ f \circ \phi_{\mathcal{V}}^{-1}\right)(e_j)$ ist dann einfach der Komponentenvektor von $f(v_j)$ bezüglich der Basis $\mathcal{W}$, d.h. die j-te Spalte der darstellenden Matrix.

Satz 4.21 *Seien $f : V \to W$ und $g : W \to X$ lineare Abbildungen. Seien ferner Basen $\mathcal{V}$, $\mathcal{W}$ und $\mathcal{X}$ in den K-Vektorräumen V, W bzw. X gegeben. Dann gilt*

$$A_{g \circ f} = A_g A_f, \tag{4.12}$$

wobei die darstellenden Matrizen jeweils bezüglich der entsprechenden Basen genommen werden.

Beweis. Nach der vorherigen Diskussion ist $A_{g\circ f}$ die durch die Abbildung $\phi_{\mathcal{X}} \circ (g \circ f) \circ \phi_{\mathcal{V}}^{-1}$ zwischen den Koordinatenräumen definierte Matrix. Es gilt aber

$$\phi_{\mathcal{X}} \circ (g \circ f) \circ \phi_{\mathcal{V}}^{-1} = \left(\phi_{\mathcal{X}} \circ g \circ \phi_{\mathcal{W}}^{-1}\right) \circ \left(\phi_{\mathcal{W}} \circ f \circ \phi_{\mathcal{V}}^{-1}\right),$$

was in Matrixsprechweise die Gleichung (4.12) ist. ■

Korollar 4.6 *Sei $f : V \to W$ eine lineare Abbildung und $\mathcal{V}$ und $\mathcal{W}$ seien Basen von V bzw. von W. Dann ist f genau dann ein Isomorphismus, wenn A_f quadratisch und regulär ist, und es gilt $A_{f^{-1}} = A_f^{-1}$.*

Beweis. Ist f ein Isomorphismus mit inverser Abbildung f^{-1}, so gilt nach dem vorangegangenen Satz

$$A_f A_{f^{-1}} = A_{f^{-1}} A_f = E,$$

woraus folgt, dass A_f regulär ist mit Inverser $A_{f^{-1}}$.

Ist A_f quadratisch und regulär, so gilt $\dim V = \dim W$ und die Abbildung $K^{\dim V} \ni x \mapsto A_f x \in K^{\dim V}$ ist ein Isomorphismus. Demzufolge ist auch $f = \phi_{\mathcal{W}}^{-1} \circ A_f \circ \phi_{\mathcal{V}}$ ein Isomorphismus. ■

Um die Sache noch etwas komplizierter zu machen, untersuchen wir nun, was mit der darstellenden Matrix passiert, wenn wir die Basen in den entsprechenden Vektorräumen ändern. Wir betrachten also zu den Basen $\mathcal{V}$ und $\mathcal{W}$, jeweils in V und W, in diesen beiden Vektorräumen zwei "neue" Basen $\mathcal{V}' = (v_1', \ldots, v_n')$ und $\mathcal{W}' = (w_1', \ldots, w_m')$, mit regulären Matrizen der Basistransformationen: $T = (t_{ij}) \in GL(n, K)$ für die Transformation von $\mathcal{V}$ nach $\mathcal{V}'$:

$$v_j' = \sum_{i=1}^{n} t_{ij} v_i,$$

und $S = (s_{ij}) \in GL(m, K)$ für die Transformation von $\mathcal{W}$ nach $\mathcal{W}'$:

$$w_j' = \sum_{i=1}^{m} s_{ij} w_i.$$

Die Matrix der Basistransformation von $\mathcal{W}'$ nach $\mathcal{W}$ ist dann einfach $S^{-1} = \left(s_{ij}^{(-1)}\right)$. Sei weiter $f \in \hom(V, W)$ und A sei die darstellende Matrix bezüglich der Basen $\mathcal{V}$ und $\mathcal{W}$, während B die darstellende Matrix bezüglich der Basen $\mathcal{V}'$ und $\mathcal{W}'$ sei. In welcher Beziehung stehen diese Matrizen? Hier die Antwort:

Satz 4.22

$$B = S^{-1} A T. \tag{4.13}$$

Beweis. Nach Bemerkung 4.4 ist die Matrix der Basistransformation von $\mathcal{V}$ nach $\mathcal{V}'$ durch $\phi_{\mathcal{V}} \circ \phi_{\mathcal{V}'}^{-1} : K^n \to K^n$ gegeben und analog für die Basistransformation von $\mathcal{W}$ nach $\mathcal{W}'$. Wir schreiben zur Verdeutlichung $A_{f,\mathcal{V},\mathcal{W}}$ für die darstellende Matrix bezüglich der Basen $\mathcal{V}$ und $\mathcal{W}$. Dann gilt

$$\begin{aligned} B = A_{f,\mathcal{V}',\mathcal{W}'} &= \phi_{\mathcal{W}'} \circ f \circ \phi_{\mathcal{V}'}^{-1} = \phi_{\mathcal{W}'} \circ \phi_{\mathcal{W}}^{-1} \circ \phi_{\mathcal{W}} \circ f \circ \phi_{\mathcal{V}}^{-1} \circ \phi_{\mathcal{V}} \circ \phi_{\mathcal{V}'}^{-1} \\ &= \left(\phi_{\mathcal{W}} \circ \phi_{\mathcal{W}'}^{-1}\right)^{-1} \circ \left(\phi_{\mathcal{W}} \circ f \circ \phi_{\mathcal{V}}^{-1}\right) \circ \left(\phi_{\mathcal{V}} \circ \phi_{\mathcal{V}'}^{-1}\right) \\ &= S^{-1} A_{f,\mathcal{V},\mathcal{W}} T = S^{-1} A T. \end{aligned}$$

■

Übung 4.4 *(dringend empfohlen): Beweisen sie die Gleichung (4.13) "zu Fuss", indem Sie die Definitionen der darstellenden Matrizen und der Basiswechsel ausschreiben, indem Sie also in*

$$f\left(v_i'\right) = \sum_{j=1}^{n} b_{ji} w_j',$$

die Vektoren v_i', w_j' durch die Basisvektoren der anderen Basen unter Verwendung von S und T ausdrücken etc.

Wir können die obige Diskussion noch auf Endomophismen einschränken. Ist V ein K-Vektorraum, $f : V \to V$ ein lineare Abbildung und $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis in V, so ist die darstellende Matrix $A = (a_{ij})$ von f bezüglich dieser Basis durch

$$f\left(v_j\right) = \sum_{i=1}^{n} a_{ij} v_i$$

definiert. Im Unterschied zu der früheren Situation mit zwei Vektorräumen arbeiten wir hier natürlich nur mit einer Basis. Ist $\mathcal{U} = (u_1, \ldots, u_n)$ eine neue Basis mit einer regulären Matrix $S = (s_{ij})$ der Basistransformation:

$$u_j = \sum_{i=1}^{n} s_{ij} v_i,$$

so spezialisiert sich der Satz 4.22 wie folgt: Ist B die darstellende Matrix von f bezüglich der Basis $\mathcal{U}$, so gilt

$$B = S^{-1} A S. \tag{4.14}$$

Definition 4.18 *Zwei Matrizen $A, B \in M\left(n, K\right)$ heissen **ähnlich**, wenn eine reguläre $n \times n$-Matrix S existiert mit (4.14).*

Ähnliche Matrizen definieren dieselbe Abbildung bezüglich verschiedenen Basen.

Übung 4.5 *Zeigen Sie dass*

$$A \sim B \Longleftrightarrow \exists S \in GL\left(n, K\right) \text{ mit } B = S^{-1} A S$$

ein Äquivalenzrelation auf $M\left(n, K\right)$ definiert.

5 Determinanten

5.1 Permutationen

Wir haben schon früher Permutationen kennengelernt: Eine Permutation π einer endlichen Menge M ist eine bijektive Abbildung $M \to M$. Wir können diese endliche Menge durchnummerieren und deshalb ohne Einschränkung der Allgemeinheit annehmen, dass $M = M_n := \{1, \ldots, n\}$ gilt. Wir schreiben dann

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}.$$

Wir bezeichnen mit Σ_n die Menge aller Permutationen von n Elementen. Wie wir schon in Kapitel 2 gesehen haben, ist Σ_n unter der zweistelligen Verknüpfung der Komposition eine Gruppe. Das Neutralelement ist die identische Abbildung id_M. Ganz allgemein bezeichnet man ein Element $i \in M$ mit $\pi(i) = i$ als einen **Fixpunkt** der Permutation π. Die identische Abbildung hat natürlich die ganze Menge M als Fixpunktmenge. Wir nennen eine Teilmenge $A \subset M$ **invariant** unter der Permuation π, wenn $\pi(i) \in A$ für alle $i \in A$ gilt.

Spezielle Permutationen sind die sogenannte **Zyklen**. Seien $m_1, \ldots, m_k \in M$ verschiedene Elemente. Wir bezeichnen mit $\pi = (m_1, \ldots, m_k)$ die Permutation, die die Elemente $m_1, \ldots, m_k$ in dieser Reihenfolge zyklisch vertauscht und die Elemente ausserhalb $\{m_1, \ldots, m_k\}$ fest lässt. Anders ausgedrückt:

$$\begin{aligned} \pi(m_i) &= m_{i+1},\ 1 \le i \le k-1, \\ \pi(m_k) &= m_1, \\ \pi(i) &= i,\ i \notin \{m_1, \ldots, m_k\}. \end{aligned}$$

Man beachte, dass $(m_2, m_3, \ldots, m_k, m_1)$ dieselbe Permutation wie $(m_1, \ldots, m_k)$ ist. Die Notation ist also nicht ganz eindeutig. Natürlich ist $\{m_1, \ldots, m_k\}$ invariant unter dem Zyklus. Wir bezeichnen mit k die **Länge** des Zyklus. Von besonderer Bedeutung sind Zyklen der Länge 2. Man nennt sie **Transpositionen,** und wir schreiben sie üblicherweise als $\tau_{i,j} := (i, j)$. Eine Transposition tauscht einfach die beiden bezeichneten Elemente der Menge M aus. Die Zyklen der Länge 1 sind natürlich trivialerweise einfach die Identität.

Ist π eine Permutation, so definieren wir die ganzzahligen Potenzen von π rekursiv wie folgt:

$$\pi^0 := \mathrm{id}_M, \quad \pi^{k+1} := \pi^k \circ \pi,\ k \ge 0.$$

Man hat also einfach $\pi^1 = \pi$, $\pi^2 = \pi \circ \pi$, $\pi^3 = \pi \circ \pi \circ \pi$ etc.

Lemma 5.1 *Jeder Zyklus $(m_1, m_2, \ldots, m_k)$ lässt sich als Produkt von Transpositionen wie folgt darstellen:*

$$(m_1, m_2, \ldots, m_k) = \tau_{m_1,m_2} \circ \tau_{m_2,m_3} \circ \ldots \circ \tau_{m_{k-1},m_k}.$$

Beweis. Nachrechnen. ■

Zwei Zyklen ζ_1, ζ_2 kommutieren im allgemeinen nicht, d.h. es gilt im allgemeinen $\zeta_1 \circ \zeta_2 \neq \zeta_2 \circ \zeta_1$. So ist etwa

$$(1,2) \circ (2,3) = (1,2,3)\,,$$

und

$$(2,3) \circ (1,2) = (1,3,2) \neq (1,2,3)\,.$$

Sind $\{m_1, \ldots, m_k\}$ und $\{m'_1, \ldots, m'_{k'}\}$ jedoch disjunkte Teilmengen von M, so gilt offensichtlich

$$(m_1, \ldots, m_k) \circ (m'_1, \ldots, m'_{k'}) = (m'_1, \ldots, m'_{k'}) \circ (m_1, \ldots, m_k)\,,$$

denn $(m_1, \ldots, m_k)$ verschiebt die Elemente nur innerhalb der Menge $\{m_1, \ldots, m_k\}$ und lässt diejenigen ausserhalb als Fixpunkte und analog für $(m'_1, \ldots, m'_{k'})$. Die Reihenfolge dieser Verschiebungen spielt offensichtlich keine Rolle, wenn $\{m_1, \ldots, m_k\} \cap \{m'_1, \ldots, m'_{k'}\} = \emptyset$ gilt. Wir nennen zwei Zyklen **disjunkt**, wenn diese Situation vorliegt.

Satz 5.1 *Jede Permutation π von $M = \{1, \ldots, n\}$ lässt sich als Komposition paarweise disjunkter Zyklen der Länge ≥ 2 darstellen. Diese Darstellung ist bis auf die Reihenfolge der Zyklen eindeutig.*

Beweis. Wir definieren zunächst eine Äquivalenzrelation auf M : $i \sim j$, falls $n \in \mathbb{N}_0$ existiert mit $j = \pi^n(i)$. $\sim$ ist tatsächlich eine Äquivalenzrelation:

- $i \sim i$ gilt wegen $i = \pi^0(i)$.
- Transitivität: Ist $i \sim j$ und $j \sim l$, so existieren $m, n \in \mathbb{N}_0$ mit $j = \pi^m(i)$ und $l = \pi^n(j)$. Dann ist $l = \pi^{m+n}(i)$, und es folgt somit $i \sim l$.
- Symmetrie: Es gelte $i \sim j$. Wir können voraussetzen, dass $i \neq j$ gilt, denn sonst wäre $j \sim i$ trivial. Dann existiert $m \in \mathbb{N}$ mit $j = \pi^m(i)$. m sei die kleinste Zahl, für die diese Gleichung gilt. Wir untersuchen die Folge von Elementen $i_0 := i$, $i_1 := \pi(i_0)$, $i_2 := \pi(i_1)$, ... Offenbar ist $j = i_m$. Da M eine endliche Menge ist, können nicht alle Elemente dieser Folge verschieden sein. Wir setzen

  $$k := \min\{l \geq 2 : i_l \in \{i_0, \ldots, i_{l-1}\}\}\,.$$

  Ich behaupte, dass $i_k = i_0\,(= i)$ gilt. Wäre dem nicht so und $i_k = i_l$, $1 \leq l \leq k-1$, so würde wegen der Injektivität von π $i_{k-1} = i_{l-1}$ folgen, was der Definition von k widerspricht. Die obige Folge $i_0, i_1, i_2, \ldots$ ist also einfach die endliche Folge $i_0, i_1, i_2, \ldots, i_{k-1}$, die danach einfach wieder neu durchlaufen wird. Es folgt auch sofort, dass $1 \leq m \leq k-1$ gelten muss, denn sonst wäre i_m nicht in dieser Liste enthalten. Damit folgt nun $i = \pi^{k-m}(j)$, d.h. $j \sim i$.

Betrachten wir nun die Äquivalenzklassen dieser Relation. Die Klassen mit einem Element sind einfach die Fixpunkte. Sei $A \subset M$ eine Klasse, die mehr als ein Element enthält. Nach der eben geführten Überlegung im Beweis der Symmetrie werden die Elemente von A einfach zyklisch vertauscht: Wir beginnen mit einem beliebigen Element $i \in A$ und definieren wie oben die Folge $i_0, i_1, \ldots, i_{k-1}$. Dann ist $A = \{i_0, i_1, \ldots, i_{k-1}\}$ und $\pi(i_j) = i_{j+1}$, $0 \leq j \leq k-2$, $\pi(i_{k-1}) = i_0$. Dies führt offensichtlich zu einer Zerlegung von π in eine Komposition von paarweise disjunkten Zyklen.

Die *Eindeutigkeit* ist klar: Sei $\pi = \zeta_1 \circ \ldots \circ \zeta_m$ eine Darstellung der Permutation π als Komposition von paarweise disjunkter Zyklen, und sei $Z(\zeta_j) \subset M$ die Menge der Elemente, die unter ζ_j zyklisch vertauscht werden. Dann sind diese $Z(\zeta_j)$ natürlich einfach die Klassen der oben eingeführten Äquivalenzrelation und $\pi = \zeta_1 \circ \ldots \circ \zeta_m$ ist genau die Zerlegung von π wie sie oben konstruiert wurde (bis möglicherweise auf die Reihenfolge). ■

Bemerkung 5.1 *Ist $\pi = \zeta_1 \circ \ldots \circ \zeta_m$ eine derartige Zerlegung in paarweise disjunkte Zyklen, so ist*

$$F := M \setminus \left(\bigcup_{j=1}^{k} Z(\zeta_j) \right)$$

einfach die Fixpunktmenge der Permutation. Es ist weiter unten praktisch, in die Zyklenzerlegung noch für jeden Fixpunkt $f \in F$ einen Einerzyklus (f) hinzuschreiben, der natürlich einfach die Identität ist, und daher nur "kosmetischen" Einfluss hat. Der Vorteil dieser Darstellung besteht darin, dass nach Hinzunahme diser trivialen Einerzyklen die $Z(\zeta_j)$ eine vollständige Zerlegung der Menge M bilden und man nicht in allen Überlegungen die Fixpunkte gesondert betrachten muss.

Beispiel 5.1 *$n = 10$ und*

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 5 & 6 & 8 & 4 & 10 & 1 & 7 & 9 \end{pmatrix} \\ &= (1,3,5,8) \circ (4,6) \circ (7,10,9)\,. \end{aligned}$$

Die Fixpunktmenge ist $\{2\}$, sodass wir π auch als

$$\pi = (1,3,5,8) \circ (4,6) \circ (7,10,9) \circ (2)$$

schreiben können, sodass nun die zu den einzelnen Zyklen gehörenden Teilmengen die Menge $\{1, \ldots, 10\}$ zerlegen. Die Reihenfolge in dieser Komposition spielt offensichtlich keine Rolle.

Als Korollar des obigen Satzes und Lemma 5.1 erhalten wir

Satz 5.2 *Jede Permutation lässt sich als Produkt von Transpositionen darstellen.*

Es muss hier betont werden, dass diese Darstellung keinesfalls eindeutig ist. Die Transpositionen, d.h. die Zweierzyklen, sind natürlich im allgemeinen auch nicht disjunkt.

Wir kommen nun zu einer wichtigen Definition:

Definition 5.1 *Sei π eine Permutation mit Zyklenzerlegung*

$$\pi = \zeta_1 \circ \zeta_2 \circ \ldots \circ \zeta_k.$$

*Die Längen der Zyklen seien $n_1, \ldots, n_k \geq 2$. Die **Signatur** von π ist definiert durch*

$$\operatorname{sign}(\pi) = (-1)^{\sum_{i=1}^{k}(n_i-1)}. \tag{5.1}$$

*Ist $\operatorname{sign}(\pi) = 1$, so bezeichnet man die Permutation als **gerade**, sonst als **ungerade**.*

Man sollte bemerken, dass es in der obigen Darstellung egal ist, ob die trivialen Einerzyklen für die Fixpunkte mit in der Zyklenzerlegung verwendet werden, denn für diese ist natürlich $n_i - 1 = 0$.

Ein Zyklus ist gerade, sofern die Länge des Zyklus ungerade ist, und ungerade, sofern diese Länge gerade ist. Die Signatur einer Transposition ist also -1. Die Signatur einer Permutation ergibt sich dann als das Produkt der Signaturen ihrer Zyklenzerlegung.

Lemma 5.2 *Ist $\tau_{i,j}$ eine Transposition und π eine beliebige Permutation, so gilt*

$$\operatorname{sign}(\pi \circ \tau_{i,j}) = -\operatorname{sign}(\pi)$$

Beweis. Wir betrachten die Zerlegung von π in paarweise disjunkte Zyklen:

$$\pi = \zeta_1 \circ \ldots \circ \zeta_k,$$

wobei für jeden Fixpunkt ein Einerzyklus vorkommt. Wir untersuchen nun, welche Auswirkungen die Komposition mit einer Transposition $\tau_{i,j}$ auf die obigen Zyklenzerlegung hat.

Fall I: i, j gehören beide zu einer der Mengen $Z(\zeta_l)$. Dann ist

$$\zeta_1 \circ \ldots \circ \zeta_k \circ \tau_{i,j} = \zeta_1 \circ \ldots \circ \zeta_{l-1} \circ (\zeta_l \circ \tau_{i,j}) \circ \zeta_{l+1} \circ \ldots \circ \zeta_k.$$

Wir müssen also nur untersuchen, wie die Permutation $\zeta_l \circ \tau_{i,j}$ aussieht, die natürlich auch eine Permutation der Elemente von $Z(\zeta_l)$ ist. Die Durchnummerierung der Elemente spielt offensichtlich keine Rolle, sodass wir annehmen können, dass $\zeta_l = (1, \ldots, m)$ und $1 \leq i < j \leq m$ gelten. Dann verschiebt $\zeta_l \circ \tau_{i,j}$ die Elemente in $\{1, \ldots, m\}$ nach dem folgenden Schema:

$$i \to j+1 \to j+2 \to \ldots \to m \to 1 \to \ldots \to i$$

und

$$j \to i+1 \to \ldots \to j.$$

$\zeta_l \circ \tau_{i,j}$ ist also das Produkt zweier disjunkter Zyklen. Es ist daher klar, dass in der Definition (5.1) sich die Summe $\Sigma_{i=1}^{k}(n_i - 1)$ um 1 vermindert. Damit ist $\operatorname{sign}(\pi \circ \tau_{i,j}) = -\operatorname{sign}(\pi)$ in diesem Fall nachgewiesen.

Fall II. i und j gehören zu verschiedenen der Mengen $Z(\zeta_l)$. Wieder spielt die Durchnummerierung der Zyklen natürlich keine Rolle und wir können deshalb annehmen, dass die beiden relevanten Zyklen durch $(1, \ldots, m)$ und $(m+1, \ldots, m+r)$ gegeben sind. Weiter können wir annehmen, dass $i = 1$ und $j = m+1$ ist. Dann verschiebt $(1, \ldots, m) \circ (m+1, \ldots, m+r) \circ \tau_{1,m+1}$ die Elemente der Menge $\{1, \ldots, m+r\}$ nach dem folgenden Schema:

$$\begin{aligned} 1 &\to m+2 \to m+3 \to \ldots \to m+r \to m+1 \to 2 \\ &\to 3 \to \ldots \to m \to 1. \end{aligned}$$

Wir sehen also, dass die vorher zwei Zyklen zu einem einzelnen zusammengeschweisst werden. Damit erhöht sich die Summe $\Sigma_{i=1}^{k}(n_i - 1)$ um 1 und wir erhalten auch in diesem Fall $\operatorname{sign}(\pi \circ \tau_{i,j}) = -\operatorname{sign}(\pi)$. Damit ist die Aussage des Satzes vollständig bewiesen. ■

Korollar 5.1 *Ist* $\operatorname{sign}(\pi) = 1$, *so ist die Anzahl der Transpositionen in jeder Darstellung von* π *als Produkt von Transpositionen gerade. Ist* $\operatorname{sign}(\pi) = -1$, *so ist diese Anzahl stets ungerade.*

Beweis. Dies folgt sofort aus dem vorangegangen Lemma: Ist

$$\pi = \tau^{(1)} \circ \tau^{(2)} \circ \ldots \circ \tau^{(k)}$$

eine Darstellung von π als Produkt von Transpositionen, so ist

$$\mathrm{id} = \pi \circ \tau^{(k)} \circ \ldots \circ \tau^{(1)},$$

also nach dem vorangegangenen Lemma:

$$1 = \operatorname{sign}(\mathrm{id}) = \operatorname{sign}(\pi)(-1)^k.$$

Daraus folgt $\operatorname{sign}(\pi) = (-1)^k$. ■

5.2 Multilinearformen, alternierende Multilinearformen

Sei V ein K-Vektorraum. Wir hatten schon den Dualraum V^* kennengelernt: Die Elemente von V^* sind die linearen Abbildungen $V \to K$. Wir betrachten nun Erweiterungen dieser Situation:

Definition 5.2 *Sei $k \in \mathbb{N}$. Eine Abbildung $\varphi : V^k \to K$ heisst **multilinear**, wenn für jedes $i \in \{1, \ldots, k\}$ und $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k \in V$ die Abbildung*

$$V \ni w \to \varphi(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_k) \in K$$

*linear ist. Anders ausgedrückt: Bei festgehaltenen Argumenten $1, \ldots, i-1, i+1, \ldots, k$ ist die Abbildung im i-ten Argument linear. Dies muss für jedes i gelten. Man nennt eine derartige multilineare Abbildung auch eine **k-Form.***

*Im Spezialfall $k = 2$ nennt man eine derartige Abbildung **bilinear**.*

*Eine k-Form φ heisst **symmetrisch**, wenn für $1 \leq i < j \leq k$ und $v_1, \ldots, v_k \in V$ die Gleichung*

$$\varphi(v_1, \ldots, v_k) = \varphi(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_k)$$

*gilt, d.h. wenn die Form invariant unter Vertauschung von zwei Argumenten ist. Eine k-Form φ heisst **antisymmetrisch**, oder **alternierend**, wenn für $1 \leq i < j \leq k$ und $v_1, \ldots, v_k \in V$ die Gleichung*

$$\varphi(v_1, \ldots, v_k) = -\varphi(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, , v_{j+1} \ldots, v_k)$$

gilt.

Bemerkung 5.2 *Ist eine k-Form symmetrisch, so gilt offensichtlich, dass für jede Permutation π von $\{1, \ldots, k\}$ die Gleichung*

$$\varphi(v_1, \ldots, v_k) = \varphi\left(v_{\pi(1)}, \ldots, v_{\pi(k)}\right).$$

Dies folgt einfach aus der im letzten Abschnitt bewiesenen Tatsache, dass sich jede Permutation als Komposition von Transpositionen darstellen lässt.

Ist hingegen φ alternierend, so gilt

$$\varphi\left(v_{\pi(1)}, \ldots, v_{\pi(k)}\right) = \operatorname{sign}(\pi)\, \varphi(v_1, \ldots, v_k),$$

was ebenfalls unmittelbar aus der Diskussion der Signatur einer Permutation folgt.

Wir bezeichnen mit $M_k(V)$ die Menge aller multilinearen k -Formen, mit $S_k(V)$ die Teilmenge der symmetrischen k -Formen und mit $A_k(V)$ die Menge der alternierenden k -Formen. Offensichtlich ist die 0-Abbildung $V^k \to K$ sowohl multilinear, wie symmetrisch und alternierend. Demzufolge sind $M_k(V)$, $S_k(V)$ und $A_k(V)$ nicht leer. Auf $M_k(V)$ können wir die Struktur eines K-Vektorraums definieren: Sind φ und $\psi \in M_k(V)$, so definieren wir $\varphi + \psi$ durch

$$(\varphi + \psi)(v_1, \ldots, v_k) := \varphi(v_1, \ldots, v_k) + \psi(v_1, \ldots, v_k)$$

und für $\alpha \in K$ und $\varphi \in M_k(V)$ die Abbildung $\alpha\varphi$ durch

$$(\alpha\varphi)(v_1, \ldots, v_k) := \alpha\varphi(v_1, \ldots, v_k).$$

Man prüft ganz einfach nach, dass $\varphi + \psi$ und $\alpha\varphi$ wieder multilinear sind, und dass mit diesen Verknüpfungen die Vektorraumaxiome erfüllt sind. Sind ferner $\alpha, \beta \in K$ und φ, ψ symmetrische [alternierende] k-Formen, so ist auch $\alpha\varphi + \beta\psi$ symmetrisch [bzw. alternierend], wie man ganz einfach nachrechnet. Wir haben deshalb das folgende Resultat:

Lemma 5.3 *$M_k(V)$ ist ein K-Vektorraum. $S_k(V)$ und $A_k(V)$ sind Unterräume von $M_k(V)$.*

Wir werden später sehr ausführlich Bilinearformen diskutieren. Determinanten sind jedoch alternierende Formen.

Lemma 5.4 *Sei $\mathrm{char}(K) \neq 2$, und sei φ eine alternierende k-Form. Dann gelten die folgenden Eigenschaften:*

a) Sind zwei der Vektoren $v_1, \ldots, v_k$ gleich, so gilt

$$\varphi(v_1, \ldots, v_k) = 0.$$

b) Sind die Vektoren $v_1, \ldots, v_k$ linear abhängig, so gilt

$$\varphi(v_1, \ldots, v_k) = 0.$$

c) Ist $i \neq j$ und $\alpha \in K$ so gilt

$$\varphi(v_1, \ldots, v_i, \ldots, v_j + \alpha v_i, \ldots, v_k) = \varphi(v_1, \ldots, v_k),$$

d.h. addiert man das α-fache des i-ten Arguments zum j-ten, so verändert sich die Form nicht.

Beweis. a) Sei $i \neq j$. Austausch des i-ten mit den j-ten Argument wechselt in der Form nach Voraussetzung das Vorzeichen. Ist $v_i = v_j$ so folgt somit

$$\varphi(v_1, \ldots, v_k) + \varphi(v_1, \ldots, v_k) = 0,$$

was wegen $\mathrm{char}(K) \neq 2$ die Gleichung

$$\varphi(v_1, \ldots, v_k) = 0$$

impliziert.

b) Sind $v_1, \ldots, v_k$ linear abhängig, so lässt sich einer der Vektoren, sagen wir der i-te, als Linearkombination der anderen darstellen:

$$v_i = \sum_{j:j\neq i} \alpha_j v_j.$$

Wegen der Multilinearität folgt dann

$$\varphi(v_1,\ldots,v_k)=\sum_{j:j\neq i}\alpha_j\,\varphi(v_1,\ldots,v_j,\ldots,v_j,\ldots,v_k)=0,$$

nach a).

c)

$$\begin{aligned}&\varphi(v_1,\ldots,v_i,\ldots,v_j+\alpha v_i,\ldots,v_k)\\&\quad=\varphi(v_1,\ldots,v_k)+\alpha\varphi(v_1,\ldots,v_i,\ldots,v_i,\ldots,v_k)=\varphi(v_1,\ldots,v_k)\end{aligned}$$

nach a). ■

5.3 Die Determinantenform

Im Laufe der nachfolgenden Diskussion werden wir den folgenden Satz beweisen:

Satz 5.3 *Sei K ein Körper mit* $\operatorname{char}(K)\neq 2$, *und sei V ein K-Vektorraum der Dimension n. Dann gilt*

$$\dim(A_n(V))=1$$

Die Aussage $\dim(A_n(V))=1$ bedeutet erstens, dass es eine alternierende n-Form gibt, die nicht die Nullform ist, und zweitens, dass je zwei n-Formen $\varphi,\psi\neq 0$ proportional sind. Das bedeutet, dass es bis auf eine Normierung nur eine alternierende n -Form gibt.

Definition 5.3 *Eine von der 0-Form verschiedene alternierende n-Form heisst* ***Determinantenform.***

Generalvoraussetzung für den Rest des Kapitels:

$$\boxed{\operatorname{char}(K)\neq 2}$$

Es ist im obigen Satz wichtig, dass alternierende k-Formen mit $k=\dim V$ betrachtet werden. Für $k>\dim V$ ist $\dim(A_k(V))=0$, was weiter unten klar werden wird. Für $k<\dim V$ ist $A_k(V)$ ein komplizierteres Objekt, das wir erst später etwas ausführlicher diskutieren werden (insbesondere für $k=2$).

Die für den Beweis benötigten Notationen sind etwas aufwendig. Um die einfache Grundidee zu erklären, betrachten wir erst einen engen Spezialfall und diskutieren den obigen Satz im Fall $\mathbb{R}^2$. Wir bezeichnen wie üblich mit (e_1,e_2) die Standardbasis. Für $x=(x_1,x_2)$, $y=(y_1,y_2)\in\mathbb{R}^2$ gilt $x=x_1e_1+x_2e_2$ und $y=y_1e_1+y_2e_2$. Ist φ eine beliebige alternierende 2-Form, so gilt wegen der Bilinearität

$$\begin{aligned}\varphi(x,y)&=\varphi(x_1e_1+x_2e_2,y_1e_1+y_2e_2)\\&=x_1y_1\varphi(e_1,e_1)+x_1y_2\varphi(e_1,e_2)\\&\quad+x_2y_1\varphi(e_2,e_1)+x_2y_2\varphi(e_2,e_2).\end{aligned}$$

Wenn φ alternierend ist, müssen die folgenden Gleichungen gelten:

$$\begin{aligned}\varphi(e_2, e_1) &= -\varphi(e_1, e_2),\\ \varphi(e_1, e_1) &= -\varphi(e_1, e_1),\\ \varphi(e_2, e_2) &= -\varphi(e_2, e_2).\end{aligned}$$

Aus den letzten zwei Gleichungen folgt natürlich $\varphi(e_1, e_1) = \varphi(e_2, e_2) = 0$ (wegen $\mathrm{char}(\mathbb{R}) \neq 2$!). Also erhalten wir

$$\varphi(x, y) = (x_1 y_2 - x_2 y_1)\,\varphi(e_1, e_2).$$

Ist nun $\varphi(e_1, e_2) = 0$, so ist φ einfach die Form identisch Null. Einen weiteren Spezialfall erhält man mit der Wahl $\varphi(e_1, e_2) = 1$. Wir bezeichnen die entsprechende Funktion φ mit $\overline{\varphi}$, und es ist dann

$$\overline{\varphi}(x, y) = x_1 y_2 - x_2 y_1 = \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix},$$

mit der Ihnen wahrscheinlich bekannten Determinante einer 2×2 -Matrix. Man überzeugt sich sofort davon, dass diese Determinatenfunktion *tatsächlich* eine alternierende 2-Form auf $\mathbb{R}^2$ definiert. Daraus folgt aber nun sofort, dass *jede* alternierende 2 -Form φ auf $\mathbb{R}^2$ die Darstellung

$$\varphi = \varphi(e_1, e_2)\,\overline{\varphi}$$

hat. Damit haben wir gezeigt, dass $A_2(\mathbb{R}^2)$ eindimensional ist mit der Basis bestehend aus dem einen Vektor $\overline{\varphi}$. Das ist natürlich nur etwas kompliziert ausgedrückt der folgenden Sachverhalt: Jede alternierende 2-Form φ auf $\mathbb{R}^2$ ist proportional zur Determinante, d.h. bis auf eine Normierung gibt es nur eine nicht-triviale 2-Form φ. Damit haben wir den Satz 5.3 im Spezialfall $V = \mathbb{R}^2$ gezeigt.

Der allgemeine Fall geht im wesentlichen genau gleich, ist aber natürlich etwas komplizierter aufzuschreiben. Wir beginnen damit, zu zeigen, dass *jede* alternierende n-Form φ auf V proportional zu einer von der 0-Funktion verschiedene Funktion $\overline{\varphi} : V^n \to K$ ist, wobei wir anschliessend zeigen, dass dieses $\overline{\varphi}$ tatsächlich eine alternierende Form ist. Damit ist dann der Satz 5.3 bewiesen, denn wir haben dann gezeigt, dass $A_n(V) \neq \{0\}$ ist, da $\overline{\varphi} \in A_n(V)$ gilt, und weiter, dass jedes andere Element $\varphi \in A_n(V)$ proportional zu $\overline{\varphi}$ ist, was belegt, dass $(\overline{\varphi})$ ein Erzeugendensystem von $A_n(V)$ ist und damit eine Basis.

Wir wählen zunächst eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$ fest in V. Jeder Vektor $u \in V$ hat eine eindeutige Darstellung als Linearkombination dieser Basis. Für die n-Form müssen wir n derartige Vektoren $u_1, \ldots, u_n$ betrachten. Wir schreiben sie als

$$u_i = \sum_{j=1}^{n} a_{ji} v_j. \tag{5.2}$$

Dann ist

$$\varphi(u_1,\ldots,u_n)=\sum_{j=1}^{n}a_{j1}\varphi(v_j,u_2,\ldots,u_n)$$

wegen der Linearität im 1. Argument. Nun fahren wir auf diese Weise weiter, indem wir die Linearität im zweiten Argument ausnützen, dann im dritten etc. Auf diese Weise erhalten wir

$$\varphi(u_1,\ldots,u_n)=\sum_{j_1=1}^{n}\sum_{j_2=1}^{n}\ldots\sum_{j_n=1}^{n}a_{j_1 1}a_{j_2 2}\cdot\ldots\cdot a_{j_n n}\,\varphi(v_{j_1},v_{j_2},\ldots,v_{j_n}).$$

Aus Lemma 5.4 folgt jedoch, dass $\varphi(v_{j_1},v_{j_2},\ldots,v_{j_n})=0$ ist, wenn zwei der Vektoren gleich sind. Demzufolge haben wir in den Summen nur über diejenigen n -Tupel $(j_1,\ldots,j_n)$ zu summieren, für die die Komponenten alle verschieden sind. Ein derartiges n-Tupel ist jedoch einfach eine Permutation von $\{1,\ldots,n\}$. Wir schreiben daher $j_k=\pi(k)$ und müssen nun über alle Permutationen π summieren:

$$\begin{aligned}\varphi(u_1,\ldots,u_n)&=\sum_{\pi\in\Sigma_n}a_{\pi(1),1}a_{\pi(2),2}\cdot\ldots\cdot a_{\pi(n),n}\,\varphi\left(v_{\pi(1)},v_{\pi(2)},\ldots,v_{\pi(n)}\right)\\&=\varphi(v_1,\ldots,v_n)\sum_{\pi\in\Sigma_n}\operatorname{sign}(\pi)\;a_{\pi(1),1}a_{\pi(2),2}\cdot\ldots\cdot a_{\pi(n),n},\end{aligned}$$

die letzte Gleichung nach Bemerkung 5.2. Definieren wir die Funktion $\overline{\varphi}:V^n\to K$ durch:

$$\overline{\varphi}(u_1,\ldots,u_n):=\sum_{\pi\in\Sigma_n}\operatorname{sign}(\pi)\;a_{\pi(1),1}a_{\pi(2),2}\cdot\ldots\cdot a_{\pi(n),n},\tag{5.3}$$

so erhalten wir, dass jede alternierende n-Form φ die Gleichung

$$\varphi=\varphi(v_1,\ldots,v_n)\,\overline{\varphi}$$

erfüllt.

Wir müssen nun noch nachweisen, dass $\overline{\varphi}$ auch tatsächlich eine alternierende n-Form ist, denn bisher haben wir nur gezeigt, dass *wenn* φ eine alternierende n-Form ist, φ proportional zu der obigen *Funktion* $\overline{\varphi}$ ist. Wäre $\overline{\varphi}$ keine alternierende n-Form, so hätten wir nur gezeigt, dass es keine alternierenden von der 0-Form verschiedenen n-Formen gibt. Man beachte, dass

$$\overline{\varphi}(v_1,\ldots,v_n)=1\tag{5.4}$$

gilt, was einfach eine Normierung ist.

Zunächst die Multilinearität. Wir betrachten die Linearität im ersten Argument. Die anderen gehen genau gleich. Seien also $u_1,u_1',u_2,\ldots,u_n\in V$ und $\alpha,\beta\in K$. Wir verwenden die Darstellung (5.2) und

$$u_1'=\sum_{j=1}^{n}a_{j1}'v_j.$$

Dann hat $\alpha u_1 + \beta u_1'$ die Darstellung in der $\mathcal{V}$-Basis:

$$\alpha u_1 + \beta u_1' = \sum_{j=1}^{n} \left(\alpha a_{j1} + \beta a_{j1}'\right) v_j.$$

Demzufolge ist

$$\begin{aligned}
\overline{\varphi}\left(\alpha u_1 + \beta u_1', \ldots, u_n\right) &= \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi) \left(\alpha a_{\pi(1),1} + \beta a_{\pi(1),1}'\right) a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \\
&= \alpha \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\, a_{\pi(1),1} a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \\
&\quad + \beta \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\, a_{\pi(1),1}' a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \\
&= \alpha \overline{\varphi}\left(u_1, \ldots, u_n\right) + \beta \overline{\varphi}\left(u_1', \ldots, u_n\right).
\end{aligned}$$

Damit ist die Linearität im 1. Argument gezeigt und mit den anderen Argumenten geht der Beweis genau gleich. Wir zeigen nun noch, dass $\overline{\varphi}$ alternierend ist, d.h. dass bei einer Vertauschung von zwei Argumenten das Vorzeichen wechselt. Der Einfachheit halber vertauschen wir das erste und das zweite Argument:

$$\overline{\varphi}\left(u_2, u_1, u_3, \ldots, u_n\right) = \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\, a_{\pi(1),2} a_{\pi(2),1} a_{\pi(3),3} \cdot \ldots \cdot a_{\pi(n),n}.$$

Für $\pi \in \Sigma_n$ definieren wir $\pi' := \pi \circ \tau_{1,2}$. Man beachte, dass dann $\pi = \pi' \circ \tau_{1,2}$ gilt (wegen $\tau_{1,2} \circ \tau_{1,2} = \mathrm{id}$). Ferner ist die Abbildung $\Sigma_n \ni \pi \to \pi' \in \Sigma_n$ eine Bijektion. Deshalb ist

$$\begin{aligned}
&\overline{\varphi}\left(u_2, u_1, u_3, \ldots, u_n\right) \\
&\qquad = \sum_{\pi \in \Sigma_n} \operatorname{sign}\left(\pi' \circ \tau_{1,2}\right) a_{\pi' \circ \tau_{1,2}(1),2} a_{\pi' \circ \tau_{1,2}(2),1} a_{\pi' \circ \tau_{1,2}(3),3} \cdot \ldots \cdot a_{\pi' \circ \tau_{1,2}(n),n} \\
&\qquad = \sum_{\pi \in \Sigma_n} \operatorname{sign}\left(\pi' \circ \tau_{1,2}\right) a_{\pi'(1),1} a_{\pi'(2),2} \cdot \ldots \cdot a_{\pi'(n),n} \\
&\qquad = -\sum_{\pi \in \Sigma_n} \operatorname{sign}\left(\pi'\right) a_{\pi'(1),1} a_{\pi'(2),2} \cdot \ldots \cdot a_{\pi'(n),n} \\
&\qquad = -\sum_{\pi' \in \Sigma_n} \operatorname{sign}\left(\pi'\right) a_{\pi'(1),1} a_{\pi'(2),2} \cdot \ldots \cdot a_{\pi'(n),n} \\
&\qquad = -\overline{\varphi}\left(u_1, u_2, u_3, \ldots, u_n\right).
\end{aligned}$$

Den Vorzeichenwechsel bei Vertauschung von anderen Argumenten zeigt man genau gleich.

Damit haben wir gezeigt, dass die Abbildung $\overline{\varphi} : V^n \to K$ eine alternierende n-Form ist, die natürlich von der Nullfunktion verschieden ist, und damit ist der Satz 5.3 vollständig gezeigt.

Wie wir also sehen, gibt es in einem n-dimensionalen Vektorraum "im wesentlichen" genau eine alternierende n-Form. Genauer: Zwei n-Formen unterscheiden sich nur durch einen Streckungsfaktor. Zu jeder Basis $\mathcal{V}$ gibt es genau eine Determinantenform, die der Normierung (5.4) genügt.

Der auf der rechten Seite von (5.3) stehende Ausdruck hängt natürlich nur von der quadratischen Matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ ab.

Definition 5.4 *Ist $A = (a_{ij})$ eine $n \times n$-Matrix, so ist*

$$\det(A) := \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\ a_{\pi(1),1} a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}$$

*die **Determinante** von A.*

Ist also $\mathcal{V} = (v_1, \ldots, v_n)$ eine beliebige Basis von V, so ist die eindeutige alternierende n-Form $\overline{\varphi}$, die der Normierung $\overline{\varphi}(v_1, \ldots, v_n) = 1$ genügt, gegeben durch

$$\overline{\varphi}(u_1, \ldots, u_n) = \det(A),$$

wobei $A = (a_{ij})$ die Matrix ist, die das n-Tupel $(u_1, \ldots, u_n)$ durch die Basis $\mathcal{V}$ darstellt:

$$u_i = \sum_{i=1}^{n} a_{ji} v_j.$$

Wir bezeichnen die so normierte Determinantenform auch mit $\varphi_{\mathcal{V}}$.

5.4 Die Determinante eines Endomorphismus

Wir können nun auch die **Determinante eines Endomorphismus $f : V \to V$** definieren. Sei $\mathcal{V}$ eine beliebige Basis von V und $\varphi_{\mathcal{V}}$ die dazugehörige normierte Determinantenform. Dann ist die Abbildung $V^n \to K$, die definiert ist durch

$$V^n \ni (u_1, \ldots, u_n) \to \varphi_{\mathcal{V}}(f(u_1), f(u_2), \ldots, f(u_n))$$

eine alternierende n-Form auf V, was man sofort nachrechnet. Wir bezeichnen diese Form (leicht missbräuchlich) mit $\varphi_{\mathcal{V}} \circ f$. Aus Satz 5.3 folgt also, dass ein Skalar $\alpha \in K$ existiert mit

$$\varphi_{\mathcal{V}} \circ f = \alpha \varphi_{\mathcal{V}}.$$

So wie α definiert ist, kann dieser Skalar natürlich von f und der gewählten Basis $\mathcal{V}$ abhängen. Wir schreiben daher $\alpha(f, \mathcal{V})$. Wir zeigen nun aber, dass $\alpha(f, \mathcal{V})$ nicht von $\mathcal{V}$ abhängt: Ist nämlich $\mathcal{U}$ eine andere Basis, so existiert $\beta \in K$, $\beta \neq 0$, mit $\varphi_{\mathcal{U}} = \beta \varphi_{\mathcal{V}}$. Dann gilt natürlich auch $\varphi_{\mathcal{U}} \circ f = \beta(\varphi_{\mathcal{V}} \circ f)$. Daraus folgt

$$\alpha(f, \mathcal{U})\, \varphi_{\mathcal{U}} = \varphi_{\mathcal{U}} \circ f = \beta(\varphi_{\mathcal{V}} \circ f) = \beta\alpha(f, \mathcal{V})\, \varphi_{\mathcal{V}} = \alpha(f, \mathcal{V})\, \varphi_{\mathcal{U}}.$$

Da $\varphi_{\mathcal{U}}$ nicht die Nullform ist, folgt $\alpha(f, \mathcal{U}) = \alpha(f, \mathcal{V})$. Der Skalar α hängt daher nur von f ab und nicht von einer speziell gewählten Basis.

Definition 5.5 *$\alpha(f)$ heisst die **Determinante** von f. Wir bezeichnen sie mit* $\det(f)$.

Lemma 5.5 *a)*

$$\det(\mathrm{id}_V) = 1.$$

b) Sind f, g zwei Endomorphismen von V so gilt

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

Beweis. Wir wählen eine beliebige Basis $\mathcal{V}$ in V.
a) ist evident, denn es gilt natürlich $\varphi_{\mathcal{V}} \circ \mathrm{id}_V = \varphi_{\mathcal{V}}$.
b) folgt aus $\varphi_{\mathcal{V}} \circ (f \circ g) = (\varphi_{\mathcal{V}} \circ f) \circ g$. Daraus ergibt sich

$$\begin{aligned}\det(f \circ g)\,\varphi_{\mathcal{V}} &= \varphi_{\mathcal{V}} \circ (f \circ g) = (\varphi_{\mathcal{V}} \circ f) \circ g \\ &= \det(g)\,(\varphi_{\mathcal{V}} \circ f) = \det(g)\det(f)\,\varphi_{\mathcal{V}},\end{aligned}$$

und da $\varphi_{\mathcal{V}}$ nicht die Nullform ist, ergibt sich die Behauptung. ■

Satz 5.4 *Sie $f : V \to V$ ein Endomorphismus. Dann gilt* $\det(f) \neq 0$ *genau dann, wenn f ein Isomorphismus ist. Ist f ein Isomorphismus, so gilt*

$$\det\left(f^{-1}\right) = \frac{1}{\det(f)}.$$

Beweis. Ist f ein Isomorphismus, so existiert eine Inverse f^{-1}. Aus dem obigen Lemma folgt dann

$$1 = \det(\mathrm{id}_V) = \det\left(f \circ f^{-1}\right) = \det(f)\det\left(f^{-1}\right).$$

Ist f kein Isomorphismus, so ist $\dim(\mathrm{im}(f)) < n$. Ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine beliebige Basis von V so sind die Vektoren $f(v_1), \ldots, f(v_n)$ linear abhängig. Nach Lemma 5.4 gilt

$$\varphi_{\mathcal{V}}(f(v_1), \ldots, f(v_n)) = 0.$$

Daraus folgt $\det(f) = 0$. ■

Die Determinante eines Endomorphismus ist einfach die Determinante der darstellenden Matrix bezüglich einer beliebigen Basis, wie das folgende Resultat zeigt:

Proposition 5.1 *Sie $f : V \to V$ ein Endomorphismus und A die darstellende Matrix von f bezüglich einer beliebigen Basis $\mathcal{V} = (v_1, \ldots, v_n)$. Dann gilt*

$$\det(f) = \det(A).$$

Beweis. Sei $u_i := f(v_i)$, $i = 1, \ldots, n$. Dann sind die Spalten von A genau die Koordinaten der u_i bezüglich der Basis $\mathcal{V}$. Nach (5.3) und der Definition der Determinante einer Matrix folgt daraus

$$\det(f) = \varphi_{\mathcal{V}}(u_1, \ldots, u_n) = \det(A).$$

■

5.5 Eigenschaften der Determinante einer quadratischen Matrix, Cramersche Regeln

Wir diskutieren in diesem Abschnitt einige wichtige Eigenschaften von Determinanten von Matrizen. Eine $n \times n$-Matrix A definiert, wie wir schon wissen, einen Endomorphismus $K^n \to K^n$. Die darstellende Matrix dieses Endomorphismus bezüglich der Standardbasis $\mathcal{E}$ ist dann genau A. Damit ist nach der Diskussion im letzten Abschnitt $\det(A)$ auch genau die Determinante dieses Endomorphismus. Als n-Form können wir $\det(A)$ als $\varphi_{\mathcal{E}}(s_1, \ldots, s_n)$ auffassen, wobei $s_1, \ldots, s_n$ die Spaltenvektoren der Matrix sind. Sie hat damit auch alle Eigenschaften einer alternierenden n-Form.

Satz 5.5 *Sei A ein $n \times n$-Matrix. Dann gilt*

a) $\det(A) = \det\left(A^T\right)$.

b) $\det(AB) = \det(A)\det(B)$.

c) A ist genau dann regulär, wenn $\det(A) \neq 0$ *gilt. In diesem Fall ist*

$$\det\left(A^{-1}\right) = \frac{1}{\det(A)}.$$

d) Ist A eine obere Dreiecksmatrix, d.h. gilt $a_{ij} = 0$ für $i > j$, so gilt

$$\det(A) = \prod_{i=1}^{n} a_{ii}$$

Beweis. a) Die Abbildung $\Sigma_n \ni \pi \to \pi^{-1} \in \Sigma_n$ ist bijektiv. Man beachte auch, dass $\operatorname{sign}(\pi) = \operatorname{sign}(\pi^{-1})$ gilt. Daraus folgt

$$\begin{aligned}
\det(A) &:= \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\ a_{\pi(1),1} a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n} \\
&= \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\ a_{1,\pi^{-1}(1)} a_{2,\pi^{-1}(2)} \cdot \ldots \cdot a_{n,\pi^{-1}(n)} \\
&= \sum_{\pi \in \Sigma_n} \operatorname{sign}\left(\pi^{-1}\right)\ a_{1,\pi^{-1}(1)} a_{2,\pi^{-1}(2)} \cdot \ldots \cdot a_{n,\pi^{-1}(n)} \\
&= \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi)\ a_{1,\pi(1)} a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)} = \det\left(A^T\right).
\end{aligned}$$

Die zweite Gleichung folgt aus einer Umstellung der Faktoren, die dritte wegen $\operatorname{sign}(\pi) = \operatorname{sign}(\pi^{-1})$ und die vierte wegen der erwähnten Bijektion $\Sigma_n \ni \pi \to \pi^{-1} \in \Sigma_n$, die einfach zu einer Umstellung der Summe führt.

b) folgt aus Lemma 5.5 und der Interpretation von $\det(A)$ als die Determinante des durch A definierten Endomorphismus $K^n \to K^n$.

c) folgt aus Satz 5.4.

d) Ist eine Permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ nicht die Identität, so gibt es ein i mit $\pi(i) < i$ (Überlegen Sie sich das selbst!). Demzufolge fallen für eine obere Dreiecksmatrix bei der Definition der Permutation die Beiträge von allen Permutationen weg, ausser dem von $\pi = \mathrm{id}$. ■

Bemerkung 5.3 *Aus der Interpretation von* $\det(A)$ *als* $\varphi_{\mathcal{E}}(s_1, \ldots, s_n)$, *wobei die* s_i *die Spaltenvektoren der Matrix sind, folgt die Multilinearität der Determinante einer Matrix in den Spaltenvektoren. Wegen Teil a) des obigen Satzes folgt dann auch die Multilinearität als Funktion der n Zeilenvektoren. Insbesondere wissen wir genau, wie sich die Determinante bei elementaren Zeilenoperationen verhält: Beim Vertauschen von zwei Zeilen wechselt das Vorzeichen, bei Multiplikation eine Zeile mit einem Skalar wird die Determinante entsprechend multipliziert, und bei Z3 verändert sich die Determinante nicht. Die Determinante einer Matrix lässt sich also dadurch berechnen, dass man die Matrix mittels Zeilen- und Spaltenoperationen auf eine obere Dreiecksmatrix transformiert und dann das Produkt der Diagonalkomponenten bildet.*

Beispiel 5.2

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

$$= -\det\begin{pmatrix} 1 & -2 & 2 & 3 \\ 0 & 1 & 5 & 4 \\ 0 & 6 & -5 & -2 \\ 0 & 5 & -3 & -5 \end{pmatrix} = -\det\begin{pmatrix} 1 & -2 & 2 & 3 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & -35 & -26 \\ 0 & 0 & -28 & -25 \end{pmatrix}$$

$$= -\det\begin{pmatrix} 1 & -2 & 2 & 3 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & 35 & 26 \\ 0 & 0 & 28 & 25 \end{pmatrix} = -\det\begin{pmatrix} 1 & -2 & 2 & 3 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & 7 & 1 \\ 0 & 0 & 28 & 25 \end{pmatrix}$$

$$= \det\begin{pmatrix} 1 & -2 & 3 & 2 \\ 0 & 1 & 4 & 5 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 25 & 28 \end{pmatrix} = \det\begin{pmatrix} 1 & -2 & 3 & 2 \\ 0 & 1 & 4 & 5 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & -147 \end{pmatrix} = -147.$$

Als Nächstes diskutieren wir den sogenannten Entwicklungssatz für Determinanten. Wenn A eine $n \times n$-Matrix ist, so können wir für jeden Zeilenindex i und jeden Spaltenindex j die $(n-1) \times (n-1)$-Matrix $A^{i,j}$betrachten, die man aus A erhält, indem man die i-te Zeile und die j-te Spalte streicht.

Satz 5.6 *Für jede* $n \times n$*-Matrix* $A = (a_{ij})$ *und* $1 \leq i, j \leq n$ *gilt*

$$\det(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det\left(A^{i,k}\right) = \sum_{k=1}^{n} (-1)^{j+k} a_{kj} \det\left(A^{k,j}\right)$$

Die Darstellung in der ersten Zeile nennt man aus naheliegenden Gründen die Entwicklung nach der i-ten Zeile der Matrix, und die zweite die Entwicklung nach der j-ten Spalte.

Beweis. Wegen $\det(A) = \det\left(A^T\right)$ brauchen wir nur die Entwicklung nach den Spalten zu betrachten. Wir schreiben die j-te Spalte wie folgt:

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ \vdots \\ a_{nj} \end{pmatrix} = \sum_{k=1}^{n} a_{kj} e_k,$$

wobei wie üblich e_k der k-te Vektor der Standardbasis ist (als Spaltenvektor geschrieben). Unter Benützung der Multilinearität der Determinate erhalten wir also

$$\det(A) = \sum_{k=1}^{n} a_{kj} \det\left(B^{k,j}\right),$$

wobei $B^{k,j}$ die Matrix ist, bei der die j-te Spalte durch e_k ersetzt wird:

$$B^{k,j} = \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & & \vdots & & & \\ a_{k-1,1} & \cdots & \cdots & 0 & \cdots & \cdots & a_{k-1,n} \\ a_{k,1} & \cdots & a_{k,j-1} & 1 & a_{k,j+1} & \cdots & a_{k,n} \\ a_{k+1,1} & \cdots & \cdots & 0 & \cdots & \cdots & a_{k+1,n} \\ \vdots & & & \vdots & & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & 0 & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix}.$$

Nun vertauschen wir die j-te Spalte mit der $(j-1)$-ten, dann die $(j-1)$-te mit der $(j-2)$-ten etc, bis e_k die erste Spalte ist. Mit diesen Operationen haben wir $j-1$ mal das Vorzeichen gewechselt. Nun wollen wir noch die 1 in die erste Zeile bringen. Dazu vertauschen wir die k-te Zeile mit der $(k-1)$ -ten, dann die $(k-1)$-te mit der $(k-2)$-ten etc. Insgesamt haben wir mit diesen Spaltenvertauschungen $k-1$ mal das Vorzeichen gewechselt. Nach diesen Zeilen- und Spaltenvertauschungen sind wir ausgehend von der Matrix $B^{k,j}$ bei der Matrix

$$\begin{pmatrix} 1 & * \\ 0 & A^{k,j} \end{pmatrix}$$

angelangt, wobei $A^{k,j}$ die oben eingeführte $(n-1)\times(n-1)$-Matrix ist, 0 für den Spaltenvektor der Länge $n-1$ mit alles Nullen steht, und $*$ ein Zeilenvektor der Länge $n-1$ ist, der uns nicht weiter zu interessieren braucht. Wir erinnern uns, dass wir ausgehend von $B^{k,j}$ insgesamt $k+j-2$ mal das Vorzeichen geändert

haben, was auf dasselbe hinausläuft, wie $k+j$ mal das Vorzeichen zu ändern. Wir erhalten also

$$\det\left(B^{k,j}\right) = (-1)^{k+j} \det\begin{pmatrix} 1 & * \\ 0 & A^{k,j} \end{pmatrix}.$$

Nun gehen wir zurück zur Definition der Determinante in Definition 5.4 um $\det\begin{pmatrix} 1 & * \\ 0 & A^{k,j} \end{pmatrix}$ zu berechnen. Offenbar geben nur diejenigen Permutation $\pi \in \Sigma_n$ einen Beitrag, für die $\pi(1) = 1$ gilt, für die also 1 ein Fixpunkt ist. Die Menge der Permutationen $\pi \in \Sigma_n$, welche 1 als Fixpunkt haben kann bijektiv auf die Menge der Permutationen der Menge $\{2, \ldots, n\}$ abgebildet werden: einfach durch die Einschränkung π' von π auf diese Menge. Ferner ist offensichtlich die Signatur dieser Einschränkung dieselbe wie die von π. Demzufolge ist

$$\det\begin{pmatrix} 1 & * \\ 0 & A^{k,j} \end{pmatrix} = \sum_{\pi \in \Sigma_{n-1}} \operatorname{sign}(\pi') \prod_{t=1}^{n-1} \left(A^{k,j}\right)_{\pi(t),t} = \det\left(A^{k,j}\right).$$

Dabei ist $\left(A^{k,j}\right)_{s,t}$ die s,t-te Komponente der $(n-1)\times(n-1)$-Matrix $A^{k,j}$. ■

Definition 5.6 *Sei A eine $n \times n$-Matrix. Die* ***adjungierte Matrix*** $\operatorname{adj}(A)$ *ist definiert durch*

$$\left(\operatorname{adj}(A)\right)_{i,j} = (-1)^{i+j} \det\left(A^{i,j}\right),\ 1 \le i,j \le n.$$

Satz 5.7

$$\operatorname{adj}(A)^T\ A = A\ \operatorname{adj}(A)^T = \det(A)\, E_n.$$

Beweis. Die i,j-te Komponente von $\operatorname{adj}(A)^T\ A$ ist

$$\sum_{k=1}^{n} \left(\operatorname{adj}(A)\right)_{k,i} a_{kj} = \sum_{k=1}^{n} (-1)^{i+k} \det\left(A^{k,i}\right)\ a_{kj}.$$

Nach dem Entwicklungssatz ist das einfach die Determinante der Matrix, die man aus A erhält, indem man die i-te Spalte durch die j-te ersetzt. Ist $i \neq j$, so hat diese Matrix zwei gleiche Spalten und ihre Determinante ist somit 0. Ist $i = j$, so ist es einfach $\det(A)$. Damit ist $\operatorname{adj}(A)^T\ A = \det(A)\, E_n$ bewiesen. $A\ \operatorname{adj}(A)^T = \det(A)\, E_n$ geht analog. ■

Korollar 5.2 *Ist A regulär so gilt*

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)^T.$$

Wir kommen nun nochmals auf das Gleichungssystem

$$Ax = b$$

zurück, wobei A eine $n \times n$-Matrix, und b ein Spaltenvektor aus K^n ist. Ist A regulär, so ist die eindeutige Lösung gegeben durch

$$x = A^{-1}b = \frac{\operatorname{adj}(A)^T b}{\det(A)}.$$

Die k-te Komponente ist dann

$$x_k = \frac{\sum_{j=1}^{n} \operatorname{adj}(A)_{k,j} b_k}{\det(A)} = \frac{\sum_{j=1}^{n} (-1)^{k+j} \det\left(A^{k,j}\right) b_k}{\det(A)}.$$

Nach dem Entwicklungssatz ist der Zähler die Determinante der Matrix, die man erhält, indem man in der Matrix A die k-te Spalte durch b ersetzt:

Satz 5.8 (Cramersche Regel) *Sei A eine reguläre $n \times n$-Matrix und $b \in K^n$ (als Spaltenvektor geschrieben). Dann ist die eindeutige Lösung des Gleichungssystems*

$$\sum_{j=1}^{n} a_{ij} x_j = b_i,\ 1 \leq i \leq n$$

gegeben durch

$$x_k = \frac{\det\left(A^{b,k}\right)}{\det(A)},\ 1 \leq k \leq n,$$

wobei $A^{b,k}$ die Matrix ist, die man aus A erhält, indem man die k -te Spalte durch den Spaltenvektor b ersetzt.

6 Invariante Unterräume, Eigenwerte und Eigenvektoren

6.1 Direkte Summe von Unterräumen

Wir haben schon den Begriff „Summe von Unterräumen $U_1, \ldots, U_m$ eines K-Vektorraums V“ kennengelernt:

$$\sum_{i=1}^{m} U_i = \left\{ \sum_{i=1}^{m} u_i : u_j \in U_j \,\text{für}\, 1 \leq j \leq m \right\}.$$

Definition 6.1 *V heisst die **direkte Summe** der Unterräume $U_1, \ldots, U_m$, wenn jeder Vektor $v \in V$ sich **eindeutig** als Summe $v = \sum_{i=1}^{m} u_i$ mit $u_j \in U_j$, $1 \leq j \leq m$, darstellen lässt. Es gelten also die folgenden zwei Eigenschaften:*

a)

$$V = \sum_{i=1}^{m} U_i.$$

b) Gilt

$$\sum_{i=1}^{m} u_i = \sum_{i=1}^{m} u_i' \text{ mit } u_j, u_j' \in U_j \text{ für } 1 \leq j \leq m,$$

so folgt $u_j = u_j'$, $1 \leq j \leq m$.

Wir schreiben dann

$$V = U_1 \oplus U_2 \oplus \ldots \oplus U_m = \bigoplus_{i=1}^{m} U_i.$$

Bemerkung 6.1 *Die Eindeutigkeit der Darstellung in der obigen Definition lässt sich auch einfach durch die folgende Bedingung ersetzen: Gilt*

$$0 = \sum_{i=1}^{m} u_i \text{ mit } u_j \in U_j \text{ für } 1 \leq j \leq m,$$

so folgt $u_1 = \ldots = u_m = 0$. Man überlegt sich sofort, dass daraus die Eigenschaft b) in der obigen Definition folgt.

Eine direkte Summe von Unterräumen ist immer eine Summe dieser Unterräume. Die Notation ist leider nicht ganz glücklich, denn ob eine Summe eine direkte ist hängt nur von Eigenschaften der Familie der Unterräume ab. Wir formulieren diese Eigenschaft in dem folgenden Satz:

Satz 6.1 *Es seien $U_1, \ldots, U_m$ Unterräume von V. Dann gilt $V = \bigoplus_{i=1}^m U_i$ genau dann, wenn $V = \sum_{i=1}^m U_i$ gilt und wenn für jedes i*

$$U_i \cap \left(\sum_{j:j\neq i} U_j \right) = \{0\} \tag{6.1}$$

ist.

Beweis. I) Wir setzen zunächst voraus, dass $V = \bigoplus_{i=1}^m U_i$ gilt. Per Definition gilt dann natürlich $V = \sum_{i=1}^m U_i$. Wir müssen also nur noch die Eigenschaft (6.1) nachweisen.

Ist $u \in U_i \cap \left(\sum_{j:j\neq i} U_j \right)$, so gilt

$$u = \sum_{j:j\neq i} u_j$$

mit $u_j \in U_j$. Dann ist

$$0 = u - \sum_{j:j\neq i} u_j,$$

wobei nach Voraussetzung $u \in U_i$ gilt. Demzufolge liegt eine Darstellung des Nullvektors als Linearkombination von Vektoren aus den U_j vor, also gilt $u = 0$.

II) Wir setzen $V = \sum_{i=1}^m U_i$ und (6.1) voraus, und wir wollen zeigen, dass die Summe eine direkte Summe ist. Nach Bemerkung 6.1 genügt es zu zeigen, dass der Nullvektor nur eine triviale Darstellung als Summe von Vektoren aus den U_j hat. Sei also

$$0 = \sum_{j=1}^m u_j,\ u_j \in U_j.$$

Dann gilt für jedes i :

$$u_i = -\sum_{j:j\neq i} u_j.$$

Die rechte Seite ist in $\sum_{j:j\neq i} U_j$ und die linke Seite in U_i. Demzufolge gilt

$$u_i \in U_i \cap \left(\sum_{j:j\neq i} U_j \right),$$

und ist daher nach der Voraussetzung (6.1) gleich 0. Dies gilt für alle i. ■

Sind $U_1, \ldots, U_m$ Unterräume von V, so ist $U := \sum_{i=1}^m U_i$ natürlich immer ein Unterraum von V, gleichgültig ob $U = V$ gilt oder nicht. Die U_i sind dann Unterräume von U. Gilt die Eigenschaft (6.1), so schreiben wir $U = \bigoplus_{i=1}^m U_i$. In diesem Fall hat dann jeder Vektor $u \in U$ eine eindeutige Darstellung als Summe von Vektoren aus den U_i.

Beispiel 6.1 *Ist V ein endlichdimensionaler Vektorraum mit einer Basis $\mathcal{U} = (u_1, \ldots, u_n)$, und sind die Unterräume U_i definiert durch*

$$U_i := \{\alpha u_i : \alpha \in K\},$$

so gilt $V = \bigoplus_{i=1}^{n} U_i$. In der Tat hat ja jeder Vektor $v \in V$ die eindeutige Darstellung

$$v = \sum_{i=1}^{n} \alpha_i u_i,$$

und die $\alpha_j u_j$ sind in U_j.

Beispiel 6.2 $V = \mathbb{R}^3$.

$$U_1 := L\left[\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right],\ U_2 = L\left[\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right].$$

Dann gilt zwar $\mathbb{R}^3 = U_1 + U_2$, aber nicht $\mathbb{R}^3 = U_1 \oplus U_2$.

Für endlichdimensionale Vektorräume kann die Direktheit einer Summe von Unterräumen auch einfach über die Dimension charakterisiert werden:

Satz 6.2 *Es seien $U_1, \ldots, U_m$ Unterräume des endlichdimensionalen Vektorraums V. Dann gilt $V = \bigoplus_{i=1}^{m} U_i$ genau dann wenn $V = \sum_{i=1}^{m} U_i$ gilt und wenn*

$$\dim(V) = \sum_{i=1}^{m} \dim(U_i) \tag{6.2}$$

ist.

Beweis. I) Wir setzen $V = \bigoplus_{i=1}^{m} U_i$ voraus und beweisen (6.2) mit Induktion nach m. Für $m = 1$ ist das trivial. Nach Teil a) gilt

$$U_m \cap \left(\bigoplus_{i=1}^{m-1} U_i\right) = \{0\}.$$

Nach der Dimensionsformel (Satz 4.9) gilt

$$\dim\left(\bigoplus_{i=1}^{m} U_i\right) = \dim(U_m) + \dim\left(\bigoplus_{i=1}^{m-1} U_i\right) = \sum_{i=1}^{m} \dim(U_i),$$

die letzte Gleichung nach Induktionsvoraussetzung.

II) Wir setzen $V = \sum_{i=1}^{m} U_i$ und (6.2) voraus und beweisen, dass die Summe eine direkte Summe ist. Dazu weisen wir nach, dass (6.1) gilt. Wäre diese Gleichung für ein i falsch, so wäre

$$1 \leq \dim\left(U_i \cap \left(\sum_{j:j\neq i} U_j\right)\right).$$

Daraus ergibt sich der folgende Widerspruch:

$$\begin{aligned}\sum_{j=1}^{m} \dim(U_j) &= \dim(V) \\ &= \dim(U_i) + \dim\left(\sum_{j:j\neq i} U_j\right) - \dim\left(U_i \cap \left(\sum_{j:j\neq i} U_j\right)\right) \\ &< \dim(U_i) + \dim\left(\sum_{j:j\neq i} U_j\right) \leq \sum_{j=1}^{m} \dim(U_j).\end{aligned}$$

In der letzten Ungleichung haben wir verwendet, dass die Dimension einer Summe von Unterräumen immer kleiner oder gleich der Summe der Dimensionen dieser Unterräume ist. Das ergibt sich sofort aus der Überlegung, dass die Vereinigung von Basen dieser Unterräume ein Erzeugendensystem der Summe ist. ■

Korollar 6.1 *V sei ein endlichdimensionaler Vektorraum und $U_1, \ldots, U_m$ seien Unterräume mit $V = \sum_{i=1}^{m} U_i$. $\mathcal{U}_i = (u_{i1}, u_{i2}, \ldots, u_{i,k_i})$ seien Basen der Unterräume U_i. Dann gilt $V = \bigoplus_{i=1}^{m} U_i$ genau dann, wenn $(u_{11}, u_{12}, \ldots, u_{1k_1}, u_{21}, \ldots, u_{m,k_m})$ eine Basis von V ist.*

Beweis. $(u_{11}, u_{12}, \ldots, u_{1k_1}, u_{21}, \ldots, u_{m,k_m})$ ist auf jeden Fall ein Erzeugendensystem von V, wenn $V = \sum_{i=1}^{m} U_i$ gilt, wie wir voraussetzen. Dieses System von Vektoren ist daher genau dann eine Basis, wenn

$$\dim(V) = \sum_{i=1}^{m} k_i = \sum_{i=1}^{m} \dim(U_i)$$

gilt. Das ist aber nach dem vorangegangenen Satz äquivalent damit, dass V die direkte Summe der Unterräume U_i ist. ■

Wir diskutieren noch kurz einen Zusammenhang mit sogenannten Projektionsoperatoren.

Definition 6.2 *Sei V ein Vektorraum. Ein Endomorphismus $p : V \to V$ heisst **Projektion**, wenn*

$$p^2 := p \circ p = p$$

gilt.

Ist V die direkte Summe von zwei Unterräumen:

$$V = U \oplus W$$

so können wir eine Projektion p wie folgt definieren: Jedes Element $v \in V$ hat eine eindeutige Darstellung als $v = u + w$, $u \in U$, $w \in W$. Wir definieren $p(v) := u$. Der Leser prüfe die folgenden einfachen Eigenschaften selbst nach:

- p ist eine lineare Abbildung $V \to V$, d.h. ein Endomorphismus.
- p ist eine Projektion.
- $\ker(p) = W$.
- $\mathrm{im}(p) = U$.

Ist V die direkte Summe von mehreren Unterräumen

$$V = \bigoplus_{i=1}^{m} U_i$$

so können wir für $1 \leq i \leq m$ Projektionen p_i auf die einzelnen U_i definieren: Ist $v = \sum_{i=1}^{m} u_i$ die eindeutige Darstellung eines Vektors v als Summe von Vektoren aus den u_i, so definieren wir

$$p_i(v) := u_i.$$

Lemma 6.1 *Unter den obigen Voraussetzungen haben die p_i die folgenden Eigenschaften:*

a) Die p_i sind Projektionen.

b) Für $i \neq j$ gilt

$$p_i \circ p_j = 0, \tag{6.3}$$

wobei 0 hier die Nullabbildung $V \to V$ ist, die alle Vektoren auf den Vektor 0 abbildet.

c)

$$\sum_{i=1}^{m} p_i = \mathrm{id}_V . \tag{6.4}$$

(Wir hatten schon früher gesehen, dass $\hom(V)$ ein K-Vektorraum ist: Für $\varphi, \psi \in \hom(V)$ ist $\varphi + \psi \in \hom(V)$ definiert durch $(\varphi + \psi)(v) := \varphi(v) + \psi(v)$)

Beweis. a) hatten wir schon oben dem Leser überlassen. Wir beweisen b) und c). Ist $v \in V$ mit der eindeutigen Darstellung $v = \sum_{i=1}^{m} u_i$, $u_i \in U_i$, so erhalten wir wegen $u_i = p_i(v)$

$$v = \sum_{i=1}^{m} p_i(v) .$$

Dies beweist c). Um b) zu beweisen, beachten wir, dass $p_i(v)$ stets in U_i liegt. Nun gilt aber für jedes Element $u \in U_i$ und $j \neq i$ die Gleichung $p_j(u) = 0$, denn in der eindeutigen Darstellung von u als Summe

$$u = \sum_{j=1}^{m} w_j,\ w_j \in U_j,$$

ist natürlich einfach $w_i = u$ und $w_j = 0$ für $j \neq i$. ■

Eine Familie von Projektionen, die (6.3) und (6.4) erfüllt, nennt man auch **Auflösung der Einheit.** In Umkehrung des obigen Lemmas können wir den folgenden Satz beweisen:

Satz 6.3 *Seien $p_1, \ldots, p_m$ Projektionen des Vektorraums V, die die Gleichungen (6.3) und (6.4) erfüllen. Dann gilt*

$$V = \bigoplus_{i=1}^{m} \operatorname{im}(p_i).$$

Beweis. $V = \sum_{i=1}^{m} \operatorname{im}(p_i)$ folgt sofort aus (6.4). Um nachzuweisen, dass die Summe direkt ist, weisen wir (6.1) nach. Sei

$$v \in \operatorname{im}(p_i) \cap \left(\sum_{j:j\neq i} \operatorname{im}(p_j) \right).$$

Wegen $v \in \operatorname{im}(p_i)$ lässt sich v als $v = p_i(w)$ schreiben mit $w \in V$, und wegen $v \in \sum_{j:j\neq i} \operatorname{im}(p_j)$ aber auch als $v = \sum_{j:j\neq i} p_j(w_j)$, $w_j \in V$. Dann erhalten wir

$$v = p_i^2(w) = \sum_{j:j\neq i} p_i(p_j(w_j)) = 0,$$

die letzte Gleichung wegen (6.3) und die erste, weil p_i eine Projektion ist. ■

6.2 Invariante Unterräume

$f : V \to V$ sei ein Endomorphismus des K-Vektorraums V.

Definition 6.3 *Ein Unterraum $U \subset V$ heisst **invariant unter f**, wenn $f(u) \in U$ für alle $u \in U$ gilt.*

Die beiden trivialen Unterräume $\{0\}$ und V sind natürlich immer invariant. Andere invariante Unterräume nennen wir **nicht trivial**. Ein Endomorphismus braucht keine nicht trivialen Unterräume zu besitzen. Ein Beispiel ist etwa die Drehung von $\mathbb{R}^2$ um 45°, die gegeben ist durch die Matrix

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Wir werden später sehen, dass ein $\mathbb{C}$-Vektorraum der Dimension ≥ 2 stets nicht triviale Unterräume besitzt.

Es seien U_i, $1 \leq i \leq m$, Unterräume von V und $V = \bigoplus_{i=1}^m U_i$. Ferner seien für jedes i Endomorphismen $f_i \in \hom(U_i)$ gegeben. Wir konstruieren damit einen Endomorphismus $f : V \to V$, den wir mit $f = \bigoplus_{i=1}^m f_i$ bezeichnen. Zu $v \in V$ gehört eine eindeutige Darstellung $v = \sum_{i=1}^m u_i$, mit $u_i \in U_i$. Wir definieren

$$f(v) := \sum_{i=1}^m f_i(u_i).$$

Man überzeugt sich leicht, dass f linear ist: Sind $v, v' \in V$ mit den eindeutigen Darstellungen

$$v = \sum_{i=1}^m u_i,\ v' = \sum_{i=1}^m u_i',\ u_i, u_i' \in U_i$$

und sind $\alpha, \alpha' \in K$, so hat $\alpha v + \alpha' v'$ die eindeutige Darstellung

$$\alpha v + \alpha' v' = \sum_{i=1}^m (\alpha u_i + \alpha' u_i').$$

Demzufolge ist

$$\begin{aligned} f(\alpha v + \alpha' v') &= \sum_{i=1}^m f_i(\alpha u_i + \alpha' u_i') \\ &= \alpha \sum_{i=1}^m f_i(u_i) + \alpha' \sum_{i=1}^m f_i(u_i') = \alpha f(v) + \alpha' f(v'). \end{aligned}$$

Man beachte, dass die Unterräume U_i invariante Unterräume von f sind (wieso?).

In den nachfolgenden Kapiteln werden wir an Situationen interessiert sein, wo ein Endomorphismus invariante Unterräume hat, die den ganzen Vektorraum als direkte Summe aufspalten. Dazu der folgende einfache Satz:

Satz 6.4 *Sei $f \in \hom(V)$ und U_i, $1 \leq i \leq m$, seien invariante Unterräume von f. Ferner setzen wir voraus, dass $V = \bigoplus_{i=1}^m U_i$ gilt. Dann gilt*

$$f = \bigoplus_{i=1}^m f_i,$$

wobei f_i die Einschränkungen von f auf U_i sind: Für $u \in U_i$ ist $f_i(u) := f(u) \in U_i$.

Beweis. Da die U_i invariant sind, gilt $f_i \in \hom(U_i)$. Hat $v \in V$ die eindeutige Darstellung $v = \sum_{i=1}^m u_i$, $u_i \in U_i$, so gilt wegen der Linearität von f :

$$f(v) = \sum_{i=1}^m f(u_i) = \sum_{i=1}^m f_i(u_i).$$

■

Falls die Situation von Satz 6.4 vorliegt, vereinfacht sich die darstellende Matrix von f, falls man eine Basis verwendet, die sich aus Basen der U_i zusammensetzt. Seien also $\mathcal{U}_i = (u_{i,1}, \ldots, u_{i,k_i})$ Basen der Unterräume U_i. Nach Korollar 6.1 ist $\mathcal{U} := (u_{11}, u_{12}, \ldots, u_{m,k_m})$ eine Basis von V, falls $V = \bigoplus_{i=1}^{m} U_i$ gilt. Wir können nun die darstellende Matrix von f bezüglich dieser Basis sehr einfach aus den darstellenden Matrizen für die Restriktionen f_i zusammenstellen. Seien A_i die darstellenden Matrizen der f_i bezüglich $\mathcal{U}_i$. Die A_i sind $k_i \times k_i$-Matrizen. Die j-te Spalte von A_i enthält die Komponenten von $f_i(u_{ij})$ bezüglich der Basis $\mathcal{U}_i$. Nun gilt aber $f(u_{ij}) = f_i(u_{ij})$. Demzufolge erhält man die Komponenten von $f(u_{ij})$ bezüglich der Basis $\mathcal{U}$ einfach wie folgt: Zunächst kommen $k_1 + \ldots + k_{i-1}$ Nullen, darauf folgt die j-te Spalte von A_i und danach kommen wieder $k_{i+1} + \ldots + k_m$ Nullen. Die darstellende Matrix A von f bezüglich der Basis $\mathcal{U}$ hat also die folgende Blockstruktur:

$$A = \begin{pmatrix} A_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & A_m \end{pmatrix}.$$

Die Nulleinträge sind dabei Nullmatrizen der entsprechenden Grösse, z.B. die Null in der ersten Zeile und der zweiten Spalte ist die $k_1 \times k_2$-Nullmatrix.

Besonders einfach ist die Situation, wenn die Dimensionen der U_i alle gleich 1 sind. In diesem Fall sind die A_i 1×1-Matrizen, d.h. einfach Körperelemente: $A_i = (a_i)$, $a_i \in K$. Liegt diese Situation vor, so ist die obige darstellende Matrix A natürlich einfach eine Diagonalmatrix.

Definition 6.4 *Sei V ein endlichdimensionaler Vektorraum und $f \in \hom(V)$. Existiert eine Familie von eindimensionalen invarianten Unterräumen U_i mit $V = \bigoplus_{i=1}^{m} U_i$, so heisst f* ***diagonalisierbar.***

Aus der obigen Diskussion folgt also, dass wenn f diagonalisierbar ist, eine Basis existiert, in der die darstellende Matrix von f eine Diagonalmatrix ist. Existiert umgekehrt eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$, bezüglich der die darstellende Matrix Diagonalgestalt hat, so folgt ganz einfach, dass die Situation der obigen Definition vorliegt: Man nimmt einfach $U_i := L[v_i]$. Diagonalisierbarkeit eines Endomorphismus ist also gleichbedeutend damit, dass eine Basis existiert, bezüglich der die darstellende Matrix Diagonalgestalt hat.

Wir können das noch etwas anders formulieren. Ist eine beliebige Basis $\mathcal{V} = (v_1, \ldots, v_n)$ gegeben und ist A die darstellende Matrix von f bezüglich dieser Basis, so ist f genau dann diagonalisierbar, wenn eine reguläre Matrix S existiert, sodass $S^{-1}AS$ eine Diagonalmatrix ist. Dies folgt ganz einfach aus der Diskussion der Transformation der darstellenden Matrix bei Basiswechsel in Kapitel 4.4.

Die Situation mit eindimensionalen Unterräumen ist so wichtig, dass wir ihr ein besonderes Unterkapitel zuweisen:

6.3 Eigenwerte und Eigenvektoren

Während des ganzen Unterkapitels sei $f : V \to V$ ein Endomorphismus des K-Vektorraums V. Für die Diskussion weiter unten brauchen wir eine einfache Ergänzung zu der Diskussion von Isomorphismen aus Kapitel 4.

Lemma 6.2 *Sei V endlichdimensional und f ein Endomorphismus von V. Dann ist f genau dann ein Isomorphismus, wenn* $\ker(f) = \{0\}$ *ist.*

Beweis. Sei $\ker(f) = \{0\}$. Dann ist wegen $\dim(V) = \dim(\ker(f)) + \dim(\operatorname{im}(f))$ (Satz 4.18) $\dim(\operatorname{im}(f)) = \dim(V)$ und demzufolge $\operatorname{im}(f) = V$. Nach Lemma 4.6 folgt, dass f ein Isomorphismus ist.

Ist umgekehrt $\ker(f) \neq \{0\}$ so folgt aus demselben Lemma, dass f kein Isomorphismus ist. ■

Wenn immer wir Determinanten verwenden, setzen wir voraus, dass $\operatorname{char}(K) \neq 2$ ist.

Wir untersuchen in diesem Abschnitt eindimensionale invariante Unterräume. Ist $U \subset V$ ein eindimensionaler invarianter Unterraum: $U = L[u]$, mit $u \in V$, $u \neq 0$, so gilt $f(u) \in U$, d.h. es existiert $\lambda \in K$ mit $f(u) = \lambda u$. Natürlich gilt dann für jeden anderen Vektor $w = \alpha u \in U$, $\alpha \in K$, die Gleichung $f(w) = f(\alpha u) = \alpha f(u) = \alpha\lambda u = \lambda\alpha u = \lambda w$. Mit anderen Worten: Ist U ein invarianter Unterraum, so existiert ein Skalar $\lambda \in K$, sodass jeder Vektor in U unter f einfach mit λ gestreckt wird. Eine derartige Zahl λ nennt man Eigenwert von f.

Definition 6.5 *a) Eine Zahl $\lambda \in K$ heisst **Eigenwert** des Endomorphismus $f \in \hom(V)$, wenn ein Vektor $u \neq 0$ existiert mit*

$$f(u) = \lambda u.$$

*b) Das **Spektrum von f**,* $\operatorname{spec}(f)$*, ist definiert als die Menge aller Eigenwerte von f.*

*c) Ist $\lambda \in \operatorname{spec}(f)$, so heisst jeder Vektor $u \neq 0$ mit $f(u) = \lambda u$ ein **Eigenvektor** zu λ.*

Bemerkung 6.2 *a) Es ist sehr wichtig, dass in der Definition eines Eigenwertes verlangt wird, dass ein Vektor u existiert,* der von Null verschieden ist, *mit $f(u) = \lambda u$. In der Tat erfüllt natürlich der Nullvektor 0 stets die Gleichung $f(0) = \lambda 0$, sodass das gar keine Bedingung an λ wäre.*

b) $\lambda = 0$ kann jedoch durchaus ein Eigenwert sein. $0 \in K$ ist genau dann ein Eigenwert, wenn ein Vektor $u \neq 0$ existiert mit $f(u) = 0$. Nach Lemma 6.2 ist das gleichbedeutend damit, dass $\ker(f) \neq \{0\}$ *ist. Im Falle, dass V*

endlichdimensional ist, ist das gleichbedeutend damit, dass f kein Isomorphismus ist. Wie wir in Kapitel 5 gesehen hatten, ist das gleichbedeutend damit, dass $\det(f) = 0$ *ist.*

c) Die Diskussion zu Beginn des Abschnittes zeigt, dass $\operatorname{spec}(f) \neq \emptyset$ *genau dann gilt, wenn f mindestens einen eindimensionalen invarianten Unterraum hat.*

d) Das Spektrum eines Endomorphismus kann durchaus leer sein. So hat etwa die Drehung um 45° von $\mathbb{R}^2$ offensichtlich keinen eindimensionalen invarianten Unterraum, und demzufolge gibt es auch keinen Eigenwert.

e) Wir diskutieren hier ausschliesslich den Fall endlichdimensionaler Vektorräume. Die Verhältnisse bei unendlichdimensionalen Vektorräumen können sehr kompliziert sein.

Satz 6.5

$$\operatorname{spec}(f) = \{\lambda \in K : \det(f - \lambda \operatorname{id}_V) = 0\}.$$

Hier ist $f - \lambda \operatorname{id}_V$ *der Endomorphismus* $V \ni v \to f(v) - \lambda v$.

Beweis. λ ist genau dann ein Eigenwert, wenn ein Vektor $u \neq 0$ existiert mit $f(u) = \lambda u$, d.h. $(f - \lambda \operatorname{id}_V)(u) = 0$. Wie wir schon oben gesehen haben, ist das gleichbedeutend damit, dass $f - \lambda \operatorname{id}_V$ kein Isomorphismus ist, d.h. dass $\det(f - \lambda \operatorname{id}_V) = 0$ ist. ■

Definition 6.6 *Ist* $\lambda \in \operatorname{spec}(f)$, *so ist*

$$E(\lambda) := \{u \in V : f(u) = \lambda u\} = \ker(f - \lambda \operatorname{id}_V)$$

der ***Eigenraum*** *von λ.*

Wir nehmen auch den Nullvektor als Element des Eigenraums. Auf diese Weise ist dann $E(\lambda)$ ein Unterraum von V. Wir können natürlich $E(\lambda)$ für jedes Element $\lambda \in K$ definieren. $\lambda \in \operatorname{spec}(f)$ ist dann gleichbedeutend damit, dass $\dim(E(\lambda)) \geq 1$ ist. Ein Eigenraum eines Eigenwertes braucht nicht eindimensional zu sein. So hat id_V natürlich V als Eigenraum zum einzigen Eigenwert 1.

Satz 6.6 *Seien $\lambda_1, \ldots, \lambda_n$ verschiedene Eigenwerte von f, und sei für jedes i der Vektor u_i ein Eigenvektor ($\neq 0$) zu λ_i. Dann sind $u_1, \ldots, u_n$ linear unabhängig.*

Beweis. Wir führen eine Induktion nach n. Für $n = 1$ ist die Aussage trivial, denn ein einzelner Vektor $\neq 0$ ist linear unabhängig. Sei $n \geq 2$, und sei

$$\sum_{i=1}^{n} \alpha_i u_i = 0. \tag{6.5}$$

Anwendung von f ergibt

$$0 = f\left(\sum_{i=1}^{n} \alpha_i u_i\right) = \sum_{i=1}^{n} \alpha_i f(u_i) = \sum_{i=1}^{n} \alpha_i \lambda_i u_i. \tag{6.6}$$

Kombination von (6.5) und (6.6) ergibt:

$$0 = \lambda_n \sum_{i=1}^{n} \alpha_i u_i - \sum_{i=1}^{n} \lambda_i \alpha_i u_i = \sum_{i=1}^{n-1} (\lambda_n - \lambda_i)\, \alpha_i u_i.$$

Nach Induktionsvoraussetzung sind die $u_1, \ldots, u_{n-1}$ linear unabhängig. Demzufolge gilt $(\lambda_n - \lambda_i)\, \alpha_i = 0$ für $i = 1, \ldots, n-1$. Da alle Eigenwerte verschieden sind, folgt also $\alpha_1 = \ldots = \alpha_{n-1} = 0$. Aus (6.5) folgt dann aber $\alpha_n u_n = 0$ und wegen $u_n \neq 0$ folgt auch $\alpha_n = 0$. Damit ist die lineare Unabhängigkeit von $u_1, \ldots, u_n$ gezeigt. ■

Korollar 6.2 *a) Seien $\lambda_1, \ldots, \lambda_r$ verschiedene Eigenvektoren. Dann ist die Summe der Eigenräume eine direkte Summe:*

$$\sum_{i=1}^{r} E(\lambda_i) = \bigoplus_{i=1}^{r} E(\lambda_i).$$

b) Ist $n := \dim(V) < \infty$, so gibt es höchstens n verschiedene Eigenwerte.

Beweis. a) folgt sofort aus dem vorangegangenen Satz. b) folgt aus a). ■

Wie wir in Satz 6.5 gesehen haben gilt $\lambda \in \operatorname{spec}(f)$ genau dann, wenn $\det(f - \lambda \operatorname{id}_V) = 0$ ist. Wir definieren die Funktion $\chi_f : K \to K$, $\chi_f(\lambda) := \det(f - \lambda \operatorname{id}_V)$.

Wir wollen nun χ_f als formales Polynom auffassen — wir ersetzen dazu, wie im ersten Kapitel, λ durch x und schreiben $\chi_f(x)$: Indem wir die darstellende Matrix A von f bezüglich einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$ wählen, können wir dieses Polynom formal definieren durch

$$\chi_f(x) := \det(A - xE_n) = \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi) \prod_{j=1}^{n} \left(a_{\pi(j),j} - x\delta_{\pi(j),j}\right).$$

(Zu zeigen bliebe an dieser Stelle, dass diese Definition unabhängig ist von der Wahl der Basis $\mathcal{V}$. Dies ist aber auch in diesem formalen Kontext richtig — wir verweisen hierzu auf die Diskussion in Unterkapitel 5.4.)

Definition 6.7 *$\chi_f(x)$ heisst das **charakteristische Polynom** von f.*

Wir unterscheiden das charakteristische Polynom von der durch dieses Polynom definierten Abbildung $K \to K$. Mehr dazu im Abschnitt 6.4.

Satz 6.7 *Ist* $n := \dim(V)$, *so ist* $\chi_f(x)$ *ein Polynom von Grad* n *in* x.

Beweis. Sei A die darstellende Matrix von f bezüglich der Basis $\mathcal{V} = (v_1, \ldots, v_n)$. Dann ist

$$\chi_f(x) = \sum_{\pi \in \Sigma_n} \operatorname{sign}(\pi) \prod_{j=1}^{n} \left(a_{\pi(j),j} - x\delta_{\pi(j),j}\right).$$

Nun sind jedoch $\prod_{j=1}^{n} \left(a_{\pi(j),j} - x\delta_{\pi(j),j}\right)$ offensichtlich Polynome von Grad $\leq n$ in x. Demzufolge ist auch $\chi_f(x)$ ein Polynom von Grad $\leq n$. Wir können jedoch noch etwas mehr aussagen: Die Polynome $\prod_{j=1}^{n} \left(a_{\pi(j),j} - x\delta_{\pi(j),j}\right)$ sind für $\pi \neq \mathrm{id}$ Polynome von Grad $< n$, denn in diesem Fall enthalten nicht alle der Faktoren wirklich x. Hingegen ist für $\pi = \mathrm{id}$

$$\prod_{j=1}^{n} \left(a_{\pi(j),j} - x\delta_{\pi(j),j}\right) = \prod_{j=1}^{n} (a_{jj} - x).$$

Dies ist ein Polynom in x, das mit $(-1)^n x^n$ beginnt. Daraus folgt, dass $\chi_f(x)$ ein Polynom in x ist, das mit $(-1)^n x^n$ beginnt, also insbesondere ein Polynom von Grad n. ■

Die Koeffizienten des charakteristischen Polynoms sind im allgemeinen komplizierte Ausdrücke. Die Berechnung erfolgt natürlich in der Regel über die Wahl einer Basis und die darstellende Matrix A von f. Wir schreiben dann auch $\chi_A(x)$ für $\det(A - xE_n)$ und bezeichnen das als das charakteristische Polynom der Matrix A. Da $\chi_f(x) = \chi_A(x)$ für jede Wahl einer Basis, gilt: Ähnliche Matrizen haben dieselbe charakteristischen Polynome. Sei

$$\det(A - xE_n) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$$

Die Koeffizienten von a_i hängen in komplizierter Weise von den Komponenten a_{ij} der Matrix A ab. Einige der Koeffizienten sind jedoch einfach zu berechnen. Wie wir schon gesehen haben, ist der höchste Koeffizient $a_n = (-1)^n$. Der nächste ist ebenfalls einfach: Für $\pi \neq \mathrm{id}$ ist nämlich $\prod_{j=1}^{n} \left(a_{\pi(j),j} - x\delta_{\pi(j),j}\right)$ ein Polynom von Grad höchstens $n-2$, denn $\pi(j) \neq j$ gilt in diesem Fall für mindestens zwei j. (Eine Permutation, die nicht die Identität ist, kann nicht $n-1$ Fixpunkte haben). Nun beginnt jedoch das Polynom $\prod_{j=1}^{n} (a_{jj} - x)$ wie folgt:

$$\prod_{j=1}^{n} (a_{jj} - x) = (-1)^n x^n + (-1)^{n-1} \sum_{j=1}^{n} a_{jj}\, x^{n-1} + \ldots$$

Es folgt daher $a_{n-1} = (-1)^{n-1} \sum_{j=1}^{n} a_{jj} = (-1)^{n-1} \operatorname{trace}(A)$, wobei $\operatorname{trace}(A) := \sum_{j=1}^{n} a_{jj}$ die sogenannte **Spur** der Matrix A ist. a_0 ist ebenfalls einfach:

$$a_0 = \chi_A(0) = \det(A).$$

Beispiel 6.3 *$f : \mathbb{R}^2 \to \mathbb{R}^2$ sei durch die Matrix $A = \begin{pmatrix} -1 & 8 \\ -1 & 5 \end{pmatrix}$ gegeben. Die Determinante dieser Matrix ist 3, die Spur ist 4. Demzufolge ist*

$$\chi_A(x) = x^2 - 4x + 3 = (x-1)(x-3).$$

Damit ist

$$\operatorname{spec}(f) = \{1, 3\}.$$

Die Eigenvektoren zu den Eigenwerten sind nun einfach zu berechnen. Zu 1 :

$$\begin{pmatrix} -1 & 8 \\ -1 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

oder

$$\begin{pmatrix} -2 & 8 \\ -1 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0.$$

Nun sieht man, dass die 2×2-Matrix singulär ist (das hat man ja gerade so eingerichtet) und das Gleichungssystem hat daher eine nicht-triviale Lösung. Eine Lösung ist z.B.

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}.$$

Der Lösungsraum ist eindimensional. Der Eigenraum zum Eigenwert 1 ist daher

$$E(1) = L\left[\begin{pmatrix} 4 \\ 1 \end{pmatrix}\right].$$

Analog erhält man

$$E(3) = L\left[\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right].$$

Die Dimension des Eigenraumes $E(\lambda)$ ist per Definition mindestens 1, sie kann aber auch grösser sein.

Definition 6.8 $\dim(E(\lambda))$ *heisst die* ***geometrische Vielfachheit*** *von $\lambda \in \operatorname{spec}(f)$.*

Ein triviales Beispiel dazu. id_V hat natürlich nur den Eigenwert 1. Dieser hat geometrische Vielfachheit $\dim(V)$.

Wir kommen jetzt nochmals auf den Begriff der Diagonalisierbarkeit eines Endomorphismus zurück. Wie üblich setzen wir voraus, dass $f : V \to V$ ein Endomorphismus ist. Wie wir im letzten Unterkapitel gesehen hatten, ist Diagonalisierbarkeit gleichbedeutend damit, dass eine Basis existiert, bezüglich der die darstellende Matrix Diagonalgestalt hat. Dies ist jedoch gleichbedeutend damit, dass alle Basiselemente Eigenvektoren sind. Wir erhalten also die folgende Aussage:

Lemma 6.3 *f ist genau dann diagonalisierbar, wenn eine Basis aus Eigenvektoren existiert.*

Eine etwas andere Formulierung desselben Sachverhalts ist:

Lemma 6.4 *f ist genau dann diagonalisierbar, wenn*

$$V = \bigoplus_{\lambda \in \mathrm{spec}(f)} E(\lambda) \tag{6.7}$$

gilt.

Beweis. Gilt (6.7), so können wir in jedem der Unterräume $E(\lambda)$ eine Basis wählen. Die Vereinigung dieser Basen bildet dann wegen (6.7) eine Basis von V.

Wir setzen umgekehrt voraus, dass eine Basis von Eigenvektoren existiert. Die Anzahl der Vektoren dieser Basis, die für einen Eigenwert λ in $E(\lambda)$ liegen, ist sicher höchstens $\dim(E(\lambda))$. Damit folgt $\dim(V) \leq \sum_{\lambda \in \mathrm{spec}(f)} \dim(E(\lambda))$. Da die Summe der Eigenräume auf jeden Fall direkt ist, folgt daraus $\dim(V) = \sum_{\lambda \in \mathrm{spec}(f)} \dim(E(\lambda))$ und (6.7). ■

Wir können die Sache auch noch in der Sprache von Matrizen ausdrücken: Wir nennen eine $n \times n$-Matrix A **diagonalisierbar,** wenn eine reguläre $n \times n$-Matrix S existiert, sodass $S^{-1}AS$ eine Diagonalmatrix ist, d.h. wenn A ähnlich zu einer Diagonalmatrix ist. Ein Endomorphismus f ist nach der vorangegangen Diskussion genau dann diagonalisierbar, wenn die darstellende Matrix von f bezüglich einer beliebigen Basis im obigen Sinne diagonalisierbar ist.

Ein hinreichendes (aber kein notwendiges) Kriterium für die Diagonalisierbarkeit eines Endomorphismus ist die Existenz von $n := \dim(V)$ verschiedenen Eigenwerten:

Satz 6.8 *Hat das charakteristische Polynom $\chi_f(x)$ n verschiedene Nullstellen, so ist f diagonalisierbar.*

Beweis. Die Nullstellen des charakteristischen Polynoms sind genau die Eigenwerte. Unter der Voraussetzung des Satzes gibt es also n verschiedene Eigenwerte. Seien $v_1, \ldots, v_n$ zugehörige Eigenvektoren. Nach Satz 6.6 sind diese Eigenvektoren linear unabhängig. Sie bilden also eine Basis von V, was gleichbedeutend mit der Diagonalisierbarkeit ist. ■

Wir geben nun einige einfache Beispiele zur Diagonalisierbarkeit. Alle Beispiele sind in $\mathbb{R}^n$ und die Endomorphismen sind durch Matrizen gegeben.

Beispiel 6.4

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 3 \end{pmatrix}.$$

Es folgt sofort $\operatorname{spec}(A) = \{1, 2, 3\}$ *und mit Satz 6.8 folgt, dass A diagonalisierbar ist. Um* $S \in GL(3, \mathbb{R})$ *zu finden, mit* $S^{-1}AS = \text{diagonal}$*, müssen wir nur eine Basis aus Eigenvektoren finden.*

Einen Eigenvektor zu 1 *finden wir durch Lösen des homogenen Gleichungssystems*

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 3 \end{pmatrix} x = x$$

für $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$*. Eine Lösung ist* $x = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$*. Analog findet man Eigenvektoren zum Eigenwert* 2 *als* $x = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$ *und zu* 3 *als* $x = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$*. Schreiben wir diese Eigenvektoren in die Spalten einer Matrix:*

$$S := \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix},$$

so erhalten wir

$$S^{-1}AS = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Beispiel 6.5 $n = 2$ *und*

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

1 *ist offenbar der einzige Eigenwert von A. Der zugehörige Eigenraum ist die Lösungsmenge des homogenen Gleichungssystems*

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Das ist äquivalent zur Gleichung $x_1 = 0$*. Wir haben also*

$$E(1) = L\left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right].$$

Die Dimension dieses Eigenraums ist 1*. Nach Lemma 6.4 ist A nicht diagonalisierbar.*

Beispiel 6.6 *Wir ändern das obige Beispiel leicht ab und betrachten*

$$A = \begin{pmatrix} 1 & 0 \\ 1 & a \end{pmatrix}$$

mit $a \neq 1$*. Dann besteht das Spektrum aus zwei Eigenwerten, und A ist demzufolge diagonalisierbar.*

Beispiel 6.7

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Das charakteristische Polynom ist

$$\chi_A(x) = (1-x)^2 + 1.$$

Dieses Polynom hat keine Nullstellen in $\mathbb{R}$. *Demzufolge ist* $\operatorname{spec}(A) = \emptyset$. *Wir können A jedoch auch also Endomorphismus von* $\mathbb{C}^2$ *betrachten. Im Komplexen hat* $\chi_A(x)$ *die beiden Nullstellen* $1+i$ *und* $1-i$. *Da dies zwei verschiedene Eigenwerte sind, ist also A im Komplexen diagonalisierbar, das heisst, es gibt eine Matrix* $S \in GL(2, \mathbb{C})$ *mit*

$$S^{-1}AS = \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix}.$$

S hat einfach die Eigenvektoren zu den beiden Eigenwerten in den Spalten.

Bemerkung 6.3 *Reelle symmetrische Matrizen, d.h. Matrizen A mit* $A^T = A$, *sind reell diagonalisierbar. Das wird später bewiesen werden. Die Eigenschaft der Symmetrie hat jedoch keine basisunabhängige Bedeutung: Ist eine symmetrische Matrix A die darstellende Matrix eines Endomorphismus, so ist die darstellende Matrix desselben Endomorphismus bezüglich einer anderen Basis im allgemeinen nicht symmetrisch.*

6.4 Polynome

6.4.1 Teilbarkeit

Sei K ein Körper. Wir hatten schon früher den Polynomring $K[x]$ betrachtet. Die Elemente von $K[x]$ sind die (formalen) Polynome

$$p(x) = \sum_{j=0}^{n} a_j x^j,$$

wobei wir $x^0 := 1$ setzen. Wir setzen im allgemeinen voraus, dass $a_n \neq 0$ ist für $n \geq 1$. Das Polynom mit allen Koeffizienten 0 heisst das 0-Polynom. Wir hatten schon früher eine Multiplikation und eine Addition auf $K[x]$ definiert. $(K[x], +, \cdot)$ ist ein kommutativer Ring mit Eins. Das Neutralelement der Multiplikation (die "Eins" ist das Polynom 0-ten Grades mit $a_0 = 1$. Ist der höchste Koeffizient $a_n \neq 0$, so bezeichnet man n als den **Grad** des Polynoms. Wir schreiben ihn als $\operatorname{grad}(p(x))$. Es ist bequem (und nur eine Konvention), dem Nullpolynom den Grad $-\infty$ zuzuweisen. Dies hat den Vorteil, dass die folgende Beziehung gilt:

$$\operatorname{grad}(p(x) \cdot q(x)) = \operatorname{grad}(p(x)) + \operatorname{grad}(q(x)),$$

wobei $-\infty + n = n + (-\infty) := -\infty$ gesetzt wird.

Wie schon im ersten Kapitel erwähnt, fassen wir Polynome (zunächst) einfach als endliche Folgen $(a_0, a_1, \ldots, a_n)$ auf, mit den entsprechenden Additions- und Multiplikationsregeln. Die "Variable" x hat (im Moment) keinerlei Bedeutung und ist nur ein Label für die bequeme Notation. Obwohl wir in der Regel $p(x)$, $q(x)$ für ein Polynom schreiben, so ist das daher nicht als eine Funktion an der Stelle x zu verstehen. Wir nennen ein Polynom $\neq 0$ **normiert**, wenn der höchste Koeffizient 1 ist. Wir können jedes Polynom $\neq 0$ normieren, indem wir es mit einem Körperelement multiplizieren.

Den Körper K können wir als Teilmenge von $K[x]$ auffassen: Wir ordnen jedem Körperelement α das Polynom $p(x) = \alpha$ zu. Wir werden in dieser Weise immer stillschweigend K als Teilmenge von $K[x]$ auffassen.

Wir benötigen einige Begriffsbildungen aus der Ringtheorie.

Definition 6.9 *Sei $(R, +, \cdot)$ ein Ring mit Eins (nicht notwendigerweise kommutativ). Ein Element $r \in R$ heisst **Einheit**, wenn es invertierbar ist, d.h. wenn $r' \in R$ existiert mit*

$$rr' = r'r = 1.$$

Wie wir schon wissen, ist 0 keine Einheit. Der Ring $\mathbb{Z}$ hat offenbar die beiden Einheiten 1 und -1.

Lemma 6.5 *Die Menge der Einheiten von $K[x]$ ist $K \setminus \{0\}$.*

Beweis. Der ganz einfache Beweis sei dem Leser überlassen. ■

Definition 6.10 *$p(x), q(x)$ seien zwei von 0 verschiedene Polynome. Man sagt, $p(x)$ **teilt** $q(x)$, wenn ein Polynom $h(x)$ existiert mit $q(x) = h(x)\,p(x)$. Notation: $p(x) \mid q(x)$. In diesem Fall heisst $p(x)$ ein **Teiler** von $q(x)$. $p(x)$ heisst **echter Teiler** von $q(x)$, wenn $1 \leq \operatorname{grad}(p(x)) < \operatorname{grad}(q(x))$ gilt. Ein Polynom $q(x)$ von Grad ≥ 1 heisst **irreduzibel**, wenn es keinen echten Teiler besitzt.*

*n Polynome $p_1(x), \ldots, p_n(x)$ vom Grad ≥ 1 heissen **teilerfremd,** wenn sie keinen gemeinsamen Teiler vom Grad ≥ 1 besitzen.*

Bemerkung 6.4 *a) Per Definition ist jedes Polynom von Grad 1 irreduzibel.*

b) Gilt $p(x) \mid q(x)$ und sind $\alpha, \beta \in K \setminus \{0\}$, so gilt auch $\alpha p(x) \mid \beta q(x)$. Das Polynom $p(x)$ teilt also das Polynom $q(x)$ genau dann, wenn entsprechendes für die zugehörigen normierten Polynome gilt. Wir können uns also bei der Untersuchung der Teilbarkeit stets auf normierte Polynome zurückziehen.

c) Gilt für zwei Polynome $\neq 0$ $p(x) \mid q(x)$ und $q(x) \mid p(x)$, so existiert $\alpha \in K \setminus \{0\}$ mit $p(x) = \alpha q(x)$.

d) Die Polynome von Grad 0, d.h. die konstanten Polynome $\neq 0$ sind trivialerweise Teiler von allen Polynomen $\neq 0$. Diese trivialen Teiler spielen natürlich in der Theorie keine Rolle. Von daher kommt die Beschränkung bei den echten Teilern auf den Grad ≥ 1.

Definition 6.11 *Ein Körper K heisst* ***algebraisch abgeschlossen****, wenn $K[x]$ keine irreduziblen Polynome vom Grad ≥ 2 besitzt.*

Satz 6.9 (Hauptsatz der Algebra) $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Dieser Satz (in der Formulierung des nächsten Unterabschnitts) wurde in Diff-Int. I bewiesen.

$\mathbb{R}$ ist nicht algebraisch abgeschlossen, wie man sich ohne Schwierigkeiten überlegen kann: Das Polynom x^2+1 ist irreduzibel. Um dies nachzuweisen, nehmen wir an, dass dieses Polynom einen echten Teiler besitzt. Dieser muss per Definition den Grad 1 haben. Daraus folgt sofort, dass $a, b \in \mathbb{R}$ existieren müssten, sodass

$$x^2+1 = (x+a)(x+b)$$

gelten würde. Durch Koeffizientenvergleich ergibt sich $a+b=0$ und $ab=1$. Das ist jedoch offensichtlich nicht möglich in $\mathbb{R}$ (aber natürlich in $\mathbb{C}$ mit $a=i, b=-i$). $\mathbb{R}[x]$ hat jedoch keine irreduziblen Polynome von Grad >2, wie wir später sehen werden. Für den Körper $\mathbb{Q}$ ist die Sache noch "schlimmer". Tatsächlich hat $\mathbb{Q}[x]$ irreduzible Polynome jeden Grades, was wir jedoch in dieser Vorlesung nicht zeigen können.

Division mit Rest: Aus dem Gymnasium sollte bekannt sein, wie man Polynome mit Rest teilt: Sind $p(x)$ und $q(x)$ zwei Polynome, $q(x) \neq 0$, so existieren eindeutig Polynome $h(x)$ und $r(x)$ mit

$$p(x) = h(x)\,q(x) + r(x),$$

$$\operatorname{grad}(r(x)) < \operatorname{grad}(q(x)).$$

Der Algorithmus zur Bestimmung von $h(x)$ und $r(x)$ soll hier nicht wiederholt werden und sollte aus der Schule bekannt sein (zumindest für $K=\mathbb{R}$). Wir beweisen kurz die Eindeutigkeit: Seien

$$p(x) = h(x)\,q(x) + r(x) \text{ und } p(x) = h'(x)\,q(x) + r'(x)$$

zwei derartige Darstellungen. Dann folgt

$$0 = (h(x) - h'(x))\,q(x) + (r(x) - r'(x)).$$

Wäre $h(x) \neq h'(x)$, so hätte $(h(x)-h'(x))\,q(x)$ einen Grad $\geq \operatorname{grad}(q(x))$. Andererseits gilt aber $\operatorname{grad}(r(x)-r'(x)) < \operatorname{grad}(q(x))$. Daraus würde folgen, dass $\operatorname{grad}((h(x)-h'(x))\,q(x) + (r(x)-r'(x))) \geq 0$ gilt, was aber nicht möglich ist. Somit folgt $h(x) = h'(x)$ und damit auch $r(x) = r'(x)$.

6.4.2 Nullstellen von Polynomen

Jedes Polynom $p(x) \in K[x]$ definiert eine Abbildung $p : K \to K$. Für $\alpha \in K$ ist $p(\alpha) \in K$ dadurch definiert, dass man den Label x durch das "konkrete" Körperelement α ersetzt und $a_0 + a_1\alpha + \ldots + a_n\alpha^n$ in K ausrechnet. Wie schon früher diskutiert, soll man zwischen einem Polynom und der zugehörigen Abbildung unterscheiden. Es wäre daher korrekter, für die zu einem Polynom $p(x)$ gehörende Abbildung eine gesonderte Notation zu verwenden, z.B. $\widetilde{p} : K \to K$. Um die Notation nicht zu überladen, lassen wir es jedoch bei p bewenden. Wir benützen jedoch in der Regel kleine griechische Buchstaben für Körperelemente und schreiben dann $p(\alpha)$, wenn wir den Wert dieser Funktion an der Stelle α meinen.

Beispiel 6.8 *Wir betrachten den Körper $\mathbb{Z}_2$ und die beiden Polynome*

$$p(x) = x + x^2 + x^3,$$

$$q(x) = x^2 + x^3 + x^4.$$

Das sind zwei offensichtlich verschiedene Polynome, die jedoch dieselbe Abbildung $\mathbb{Z}_2 \to \mathbb{Z}_2$ definieren.

Definition 6.12 *Sei $p(x) \in K[x]$. $\alpha \in K$ heisst **Nullstelle** des Polynoms, wenn $p(\alpha) = 0$ ist.*

Wieder etwas Vorsicht mit der Notation: Wenn wir $p(x) = 0$ schreiben, meinen wir dass $p(x)$ das Nullpolynom ist. Wenn wir $p(\alpha) = 0$ schreiben, meinen wir, dass die zum Polynom gehörende Funktion an der Stelle α gleich dem Körperelement Null ist.

Ein Polynom von Grad 1 hat stets genau eine Nullstelle: Ist $p(x) = a_0 + a_1 x$, so ist $\alpha := -a_0/a_1$ die eindeutige Nullstelle dieses Polynoms. Polynome brauchen jedoch keine Nullstellen zu besitzen. So hat z.B. in $\mathbb{R}[x]$ das Polynom $x^{100} + 1$ keine Nullstelle.

Satz 6.10 *Sei $p(x) \in K[x]$ nicht das Nullpolynom und $\alpha \in K$. α ist genau dann eine Nullstelle dieses Polynoms, wenn das Polynom $x - \alpha$ das Polynom $p(x)$ teilt.*

Beweis. Wir dividieren $p(x)$ durch $x - \alpha$ mit Rest:

$$p(x) = (x - \alpha)\, h(x) + r(x).$$

Dabei gilt $\operatorname{grad}(r(x)) < \operatorname{grad}(x - \alpha) = 1$, d.h. $r(x)$ ist einfach eine Konstante: $r(x) = \beta$. Einsetzen von α ergibt

$$p(\alpha) = 0 \Longleftrightarrow \beta = 0.$$

■

Satz 6.11 *K ist genau dann algebraisch abgeschlossen, wenn jedes Polynom vom Grad ≥ 1 eine Nullstelle hat.*

Beweis. I) Wir setzen zunächst voraus, dass jedes Polynom vom Grad ≥ 1 eine Nullstelle hat. Sei $p(x)$ ein Polynom vom Grad ≥ 2 und α eine Nullstelle. Nach dem vorangegangen Satz gilt $x - \alpha \,|\, p(x)$. Demzufolge ist $p(x)$ nicht irreduzibel.

II) Wir setzen voraus, dass K algebraisch abgeschlossen ist. Sei $p(x)$ ein Polynom vom Grad ≥ 1. Wir zeigen mit Induktion nach $\operatorname{grad}(p(x))$, dass $p(x)$ eine Nullstelle hat. Ist $\operatorname{grad}(p(x)) = 1$, so ist dies klar. Sei also $\operatorname{grad}(p(x)) \geq 2$. Aus der algebraischen Abgeschlossenheit folgt, dass eine Zerlegung

$$p(x) = h(x)\, q(x)$$

existiert, wobei $\operatorname{grad}(q(x)) < \operatorname{grad}(p(x))$ ist. Nach Induktionsvoraussetzung hat also $q(x)$ eine Nullstelle $\alpha \in K$. Dann gilt auch $p(\alpha) = h(\alpha)\, q(\alpha) = 0$. Es ist also gezeigt, dass auch $p(x)$ eine Nullstelle hat. ■

Der sogenannte Hauptsatz der Algebra, also der Satz, dass $\mathbb{C}$ algebraisch abgeschlossen ist, besagt also, dass jedes nicht konstante komplexe Polynom eine Nullstelle hat. Der Satz wird üblicherweise so formuliert (und auch bewiesen).

Satz 6.12 *Sei $p(x)$ ein nicht konstantes Polynom und seien $\alpha_1, \ldots, \alpha_k$ seine Nullstellen. Dann hat $p(x)$ die bis auf die Reihenfolge der Faktoren eindeutige Darstellung*

$$p(x) = (x - \alpha_1)^{m_1} \cdot \ldots \cdot (x - \alpha_k)^{m_k}\, q(x),$$

wobei $q(x)$ eine Polynom ohne Nullstellen ist.

Beweis. Wir beweisen einen allgemeineren Satz im Unterkapitel 6.4.4 (Satz 6.16). ■

Korollar 6.3 *Es gilt*

$$\sum_{i=1}^{k} m_i \leq \operatorname{grad}(p(x)).$$

Insbesondere hat jedes Polynom höchstens so viele (verschiedene) Nullstellen, wie sein Grad ist.

Korollar 6.4 *In einem algebraisch abgeschlossenen Körper hat jedes Polynom $p(x) \neq 0$ eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung*

$$p(x) = \gamma\, (x - \alpha_1)^{m_1} \cdot \ldots \cdot (x - \alpha_k)^{m_k},$$

wobei $\alpha_1, \ldots, \alpha_k$ die verschiedenen Nullstellen sind und $\gamma \in K \setminus \{0\}$.

Definition 6.13 *Ist $p(x)$ ein Polynom mit den Nullstellen wie im obigen Satz 6.12. Dann heisst m_i die* ***algebraische Vielfachheit*** *der Nullstelle α_i.*

Ist $f : V \to V$ ein Endomorphismus und $\lambda \in \operatorname{spec}(f)$. Dann ist die ***algebraische Vielfachheit*** *dieses Eigenwertes definiert als die algebraische Vielfachheit von λ als Nullstelle des charakteristischen Polynoms.*

Satz 6.13 *Sei $f : V \to V$ ein Endomorphismus und $\lambda \in \operatorname{spec}(f)$. Dann ist die algebraische Vielfachheit von λ grösser oder gleich seiner geometrischen Vielfachheit.*

Beweis. Sei m die geometrische Vielfachheit von λ. Dann existieren m linear unabhängige Eigenvektoren zu $\lambda : v_1, \ldots, v_m$. Diese können zu einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$ von V ergänzt werden. Die darstellende Matrix von f in dieser Basis hat die Form

$$\begin{pmatrix} \lambda E_m & * \\ 0 & B \end{pmatrix},$$

wobei B eine $(n-m) \times (n-m)$-Matrix ist. Das charakteristische Polynom des Endomorphismus ist dann (unter Verwendung einer Übungsaufgabe)

$$\det \begin{pmatrix} (\lambda - x) E_m & * \\ 0 & B - xE_{n-m} \end{pmatrix} = (\lambda - x)^m \det(B - xE_{n-m}) = (\lambda - x)^m \chi_B(x).$$

Demzufolge ist die algebraische Vielfachheit $\geq m$. ■

Noch ein Zusammenhang mit der Diagonalisierbarkeit eines Endomorphismus:

Satz 6.14 *Sei K algebraisch abgeschlossen und $f : V \to V$ ein Endomorphismus eines endlichdimensionalen K-Vektorraums V. Dann ist f genau dann diagonalisierbar, wenn für jeden Eigenwert $\lambda \in \operatorname{spec}(f)$ die algebraische Vielfachheit gleich der geometrischen ist.*

Beweis. I) Sei zunächst vorausgesetzt, dass f diagonalisierbar ist. Für diese Richtung brauchen wir die algebraische Abgeschlossenheit von K nicht. Ist f diagonalisierbar, so existiert eine Basis aus Eigenvektoren, d.h. es existiert eine Basis bezüglich der die darstellende Matrix eine Diagonalmatrix

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

ist. In der Diagonalen von D stehen die Eigenwerte. Natürlich können einzelne Eigenwerte mehrfach vorkommen. Das charakteristische Polynom von f ist gleich $\det(D - xE_n) = \prod_{i=1}^{n} (\lambda_i - x)$. Zu jedem $\lambda \in \operatorname{spec}(f)$ steht λ so oft in der Diagonalen dieser Matrix wie die Dimension von $E(\lambda)$ ist. Das ist aber gleich

der Anzahl des Vorkommens des Faktors $(\lambda - x)$ im obigen Produkt, also gleich der algebraischen Vielfachheit.

II) Wir setzen voraus, dass K algebraisch abgeschlossen ist und dass für jedes $\lambda \in \operatorname{spec}(f)$ die algebraische Vielfachheit gleich der geometrischen ist. Wir wissen schon, dass die Summe der Eigenräume direkt ist (Korollar 6.2), und nach Lemma 6.4 müssen wir nur nachweisen, dass diese Summe auch ganz V aufspannt, d.h. dass (6.7) gilt. Dies ist nun gleichbedeutend damit, dass

$$n := \dim V = \sum_{\lambda \in \operatorname{spec}(f)} \dim\left(E\left(\lambda\right)\right) \tag{6.8}$$

ist.

Da K algebraisch abgeschlossen ist, hat das charakteristische Polynom die Darstellung

$$\chi_f\left(x\right) = \left(-1\right)^n \prod_{\lambda \in \operatorname{spec}(f)} \left(x - \lambda\right)^{m_\lambda},$$

wobei m_λ die algebraische Vielfachheit von λ ist. Daraus folgt $n = \sum_{\lambda \in \operatorname{spec}(f)} m_\lambda$. Wenn wir voraussetzen, dass die algebraischen Vielfachheiten gleich den geometrischen sind, folgt also (6.8). ■

Zum Schluss noch ein einfaches Beispiel eines irreduziblen Polynoms von Grad 3:

Beispiel 6.9 *In $\mathbb{Z}_2\left[x\right]$ ist $p\left(x\right) = 1 + x + x^3$ irreduzibel*

Beweis. $p\left(1\right) = p\left(0\right) = 1 \neq 0$, d.h. das Polynom hat keine Nullstellen. Hätte das Polynom einen echten Teiler: $p\left(x\right) = q\left(x\right) h\left(x\right)$, so müsste entweder $q\left(x\right)$ oder $h\left(x\right)$ Grad 1 haben. Jedes Polynom von Grad 1 hat jedoch (genau) eine Nullstelle. Diese Nullstelle müsste auch eine Nullstelle von $p\left(x\right)$ sein. Somit folgt, dass $p\left(x\right)$ keine Zerlegung hat. ■

6.4.3 Ideale, grösster gemeinsamer Teiler, Euklidscher Algorithmus

Vorbemerkung: Die Definitionen und Lemmas in diesem und dem folgenden Unterkapitel sind nur für den Polynomring angegeben. Sie können aber allgemeiner für nullteilerfreie Ringe mit Eins formuliert werden. Das einfachste Beispiel für einen solchen Ring ist $\mathbb{Z}$. Es ist für die Anschauung sehr hilfreich, die Aussagen immer an diesem Beispiel zu überprüfen.

Definition 6.14 *Eine nicht leere Teilmenge $J \subset K\left[x\right]$ heisst **Ideal**, falls die folgenden Bedingungen erfüllt sind:*

J1 $J \neq \{0\}$

J2 $(J, +)$ *ist eine Untergruppe von $K\left[x\right]$*

J3 *Sind $p(x) \in J$ und $q(x) \in K[x]$, so ist $p(x)\,q(x) \in J$.*

*Ist $A \subset K[x]$ eine nicht leere Teilmenge mit $0 \notin A$, so ist das von A **erzeugte Ideal** J_A definiert durch*

$$J_A := \left\{ \sum_{j=1}^{n} h_j(x)\, a_j(x) : n \in \mathbb{N},\ a_j(x) \in A,\ h_j(x) \in K[x] \right\}.$$

*Im Spezialfall $A = \{a(x)\}$, $a(x) \neq 0$, heisst J_A das von $a(x)$ erzeugte **Hauptideal**. Man schreibt dann $(a(x))$ für J_A.*

Man beachte, dass in J3 $q(x)$ beliebig ist. J3 besagt also nicht nur, dass J abgeschlossen gegenüber Produkten in J ist, sondern das jedes polynomiale Vielfache eines Elementes in J wieder in J ist.

Lemma 6.6 *Ist $A \subset K[x]$, $A \neq \emptyset$, $0 \notin A$, so ist J_A das kleinste Ideal, das A enthält, d.h. es gelten die folgenden beiden Eigenschaften:*
a) J_A ist ein Ideal mit $A \subset J_A$.
b) Ist I ein Ideal mit $A \subset I$ so gilt $J_A \subset I$.

Beweis. Der ganz einfache Beweis sei dem Leser als Übungsaufgabe überlassen. ■

Bemerkung 6.5 *a) Enthält ein Ideal J ein konstantes Polynom $\neq 0$, so ist $J = K[x]$. In der Tat: Ist das konstante Polynom $a \in J$, $a \neq 0$, so folgt für jedes Polynom $p(x)$:*

$$p(x) = a\,(p(x)/a) \in J$$

wegen J3.
b) $J = (a(x))$ mit $a(x) \neq 0$ gilt genau dann, wenn $a(x) \mid p(x)$ für jedes Polynom $p(x) \in J$ gilt.
c) $(a(x)) = (\widetilde{a}(x))$ gilt genau dann wenn $\alpha \in K \setminus \{0\}$ existiert mit $a(x) = \alpha\widetilde{a}(x)$. Dies folgt sofort aus Bemerkung 6.4 c). Zu jedem Hauptideal J existiert also ein eindeutiges normiertes Polynom $a(x)$ mit $J = (a(x))$.

Satz 6.15 *In $K[x]$ ist jedes Ideal ein Hauptideal. (Man sagt, $K[x]$ sei ein **Hauptidealring**.)*

Beweis. Wegen $J \neq \{0\}$ existiert $p(x) \in J$, $p(x) \neq 0$. Sei $a(x)$ ein beliebiges Polynom von minimalem Grad ≥ 0 in J. Wir zeigen, dass $J = (a(x))$ ist.
Sei $p(x) \in J$, $p(x) \neq 0$. Wir führen eine Division mit Rest durch:

$$p(x) = h(x)\,a(x) + r(x),$$

mit $\operatorname{grad}(r(x)) < \operatorname{grad}(a(x))$. Nun ist aber wegen J3 $h(x)\,a(x) \in J$ und dann wegen J2 $r(x) = p(x) - h(x)\,a(x) \in J$. Da $a(x)$ minimalen Grad aller Polynome

$\neq 0$ in J hatte, folgt $r(x) = 0$. Somit ist $p(x) = h(x)\, a(x)$. D.h., jedes Polynom in J, das von Null verschieden ist, ist als $h(x)\, a(x)$ darstellbar. ■

Ist $A \subset K[x]$, $0 \notin A$, so wissen wir aus dem obigen Satz, dass ein Polynom $a(x) \neq 0$ existiert mit $J_A = (a(x))$. Nach der Bemerkung 6.5 c) wissen wir, dass $a(x)$ eindeutig ist bis auf Multiplikation mit einem Körperelement $\neq 0$. Somit ist 6.5 $a(x)$ eindeutig, wenn es als normiert vorausgesetzt wird.

Wir betrachten nun eine nicht leere Teilmenge $A \subset K[x]$, $0 \notin A$ und das davon erzeugte Ideal. Nach dem vorangegangenen Satz wissen wir, dass $J_A = (a(x))$, wobei wir $a(x)$ als normiert voraussetzen.

Lemma 6.7 *$a(x)$ hat die folgenden Eigenschaften:*

a) $a(x) \mid p(x)$ für alle $p(x) \in A$

b) Ist $b(x) \in K[x]$, $b(x) \neq 0$ mit $b(x) \mid p(x)$ für alle $p(x) \in A$, so gilt $b(x) \mid a(x)$.

$a(x)$ ist eindeutig charakterisiert durch diese Eigenschaften und die Bedingung, dass es normiert ist.

Beweis. a) folgt aus $A \subset J_A = (a(x))$. Wir zeigen b): Wegen $a(x) \in J_A$ folgt, dass es Polynome $p_1(x), \ldots, p_n(x) \in A$ und $h_1(x), \ldots, h_n(x) \in K[x]$ gibt mit $a(x) = \sum_{i=1}^{n} h_i(x)\, p_i(x)$. Da $b(x) \mid p_i(x)$ gilt folgt sofort $b(x) \mid a(x)$.

Sind $a(x)$ und $\widetilde{a}(x)$ zwei normierte Polynome mit den Eigenschaften a) und b) so gilt $a(x) \mid \widetilde{a}(x)$ und $\widetilde{a}(x) \mid a(x)$. Daraus folgt $a(x) = \widetilde{a}(x)$. ■

Das Lemma legt die folgende Definition nahe:

Definition 6.15 *Sei $A \subset K[x]$, $A \neq \emptyset$, $0 \notin A$. Dann bezeichnet man das eindeutige normierte Polynom $a(x)$ mit $(a(x)) = J_A$ als den* ***grössten gemeinsamen Teiler*** *von A. Notation: $a(x) = \mathrm{ggT}(A)$. Sind $p_1(x), \ldots, p_n(x)$ endlich viele von 0 verschiedene Polynome, so schreiben wir $\mathrm{ggT}(p_1(x), \ldots, p_n(x))$ für den grössten gemeinsamen Teiler von $\{p_1(x), \ldots, p_n(x)\}$.*

Bemerkung 6.6 *Nach der obigen Diskussion ist $a(x) = \mathrm{ggT}(p_1(x), \ldots, p_n(x))$ eindeutig durch die folgenden Eigenschaften charakterisiert*

- *$a(x)$ ist normiert*
- *$a(x) \mid p_i(x)$ für $i = 1, \ldots, n$*
- *Es existieren Polynome $h_1(x), \ldots, h_n(x) \neq 0$ mit*

$$a(x) = \sum_{i=1}^{n} h_i(x)\, p_i(x).$$

Beweis. Der normierte ggT $a(x)$ ist eindeutig dadurch charakterisiert, dass er alle Polynome $p_i(x)$ teilt und gleichzeitig Element des Ideals $J_{\{p_1(x),\ldots,p_n(x)\}}$ ist. Letzteres ist aber nichts anderes als der dritte Punkt der obigen Liste. ■

Wir betrachten den Spezialfall, wo die $p_i(x)$ teilerfremd sind (siehe Definition 6.10). Dies bedeutet, dass es kein nicht konstantes Polynom gibt, das alle $p_i(x)$ teilt. Demzufolge ist $\mathrm{ggT}(p_1(x),\ldots,p_n(x)) = 1$. Nach dem dritten Punkt in der obigen Bemerkung existieren dann Polynome $h_1(x),\ldots,h_n(x) \neq 0$ mit $1 = \sum_{i=1}^{n} h_i(x)\,p_i(x)$. Damit gelangen wir zu dem folgenden Lemma:

Lemma 6.8 *n Polynome $p_1(x),\ldots,p_n(x) \neq 0$ sind genau dann teilerfremd, wenn es Polynome $h_1(x),\ldots,h_n(x) \in K[x]$ gibt mit*

$$1 = \sum_{i=1}^{n} h_i(x)\,p_i(x). \tag{6.9}$$

Beweis. Die Tatsache, dass die Eigenschaft der Teilerfremdheit die Existenz von Polynomen $h_i(x)$ impliziert, sodass die obige Gleichung erfüllt ist, haben wir schon eben diskutiert. Umgekehrt teilt natürlich 1 alle Polynome, sodass nach der vorangegangenen Bemerkung die Existenz der $h_i(x)$ mit (6.9) auch impliziert, dass 1 der grösste gemeinsame Teiler ist, d.h. dass $p_1(x),\ldots,p_n(x)$ teilerfremd sind. ■

Wir diskutieren nun kurz den **Euklidschen Algorithmus** zur Bestimmung des ggT von zwei Polynomen. Der Einfachheit halber beschränken wir uns auf zwei Polynome; der Algorithmus kann jedoch leicht verallgemeinert werden. Dieser Algorithmus ist ausserordentlich wichtig und spielt in der Kodierungstheorie eine ganz herausragende Rolle. Die schnellen Dekodierungsalgorithmen, die für die Codes benützt werden, die in den CDs verwendet werden, benützen Varianten des Euklidschen Algorithmus.

Hier der Algorithmus zur Berechnung von $\mathrm{ggT}(p(x),q(x))$. $p(x),q(x) \neq 0$. Wir können voraussetzen, dass $\mathrm{grad}(q(x)) \leq \mathrm{grad}(p(x))$ gilt. Wir definieren $l_1(x) := p(x)$ und $l_2(x) := q(x)$, und definieren $l_n(x)$ rekursiv mit einer Division mit Rest:

$$l_{n-1}(x) = h_n(x)\,l_n(x) + l_{n+1}(x),\ n \geq 2, \tag{6.10}$$

mit $\mathrm{grad}(l_{n+1}(x)) < \mathrm{grad}(l_n(x))$. Da der Grad bei jeder Iteration fällt, existiert

$$N := \min\{n : l_{n+1}(x) = 0\}.$$

Lemma 6.9 *Der $\mathrm{ggT}(p(x),q(x))$ ist das Polynom $l_N(x)$ nach Normierung.*

Beweis. Wir beweisen die Eigenschaften a)-c) der vorangegangenen Bemerkung 6.6. a) ist klar. Wegen $l_{N+1}(x) = 0$ folgt $l_N(x) \mid l_{N-1}(x)$. Wegen $l_{N-2}(x) = h_{N-1}(x)\,l_{N-1} + l_N(x)$ und $l_N(x) \mid l_{N-1}(x)$ folgt $l_N(x) \mid l_{N-2}(x)$. Fährt man in dieser Weise weiter, so folgt sehr einfach, dass $l_N(x)$ alle $l_i(x)$ teilt, $1 \leq i \leq N-1$. Damit ist b) der Bemerkung bewiesen.

Beweis von c). Wir beweisen mit Induktion nach n, dass $l_n(x)$ eine Darstellung

$$l_n(x) = a_n(x)\,p(x) + b_n(x)\,q(x) \tag{6.11}$$

hat, wobei $a_n(x), b_n(x) \in K[x]$ sind, wobei wir natürlich nur an $n \leq N$ interessiert sind. Für $n = 1, 2$ ist das trivial. Sei $2 \leq n < N$. Wir verwenden (6.10) und wenden die Induktionsvoraussetzung auf $l_n(x)$ und $l_{n-1}(x)$ an. Somit erhalten wir

$$\begin{aligned} l_{n+1}(x) &= l_{n-1}(x) - h_n(x)\,l_n(x) \\ &= a_{n-1}(x)\,p(x) + b_{n-1}(x)\,q(x) - h_n(x)\,(a_n(x)\,p(x) + b_n(x)\,q(x)) \\ &= [a_{n-1}(x) - h_n(x)\,a_n(x)]\,p(x) + [b_{n-1}(x) - h_n(x)\,b_n(x)]\,q(x). \end{aligned}$$

Mit $a_{n+1}(x) := a_{n-1}(x) - h_n(x)\,a_n(x)$ und $b_{n+1}(x) := b_{n-1}(x) - h_n(x)\,b_n(x)$ ist (6.11) für $n+1$ bewiesen.

Damit folgt, dass auch $l_N(x)$ eine derartige Darstellung hat.

Somit ist gezeigt, dass der Euklidsche Algorithmus tatsächlich zum grössten gemeinsamen Teiler führt. ■

Beispiel 6.10

$$\begin{aligned} p(x) &= x^4 + x^3 + x + 1 \\ q(x) &= x^3 + 2x^2 + 2x + 1. \end{aligned}$$

Dann ist

$$p(x) = (x-1)\,q(x) + 2x + 2,$$

$$q(x) = (2x+2)\,\frac{1}{2}\left(x^2 + x + 1\right) + 0.$$

Demzufolge ist

$$\mathrm{ggT}\,(p(x), q(x)) = x + 1.$$

6.4.4 Primfaktorzerlegung von Polynomen

Um uns nicht ständig zu wiederholen, legen wir für dieses Unterkapitel die Konvention fest, dass alle betrachteten Polynome $\neq 0$ und normiert sind, d.h. mit höchstem Koeffizienten 1.

Lemma 6.10 *Seien $h(x), p_1(x), \ldots, p_n(x)$ Polynome, und für jedes i seien die zwei Polynome $h(x)$ und $p_i(x)$ teilerfremd. Dann sind die beiden Polynome $h(x)$ und $p_1(x) \cdot \cdots \cdot p_n(x)$ teilerfremd.*

Beweis. Wir führen Induktion nach n. Für $n = 1$ ist nichts zu beweisen. Sei also $n \geq 2$. Nach Induktionsvoraussetzung sind $h(x)$ und $p_1(x) \cdot \cdots \cdot p_{n-1}(x)$ teilerfremd und nach Voraussetzung $h(x)$ und $p_n(x)$ und wir müssen nun zeigen,

dass $h(x)$ und $(p_1(x) \cdot \cdots \cdot p_{n-1}(x)) \cdot p_n(x)$ teilerfremd sind. Es genügt also, den Fall $n = 2$ zu betrachten.

Nach Lemma 6.8 existieren Polynome $r_1(x), r_2(x), l_1(x), l_2(x)$ mit

$$1 = r_1(x) h(x) + l_1(x) p_1(x) \tag{6.12}$$

$$1 = r_2(x) h(x) + l_2(x) p_2(x). \tag{6.13}$$

Aus (6.12) folgt (durch Multiplikation mit $l_2(x) p_2(x)$)

$$l_2(x) p_2(x) = r_1(x) l_2(x) p_2(x) h(x) + l_1(x) l_2(x) p_1(x) p_2(x).$$

Zusammen mit (6.13) ergibt sich daraus

$$1 = [r_2(x) + r_1(x) l_2(x) p_2(x)] h(x) + l_1(x) l_2(x) p_1(x) p_2(x).$$

Aus Lemma 6.8 folgt daraus, dass $h(x)$ und $p_1(x) p_2(x)$ teilerfremd sind. ■

Lemma 6.11 *Seien $p_1(x), \ldots, p_n(x)$ verschiedene irreduzible Polynome, ebenso $q_1(x), \ldots, q_N(x)$ verschiedene irreduzible Polynome und $m_1, \ldots, m_n \in \mathbb{N}$ sowie $M_1, \ldots, M_N \in \mathbb{N}$. Dann gilt*

$$p_1(x)^{m_1} \cdot \cdots \cdot p_n(x)^{m_n} \mid q_1(x)^{M_1} \cdot \cdots \cdot q_N(x)^{M_N} \tag{6.14}$$

dann und nur dann, wenn für jedes $i \in \{1, \ldots, n\}$ ein $j \in \{1, \ldots, N\}$ existiert mit $p_i(x) = q_j(x)$ und

$$m_i \leq M_j. \tag{6.15}$$

Beweis. Die eine Richtung ist trivial: Sind alle $p_i(x)$ in der Liste der Polynome $q_1(x), \ldots, q_N(x)$ enthalten und gilt (6.15), so gilt (6.14).

Wir beweisen die andere Richtung und nehmen an, dass (6.14) gilt. Da natürlich

$$p_i(x)^{m_i} \mid p_1(x)^{m_1} \cdot \cdots \cdot p_n(x)^{m_n}$$

gilt, genügt es, den Fall $n = 1$ zu betrachten. Wir nehmen also an, $p(x)$ sei irreduzibel und $p(x)^m$ teile $q_1(x)^{M_1} \cdot \cdots \cdot q_N(x)^{M_N}$. Dann gilt auch

$$p(x) \mid q_1(x)^{M_1} \cdot \cdots \cdot q_N(x)^{M_N}, \tag{6.16}$$

da $p(x)$ natürlich $p(x)^m$ teilt. Daraus folgt nun, dass $p(x)$ eines der $q_i(x)$ ist. Wäre dem nicht so, so wären $p(x)$ und $q_i(x)$ teilerfremd für $i = 1, \ldots, N$ und nach Lemma 6.10 wären dann auch $p(x)$ und $q_1(x)^{M_1} \cdot \cdots \cdot q_N(x)^{M_N}$ teilerfremd, was (6.16) widerspricht. Wir sehen also, dass $p(x)$ eines der $q_i(x)$ ist. Der Einfachheit halber nehmen wir $p(x) = q_1(x)$ an. Wir müssen nun noch nachweisen, dass $m \leq M_1$ gilt. Wir machen das wieder indirekt und nehmen an, dass $m > M_1$ gilt. Es existiert dann also ein Polynom $h(x)$ mit

$$h(x) p(x)^m = p(x)^{M_1} \cdot q_2(x)^{M_2} \cdot \cdots \cdot q_N(x)^{M_N},$$

$$p(x)^{M_1}\left[h(x)\,p(x)^{m-M_1}-q_2(x)^{M_2}\cdot\dots\cdot q_N(x)^{M_N}\right]=0.$$

Da $K[x]$ keine Nullteiler hat, folgt

$$h(x)\,p(x)^{m-M_1}-q_2(x)^{M_2}\cdot\dots\cdot q_N(x)^{M_N}=0,$$

d.h.

$$p(x)^{m-M_1}\mid q_2(x)^{M_2}\cdot\dots\cdot q_N(x)^{M_N}.$$

Nach demselben Argument wie oben erhalten wir, dass $p(x)$ eines der Polynome $q_2(x),\dots,q_N(x)$ ist, was der Voraussetzung widerspricht, dass die $q_i(x)$ alle verschieden sind und $p(x)$ schon $q_1(x)$ ist.

Damit ist das Lemma bewiesen. ■

Satz 6.16 *Sei $p(x)\in K[x]$, $\operatorname{grad}(p(x))\geq 1$. Dann hat $p(x)$ die bis auf die Reihenfolge der Faktoren eindeutige Zerlegung als Produkt von irreduziblen Polynomen:*

$$p(x)=q_1(x)^{M_1}\cdot\dots\cdot q_N(x)^{M_N}.$$

Die $q_i(x)$ sind irreduzibel und verschieden und die M_i sind $\in\mathbb{N}$.

Beweis. Die Eindeutigkeit folgt sofort aus dem vorangegangenen Lemma.

Wir beweisen die Existenz einer derartigen Zerlegung mit Induktion nach dem Grad von $p(x)$. Ist $\operatorname{grad}(p(x))=1$, so ist nichts zu zeigen, denn $p(x)$ ist schon irreduzibel. Sei also $\operatorname{grad}(p(x))\geq 2$. Die Induktionsannahme ist, dass eine Zerlegung für Polynome von Grad $\leq n-1$ gilt. Ist $p(x)$ irreduzibel, so ist ebenfalls nichts zu zeigen. Ist $p(x)$ nicht irreduzibel, so existieren Polynome $h(x),q(x)$ vom Grad $\leq n-1$ mit $p(x)=h(x)\,q(x)$. Wir wenden die Induktionsvoraussetzung auf $h(x)$ und $q(x)$ an und erhalten auf diese Weise eine Zerlegung von $p(x)$ als Produkt von irreduziblen Faktoren. ■

Die obige Zerlegung nennt man die **Primfaktorzerlegung** eines Polynoms. Die irreduziblen Polynome, die in der Zerlegung vorkommen, nennt man die **Primfaktoren** von $p(x)$. Die M_i nennt man aus naheliegenden Gründen die **Vielfachheiten** der Primfaktoren.

Kennt man die Primfaktorzerlegung von Polynomen $p_1(x),\dots,p_n(x)$, so lässt sich der grösste gemeinsame Teiler (ganz analog wie bei den ganzen Zahlen) wie folgt bestimmen: Für jedes irreduzible Polynom $q(x)$ sein $R_i(q(x))$ die Vielfachheit mit der $q(x)$ in der Primfaktorzerlegung von $p_i(x)$ vorkommt. Falls $q(x)$ in der Primfaktorzerlegung nicht vorkommt, so setzen wir $R_i(q(x)):=0$. Dann definieren wir

$$R(q(x)):=\min_{1\leq i\leq n}R_i(q(x)).$$

Dann gilt

Proposition 6.1

$$\mathrm{ggT}\left(p_1\left(x\right),\ldots,p_n\left(x\right)\right)=\prod_{q(x)\text{ irreduzibel}}q\left(x\right)^{R(q(x))}. \tag{6.17}$$

Dabei ist $q\left(x\right)^0:=1$.

Die Notation auf der rechten Seite braucht wohl eine kleine Erklärung: Man nimmt jedes irreduzibel Polynom mit der minimalen Anzahl seines Vorkommens in den Zerlegungen der $p_i\left(x\right)$. Natürlich kommen nur endlich viele irreduzible Polynome $q\left(x\right)$ überhaupt in irgendeiner der Primfaktorzerlegung der $p_i\left(x\right)$ vor. Obwohl also (formal) $\prod_{q(x)\text{ irreduzibel}}$ ein unendliches Produkt ist, sind alle Faktoren bis auf endlich viele einfach gleich Eins, und können daher weggelassen werden. Man kann sich darauf beschränken, dass nur die Polynome $q\left(x\right)$ überhaupt betrachtet werden, die in allen Primfaktorzerlegungen der $p_i\left(x\right)$ vorkommen, mit dem Verständnis, dass die rechte Seite von (6.17) gleich 1 ist, wenn es überhaupt kein irreduzibles Polynom gibt, die in allen Primfaktorzerlegungen vorkommt.

Der einfache Beweis der obigen Proposition sei dem Leser als Übungsaufgabe überlassen.

6.5 Polynomiale Funktionen von Endomorphismen

V sei ein endlichdimensionaler K-Vektorraum. Wie früher schon eingeführt, bezeichnen wir mit $\hom\left(V\right)$ die Menge der Endomorphismen $V\to V$. Wir hatten schon früher gesehen, dass $\hom\left(V\right)$ selbst ein K-Vektorraum ist: Sind $f,g\in\hom\left(V\right)$, so definieren wir $f+g\in\hom\left(V\right)$ durch $\left(f+g\right)\left(v\right):=f\left(v\right)+g\left(v\right)$, und für $\alpha\in K$, $f\in\hom\left(V\right)$ definieren wir $\left(\alpha f\right)\left(v\right):=\alpha f\left(v\right)$.

Lemma 6.12 *Ist* $n=\dim\left(V\right)$, *so ist* $\dim\left(\hom\left(V\right)\right)=n^2$.

Beweis. Sei $\mathcal{V}=\left(v_1,\ldots,v_n\right)$ eine Basis von V. Wir definieren für $1\leq i,j\leq n$ die Endomorphismen f_{ij} durch die Festsetzung $f_{ij}\left(v_k\right):=\delta_{ik}v_j$, $k=1,\ldots,n$. Dann bildet die Familie der f_{ij} eine Basis von $\hom\left(V\right)$ (Übungsaufgabe). ■

$\hom\left(V\right)$ hat nicht nur die Struktur eines K-Vektorraum, sondern besitzt auch ein Produkt, nämlich die Komposition: sind $f,g\in\hom\left(V\right)$, so ist $f\circ g$ die Komposition, die natürlich wieder in $\hom\left(V\right)$ liegt.

Die Operation der Komposition ist assoziativ, wie wir schon wissen, und bilinear: Für $f,g,h\in\hom\left(V\right)$ und $\alpha,\beta\in K$ gelten

$$\left(\alpha f+\beta g\right)\circ h=\alpha\left(f\circ h\right)+\beta\left(g\circ h\right)$$

$$h\circ\left(\alpha f+\beta g\right)=\alpha\left(h\circ f\right)+\beta\left(h\circ g\right),$$

wie man sofort nachprüft. $\hom\left(V\right)$ hat also die Struktur einer assoziativen K-Algebra (siehe Bemerkung 4.1). Durch die Einführung einer Basis können wir

diese mit der Menge der quadratischen Matrizen $M(n,K)$ in Beziehung setzen. Ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V, so können wir jedem Endomorphismus $f \in \hom(V)$ die darstellende Matrix bezüglich dieser Basis zuordnen und diese Zuordnung ist bijektiv. Dabei übertragen sich die Vektorraumoperationen und Komposition von Endomorphismen entspricht der Multiplikation von Matrizen. Dies hatten wir schon früher diskutiert.

Sei nun $p(x) \in K[x]$ ein Polynom, $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ und sei $f \in \hom(V)$. Wir können dann

$$p(f) := a_0 \operatorname{id}_V + a_1 f + a_2 f^2 + \ldots + a_n f^n$$

definieren. Dabei ist f^k die k-fache Komposition der Abbildung f. Wir schreiben auch $f^0 := \operatorname{id}_V$. $p(f)$ ist dann selbst wieder ein Endomorphismus.

Lemma 6.13 *a) Ist* $h(x) = \alpha p(x) + \beta q(x)$, $\alpha, \beta \in K$, $p(x), h(x), q(x) \in K[x]$, *und ist* $f \in \hom(V)$, *so gilt*

$$h(f) = \alpha p(f) + \beta q(f).$$

b) Ist $h(x) = p(x)\, q(x)$ *und ist* $f \in \hom(V)$, *so gilt*

$$h(f) = p(f) \circ q(f).$$

Beweis. Einfaches Nachrechnen. ■

Bemerkung 6.7 *a) Aus dem obigen Lemma folgt für* $p(x), q(x) \in K[x]$ *und* $f \in \hom(V)$:

$$p(f) \circ q(f) = q(f) \circ p(f),$$

obwohl natürlich im allgemeinen die Komposition von Endomorphismen nicht kommutativ ist.

b)

$$1(f) = \operatorname{id}_V$$
$$0(f) = 0.$$

Dies bedarf vielleicht einer Erläuterung: Die 1 *auf der linken Seite der ersten Gleichung ist das konstante Polynom* 1. *Die* 0 *auf der linken Seite der zweiten Gleichung ist das Nullpolynom. Die* 0 *auf der rechten Seite ist die Nullabbildung* $V \to V$.

c) Im allgemeinen gilt für $p(x) \in K[x]$, $f, g \in \hom(V)$:

$$p(f+g) \neq p(f) + p(g),$$

$$p(f \circ g) \neq p(f) \circ p(g).$$

Man kann ganz einfache Beispiele angeben. So gilt für $p(x) = x^2$

$$\begin{aligned} p(f+g) &= f^2 + f \circ g + g \circ f + g^2 \\ p(f) + p(g) &= f^2 + g^2. \end{aligned}$$

Die beiden Endomorphismen stimmen nur überein, wenn $f \circ g + g \circ f = 0$, *was natürlich im allgemeinen nicht der Fall ist, z.B. für* $f = g = \mathrm{id}_V$. *Für* $p(f \circ g) \neq p(f) \circ p(g)$ *lassen sich analoge Beispiele angeben.*

d) Sei $p(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$, $f \in \hom(V)$ *und* $\mathcal{V} = (v_1, \ldots, v_n)$ *eine Basis von V. Ist A die darstellende Matrix von f bezüglich* $\mathcal{V}$, *so ist*

$$p(A) := a_0 E_n + a_1 A + a_2 A^2 + \ldots + a_n A^n$$

die darstellende Matrix von $p(f)$ *bezüglich* $\mathcal{V}$.

Sei nun ein fester Endomorphismus $f \in \hom(V)$ gegeben. Wir fragen uns, ob es ein Polynom $p(x) \in K[x]$, $p(x) \neq 0$, gibt mit $p(f) = 0$ (das ist der 0-Endomorphismus). Wir sagen dann, dass Polynom $p(x)$ den Endomorphismus **annulliert.** Diese Frage ist sehr leicht mit "Ja" zu beantworten: Wir betrachten die Endomorphismen $\mathrm{id}_V, f, f^2, \ldots, f^{n^2}$. Dies sind n^2+1 Elemente in $\hom(V)$. Da $\dim(\hom(V)) = n^2$ ist, sind diese Endomorphismen linear abhängig. Demzufolge existieren Skalare $a_0, a_1, \ldots, a_{n^2} \in K$, nicht alle $= 0$, mit

$$a_0 \mathrm{id}_V + a_1 f + a_2 f^2 + \ldots + a_{n^2} f^{n^2} = 0.$$

Die linke Seite ist aber $p(f)$ mit $p(x) = a_0 + a_1 x + \ldots + a_{n^2} x^{n^2}$.

Wir betrachten die Menge

$$J_f := \{p(x) \in K[x] : p(f) = 0\}.$$

Wie wir oben gesehen haben, existiert ein Polynom in J_f, das nicht das Nullpolynom ist. Wie man sofort nachprüft, ist J_f ein Ideal. Nach Satz 6.15 existiert ein eindeutiges normiertes Polynom $m_f(x) \in K[x]$ mit $J_f = (m_f(x))$.

Definition 6.16 $m_f(x)$ *heisst das* ***Minimalpolynom*** *von* f.

$m_f(x)$ ist auch einfach das eindeutig bestimmte normierte Polynom minimalen Grades ≥ 0, das den Endomorphismus annulliert. Zunächst zwei triviale Bemerkungen: Ist $V \neq \{0\}$, so gibt es natürlich kein konstantes Polynom, das f annulliert, denn $1(f) = \mathrm{id}_V$, selbst wenn f die Nullabbildung ist. Demzufolge ist ausser im Trivialfall $V = \{0\}$ $\mathrm{grad}(m_f(x)) \geq 1$. Ist f die Nullabbildung so ist das Minimalpolynom offensichtlich $m_f(x) = x$. Dar Fall, wo $\mathrm{grad}(m_f(x)) = 1$ ist, ist ebenfalls sehr einfach: Ist $m_f(x) = \alpha + x$, so ist $m_f(f) = f + \alpha \mathrm{id}_V$, d.h. $f = -\alpha \mathrm{id}_V$, d.h. f ist ein Vielfaches der Identität. In allen anderen Fällen hat das Minimalpolynom Grad mindestens 2. Wie wir schon gesehen haben, gilt $\mathrm{grad}(m_f) \leq \dim(V)^2$. Wir werden jedoch sehen, dass das Minimalpolynom höchstens Grad $\dim(V)$ hat.

Satz 6.17 $\operatorname{spec}(f)$ *ist die Nullstellenmenge des Minimalpolynoms.*

Beweis. I) Sei α eine Nullstelle von $m_f(x)$. Dann gilt $m_f(x) = (x-\alpha)\,p(x)$, wobei $\operatorname{grad}(p(x)) < \operatorname{grad}(m_f(x))$ ist. Somit gilt $p(x) \notin J_f$. Demzufolge existiert $v \in V$ mit $\widetilde{v} := p(f)(v) \neq 0$. Andererseits ist jedoch $m_f(f)(v) = 0$. Daraus folgt

$$0 = m_f(f)(v) = (f-\alpha)(p(f)(v)) = (f-\alpha)(\widetilde{v}) = f(\widetilde{v}) - \alpha\widetilde{v}.$$

Demzufolge ist $\alpha \in \operatorname{spec}(f)$ mit Eigenvektor $\widetilde{v}$.

II) Sei umgekehrt $\alpha \in \operatorname{spec}(f)$. Dann existiert ein Vektor $v \neq 0$ mit $f(v) = \alpha v$. Wir betrachten

$$I := \{p(x) \in K[x] : p(f)(v) = 0\}.$$

I ist offensichtlich ein Ideal. Ferner gilt $1 \notin I$, da $v \neq 0$ ist. Andererseits ist $x - \alpha \in I$, denn $(f - \alpha\,\mathrm{id}_V)(v) = 0$ nach der Voraussetzung, dass v ein Eigenvektor ist. Daraus folgt, dass I das von $x-\alpha$ erzeugte Ideal ist. Andererseits gilt jedoch $J_f \subset I$, denn wenn $p(f)$ die Nullabbildung ist, so ist natürlich auch $p(f)(v) = 0$. Daraus folgt, dass $x-\alpha$ jedes Polynom in J_f teilt und insbesondere auch das Minimalpolynom selbst. Nach Satz 6.10 folgt, dass α eine Nullstelle des Minimalpolynoms ist. ■

Satz 6.18 *Ein Endomorphismus f ist genau dann diagonalisierbar, wenn das Minimalpolynom in einfache Linearfaktoren zerfällt, d.h. wenn*

$$m_f(x) = \prod_{\alpha \in \operatorname{spec}(f)} (x-\alpha)$$

gilt.

Beweis. Sei $\operatorname{spec}(f) = \{\alpha_1, \ldots, \alpha_k\}$.

I) Sei f diagonalisierbar. Dann gilt $V = \bigoplus_{j=1}^{k} E(\alpha_j)$. $f - \alpha_j\,\mathrm{id}_V$ annulliert jeden Vektor aus $E(\alpha_j)$, d.h. es gilt $(f - \alpha_j\,\mathrm{id}_V)(v) = 0$ für jeden Vektor aus $E(\alpha_j)$. Betrachten wir den Endomorphismus $g := \prod_{j=1}^{k}(f - \alpha_j\,\mathrm{id}_V)$. (Das Produkt ist hier als Komposition zu verstehen). Da die Reihenfolge der Faktoren keine Rolle spielt, folgt auch $g(v) = 0$ für alle $v \in E(\alpha_j)$. Dies gilt für ein beliebiges j. Somit folgt $g(v) = 0$ für alle $v \in V$. Demzufolge ist g die Nullabbildung. Nun ist aber $g = p(f)$, wobei $p(x)$ das Polynom $p(x) := \prod_{j=1}^{k}(x-\alpha_j)$ ist. Aus $p(f) = 0$ folgt aber, dass $p(x)$ das Minimalpolynom teilt. Da jedoch nach dem vorangegangenen Satz, jedes der α_j eine Nullstelle des Minimalpolynoms ist, folgt dass $p(x) = m_f(x)$ ist.

II) Wir setzen voraus, dass $m_f(x) = \prod_{j=1}^{k}(x-\alpha_j)$ gilt. Wir betrachten die Polynome

$$p_i(x) := \prod_{j=1,\, j\neq i}^{k} (x-\alpha_j).$$

Diese Polynome sind nach der Proposition 6.1 teilerfremd. Demzufolge existieren Polynome $h_1(x), \ldots, h_k(x)$ mit

$$1 = \sum_{i=1}^{k} p_i(x) h_i(x).$$

Einsetzen von f ergibt:

$$\mathrm{id}_V = \sum_{i=1}^{k} p_i(f) \circ h_i(f).$$

Damit folgt, dass für jedes Element $v \in V$ die Gleichung

$$v = \sum_{i=1}^{k} \underbrace{(p_i(f) \circ h_i(f))(v)}_{=:v_i}.$$

Nun gilt aber

$$(f - \alpha_i \mathrm{id}_V) \circ p_i(f) \circ h_i(f) = m_f(f) \circ h_i(f) = 0,$$

und demzufolge $(f - \alpha_i \mathrm{id}_V)(v_i) = 0$. Dies impliziert $v_i \in E(\alpha_i)$. Wir haben somit gezeigt, dass sich jeder Vektor als Summe von Vektoren aus den Eigenräumen schreiben lässt. Mit anderen Worten:

$$V = \sum_{i=1}^{k} E(\alpha_i).$$

Die Summe der Eigenräume ist jedoch auf jeden Fall eine direkte, sodass

$$V = \bigoplus_{j=1}^{k} E(\alpha_j)$$

folgt, was gleichbedeutend mit der Diagonalisierbarkeit ist. ■

Satz 6.19 (Cayley-Hamilton) *Das charakteristische Polynom von f annulliert f, d.h. es gilt*

$$\chi_f(f) = 0.$$

Beweis. Wir beweisen den Satz nur für algebraisch abgeschlossenen Körper.

Wir zeigen den Satz mit Induktion nach $n := \dim(V)$. Der Fall $n = 1$ ist einfach: Hier ist $f = \lambda \mathrm{id}_V$, wobei λ der einzige Eigenwert ist. Damit ist $\chi_f(x) = \lambda - x$ und $\chi_f(f) = \lambda \mathrm{id}_V - f = 0$.

Sei nun $n \geq 2$. Wir beweisen die Aussage des Satzes unter der Induktionsvoraussetzung, dass sie für Vektorräume der Dimension $\leq n-1$ gilt. Da K als algebraisch abgeschlossen vorausgesetzt wird, existiert ein Eigenwert λ. Sei v_1 ein

zugehöriger Eigenvektor. Wir ergänzen v_1 zu einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$. Wir setzen

$$V_1 := L[v_1],\ V_2 := L[v_2, \ldots, v_n].$$

Dann gilt $V = V_1 \oplus V_2$.

V_1 ist nach Voraussetzung invariant unter f, V_2 aber i.a. nicht. Ist $v \in V_2$, so können wir jedoch $f(v)$ eindeutig als $u_1 + u_2$ zerlegen, mit $u_1 \in V_1, u_2 \in V_2$. Wir definieren f ür $v \in V_2$:

$$\widetilde{f}(v) := u_2.$$

$\widetilde{f}$ ist dann ein Endomorphismus $V_2 \to V_2$. Wir betrachten die darstellende Matrix von f bezüglich $\mathcal{V}$. Diese hat die Form

$$\begin{pmatrix} \lambda & * & \ldots & * \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix},$$

wobei A eine $(n-1) \times (n-1)$-Matrix ist, offenbar die darstellende Matrix von $\widetilde{f}$ bezüglich $(v_2, \ldots, v_n)$. Demzufolge ist

$$\chi_f(x) = (\lambda - x) \det(A - xE_{n-1}) = (\lambda - x)\chi_{\widetilde{f}}(x).$$

Nun benötigen wir eine kleine *Zwischenüberlegung.*
Sei $p(x)$ ein beliebiges Polynom. Dann ist f ür jedes $v \in V_2$

$$p(f)(v) - p\left(\widetilde{f}\right)(v) \in V_1. \tag{6.18}$$

Wir führen den Beweis von (6.18) mit Induktion nach $m := \operatorname{grad}(p(x))$. Für konstante Polynome ist die Aussage trivial (wieso?). Sei also $m \geq 1$. Dann ist

$$p(x) = xq(x) + a,$$

$a \in K$, $\operatorname{grad}(q(x)) = m - 1$. Für $v \in V_2$ gilt dann mit $f\left(q\left(\widetilde{f}\right)(v)\right) = \widetilde{f}\left(q\left(\widetilde{f}\right)(v)\right) + w_1$, $w_1 \in V_1$

$$\begin{aligned} p(f)(v) - p\left(\widetilde{f}\right)(v) &= f(q(f)(v)) + av - \widetilde{f}\left(q\left(\widetilde{f}\right)(v)\right) - av \\ &= f(q(f)(v)) - f\left(q\left(\widetilde{f}\right)(v)\right) + w_1 \\ &= f\left(q(f)(v) - q\left(\widetilde{f}\right)(v)\right) + w_1 \in V_1, \end{aligned}$$

da $q(f)(v) - q\left(\widetilde{f}\right)(v)$ nach Induktionsvoraussetzung $\in V_1$ ist und V_1 invariant unter f ist. Damit ist (6.18) bewiesen.

Wir zeigen nun $\chi_f(f) = 0$, wobei wir die Induktionsvoraussetzung benützen, dass diese Aussage für Vektorrä ume der Dimension $n-1$ schon bewiesen ist. Wir müssen also zeigen, dass für jeden Vektor $v \in V$ die Gleichung $\chi_f(f)(v) = 0$ gilt. Wegen der Linearität von $\chi_f(f)$ genügt es, diese Aussage für $v \in V_1$ und für $v \in V_2$ zu beweisen.

Ist $v \in V_1$, so gilt

$$\chi_f(f)(v) = \chi_{\tilde{f}}(f) \circ (\lambda \operatorname{id}_V - f)(v) = 0.$$

Ist $v \in V_2$, so ist nach (6.18), angewendet auf $p(x) = \chi_{\tilde{f}}(x)$:

$$\begin{aligned} \chi_f(f)(v) &= (\lambda \operatorname{id}_V - f)\left(\chi_{\tilde{f}}(f)(v)\right) \\ &= (\lambda \operatorname{id}_V - f)\left(\chi_{\tilde{f}}\left(\widetilde{f}\right)(v) + w_1\right), \end{aligned}$$

mit $w_1 \in V_1$. Nach Induktionsvoraussetzung ist aber $\chi_{\tilde{f}}\left(\widetilde{f}\right) = 0$. Demzufolge ist

$$\chi_f(f)(v) = (\lambda \operatorname{id}_V - f)(w_1) = 0,$$

da jeder Vektor in V_1 einfach um λ gestreckt wird.

Damit ist der Satz für algebraisch abgeschlossene Körper bewiesen. ■

Bemerkung 6.8 *Der Satz kann wie folgt auch für nicht algebraisch abgeschlossene Kö rper bewiesen werden. Betrachten wir den Fall $K = \mathbb{R}$. Am besten formulieren wir den Satz für Matrizen. Er besagt dann offenbar, dass f ür jede reelle quadratische Matrix A die Gleichung $\chi_A(A) = 0$ (Nullmatrix) gilt. Nun ist aber jede reelle Matrix auch eine komplexe Matrix, und das im Komplexen berechnete charakteristische Polynom hat natürlich genau dieselben Koeffizienten, wie wenn sie im Reellen berechnet werden. Wir haben somit den Satz von Cayley-Hamilton auch für $K = \mathbb{R}$ bewiesen. Dieses Argument funktioniert offenbar stets, wenn wir zum Körper K eine Körpererweiterung L finden können, wobei L algebraisch abgeschlossen ist. Es gibt einen Satz in der Algebra, der besagt, dass dies immer möglich ist. Wir können ihn jedoch hier nicht beweisen. Aus diesem Satz folgt dann Cayley-Hamilton für beliebige Körper.*

Es gibt allerdings auch (nicht zu schwierige) direkte Beweise des Satzes von Cayley-Hamilton für nicht algebraisch abgeschlossene Körper.

7 Die Jordansche Normalform: Struktur der Endomorphismen

7.1 Nilpotente Endomorphismen

Während des ganzen Kapitels ist $f : V \to V$ ein Endomorphismus und V ein endlichdimensionaler K-Vektorraum, $V \neq \{0\}$.

Definition 7.1 *f heisst **nilpotent**, wenn eine natürliche Zahl $k \geq 1$ existiert mit $f^k = 0$. (f^k ist die k-fach Iterierte der Abbildung f).*

Lemma 7.1 *a) Ist f nilpotent, so gilt* $\operatorname{spec}(f) = \{0\}$.

b) Sei f nilpotent und k die kleinste natürliche Zahl mit $f^k = 0$. Dann ist das Minimalpolynom von f das Polynom x^k.

Beweis. a) Sei $\lambda \in \operatorname{spec}(f)$. Dann existiert ein Vektor $v \neq 0$ mit $f(v) = \lambda v$. Falls $f^k = 0$ ist, so ergibt k-faches Iterieren die Gleichung $0 = f^k(v) = \lambda^k v$. Wegen $v \neq 0$ folgt $\lambda^k = 0$ und damit $\lambda = 0$. Andererseits lässt sich leicht zeigen, dass 0 tatsächlich ein Eigenwert ist: Sei $v \in V$, $v \neq 0$, und $j \in \mathbb{N}$ sei die kleinste Zahl mit $f^j(v) = 0$. Dann gilt $f(f^{j-1}(v)) = 0$ und $f^{j-1}(v) \neq 0$. Damit ist gezeigt, dass 0 ein Eigenwert ist. Somit folgt $\operatorname{spec}(f) = \{0\}$.

b) ist ein einfache Übungsaufgabe. ■

Wir wollen nun nachweisen, dass jeder nilpotente Endomorphismus eine Basis besitzt, bezüglich der die darstellende Matrix eine ganz spezielle Gestalt hat.

Definition 7.2 *Sei $\lambda \in K$. Die $n \times n$-Matrix*

$$J_n^\lambda := \begin{pmatrix} \lambda & 0 & 0 & \cdots & \cdots & 0 \\ 1 & \lambda & 0 & 0 & \cdots & 0 \\ 0 & 1 & \lambda & 0 & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}$$

*heisst **Jordanblock**. Ein Jordanblock hat also in der Diagonalen λ, in der ersten unteren Nebendiagonalen Einsen und sonst überall Nullen.*

Für uns sind im Moment nur die Jordanblöcke J_n^0 wichtig. J_1^0 ist einfach die 1×1-Matrix 0. Hat ein Endomorphismus f bezüglich einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$ die darstellende Matrix J_n^0, so werden die Basisvektoren unter f nach folgendem Schema abgebildet:

$$v_1 \to v_2 \to \ldots \to v_{n-1} \to v_n \to 0.$$

Demzufolge gilt $f^n = 0$, denn alle Basisvektoren werden unter Iterierten von f nach spätestens n Iterationen nach 0 abgebildet. f ist also nilpotent. Man beachte, dass $f^{n-1} \neq 0$ ist, denn $f^{n-1}(v_1) = v_n \neq 0$.

Ersetzen wir $\mathcal{V}$ durch die umgestellte Basis $(v_n, \ldots, v_1)$, so hat die darstellende Matrix bezüglich dieser Basis einfach die Einsen in der oberen Nebendiagonalen. In vielen Büchern wird das als Jordanblock verwendet.

Wir zeigen nun, dass für jede nilpotente Abbildung eine Basis existiert, bezüglich der sich die darstellende Matrix in einfacher Weise aus Jordanblöcken zusammensetzt.

Satz 7.1 *Sei f ein nilpotenter Endomophismus, und $k \in \mathbb{N}$, $k \geq 1$, sei die kleinste Zahl mit $f^k = 0$. Dann exisistiert eine Basis von V bezüglich der die darstellende Matrix die folgende Gestalt hat:*

$$\begin{pmatrix} J^0_{d_1} & 0 & \cdots & 0 \\ 0 & J^0_{d_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J^0_{d_m} \end{pmatrix}. \tag{7.1}$$

Dabei gilt $\sum_{i=1}^m d_i = n := \dim(V)$, $k = \max_i d_i$ und m, die Anzahl der Jordanblöcke, ist die geometrische Vielfachheit des Eigenwertes 0.

*Die obige **Jordanmatrix** ist eindeutig durch f gegeben, bis auf die Reihenfolge der Jordanblöcke.*

Ein Basis bezüglich der die darstellende Matrix die obige Gestalt hat, nennt man eine **Jordanbasis**. Es muss jedoch betont werden, dass eine Jordanbasis in keiner Weise eindeutig ist.

Durch eine Umordnung der Basis kann man die Reihenfolge der Jordanblöcke in der Jordanmatrix ändern. Wir können deshalb ohne Einschränkung der Allgemeinheit annehmen, dass $d_1 \geq d_2 \geq \ldots \geq d_m$ gilt.

Ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Jordanbasis, bezüglich der die darstellende Matrix die obige Form hat (mit $d_1 \geq d_2 \geq \ldots \geq d_m$), so werden die Basisvektoren unter f nach folgendem Schema abgebildet:

$$\begin{array}{ccccc} v_1 & & & & \\ \downarrow & & & & \\ v_2 & v_{d_1+1} & & & \\ \downarrow & \downarrow & & & \\ \vdots & \vdots & \vdots & & \text{etc.} \\ & & \vdots & & \\ v_{d_1-1} & v_{d_1+d_2-1} & \downarrow & & \\ \downarrow & \downarrow & & & \\ v_{d_1} & v_{d_1+d_2} & v_{d_1+d_2+d_3} & & \\ \downarrow & \downarrow & \downarrow & & \\ 0 & 0 & 0 & & \end{array} \tag{7.2}$$

Falls ein derartiges Abbildungsverhalten einer Basis vorliegt, so gilt offensichtlich $f^{d_1} = 0$ aber $f^{d_1-1} \neq 0$. f^{d_1} schickt nämlich alle Vektoren der Basis auf den Nullvektor, während unter f^{d_1-1} der Vektor v_1 auf $v_{d_1} \neq 0$ abgebildet wird. Ferner gilt $\ker(f) = L[v_{d_1} v_{d_1+d_2}, \ldots]$, d.h. $\ker(f)$ wird von der „untersten Schicht" des obigen Schemas aufgespannt. $\dim(\ker(f))$, die geometrische Vielfachheit des (einzigen) Eigenwertes 0, ist also die Anzahl der Jordanblöcke.

Wir werden im Beweis vom Satz 7.1 mehrfach das folgende Lemma verwenden:

Lemma 7.2 *Seien U ein Unterraum des Vektorraumes V, $m = \dim U$ und $n = \dim V$. Sind $v_1, \ldots, v_k$, $k \leq n - m$, linear unabhängige Vektoren mit*

$$U \cap L[v_1, \ldots, v_k] = \{0\}, \tag{7.3}$$

so existieren Vektoren $v_{k+1}, \ldots, v_{n-m} \notin U$, sodass $v_1, \ldots, v_{n-m}$ linear unabhängig sind und

$$U \cap L[v_1, \ldots, v_{n-m}] = \{0\} \tag{7.4}$$

gilt.

Beweis. Sei $u_1, \ldots, u_m$ eine Basis von U. Wegen (7.3), Satz 6.1 und Korollar 6.1 sind $u_1, \ldots, u_m, v_1, \ldots, v_k$ linear unabhängig. Diese Vektoren lassen sich daher mit Vektoren $v_{k+1}, \ldots, v_{n-m}$ zu einer Basis von V ergänzen. Dann folgt sofort (7.4). ■

Bemerkung 7.1 *a) Das Lemma gilt auch mit $k = 0$. Es besagt dann einfach, dass es linear unabhängige Vektoren $v_1, \ldots, v_{n-m}$ mit (7.4) gibt.*

b) Wegen 6.1 ist (7.4) äquivalent zu

$$V = U \oplus L[v_1, \ldots, v_{n-m}].$$

Bevor wir den Satz 7.1 in voller Allgemeinheit beweisen, betrachten wir zwei Spezialfälle.

Zunächst der triviale Spezialfall $k = 1$. Dann ist $f = 0$ und die darstellende Matrix ist bezüglich jeder Basis die Nullmatrix, was offenbar in diesem Fall die richtige Jordanmatrix ist. (Man sieht übrigens hier, dass eine Jordanbasis in keinster Weise eindeutig ist).

Wesentlich interessanter ist der Fall $k = 2$, den wir nun diskutieren. Der Satz besagt, dass sich eine Basis finden lässt, bezüglich der sich die darstellende Matrix aus Jordanblöcken $J_2^0 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ und $J_1^0 = (0)$ zusammensetzt. Wir können annehmen, dass die Zweierblöcke zuerst kommen, dass also die Jordanmatrix wie

folgt aussieht:

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}} & & & & & 0 \\ & 0 & & & & \\ & & \ddots & & & \\ & & & \boxed{\begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}} & & \\ & \vdots & & 0 & & \\ & & & & 0 & \\ & & & & & \ddots \\ & 0 & & & & 0 \end{pmatrix}. \tag{7.5}$$

Gibt es l Zweierblöcke und ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine entsprechende Jordanbasis, so bildet f diese Basiselemete nach folgendem Schema ab:

$$v_1 \to v_2 \to 0, v_3 \to v_4 \to 0, \ldots, v_{2l-1} \to v_{2l} \to 0,\ v_{2l+1} \to 0, \ldots, v_n \to 0. \tag{7.6}$$

Wenn wir umgekehrt eine Basis finden, die unter f nach Schema (7.6) abgebildet wird, so haben wir die gewünschte Jordanbasis gefunden.

Beweis der *Eindeutigkeit* (im Fall $k = 2$): Falls wir eine Basis mit dem Abbildungsverhalten (7.6) gefunden haben, so bilden $v_2, v_4, \ldots, v_{2l}, v_{2l+1}, \ldots, v_n$ eine Basis des Kerns von f. In der Tat ist eine Linearkombination $\sum_{i=1}^{n} \alpha_i v_i$ genau dann im Kern, wenn

$$f\left(\sum_{i=1}^{n} \alpha_i v_i\right) = \sum_{i=1}^{n} \alpha_i f(v_i) = \alpha_1 v_2 + \alpha_3 v_4 + \ldots + \alpha_{2l-1} v_{2l} = 0$$

gilt, d.h. wenn $\alpha_1 = \alpha_3 = \ldots = \alpha_{2l-1} = 0$ sind. Somit wird l im Schema (7.6) durch die Abbildung f festgelegt. Da l und die Dimension n von V das Schema (bis auf die Reihenfolge) eindeutig festlegen, ist damit die Eindeutigkeit gezeigt.

Beweis der *Existenz* (im Fall $k = 2$). Es ist naheliegend, zunächst mit einer Basis des Kerns von f zu beginnen und zu versuchen, diese dann in geeigneter Weise zu einer Basis von V zu ergänzen. Es stellt sich jedoch heraus, dass das nicht die richtige Idee ist, und dass man stattdessen „von oben" beginnen muss.

Seien $U := \ker(f)$, $n := \dim(V)$ und $m := \dim(U)$. Wegen unserer Annahme $k = 2$ gilt $f \neq 0$, $f^2 = 0$ und somit

$$\{0\} \subsetneqq U \subsetneqq V.$$

Nach Lemma 7.2 existieren linear unabhängige Vektoren $u_{m+1}, \ldots, u_n \in V$ mit

$$V = U \oplus L[u_{m+1}, \ldots, u_n]. \tag{7.7}$$

Lemma 7.3 *a)* $f(u_{m+1}), \ldots, f(u_n) \in \ker(f)$

b) $f(u_{m+1}), \ldots, f(u_n)$ *sind linear unabhängig in* V.

Beweis. a) folgt sofort aus $f^2 = 0$.
b): Sei

$$\sum_{j=m+1}^{n} \alpha_j f(u_j) = 0,\ \alpha_{m+1}, \ldots, \alpha_n \in K.$$

Wegen der Linearität von f folgt $f\left(\sum_{j=m+1}^{n} \alpha_j u_j\right) = 0$, d.h. $\sum_{j=m+1}^{n} \alpha_j u_j \in \ker(f) = U$. Andererseits gilt $\sum_{j=m+1}^{n} \alpha_j u_j \in L[u_{m+1}, \ldots, u_n]$. Wegen (7.7) folgt $\sum_{j=m+1}^{n} \alpha_j u_j = 0$ und somit $\alpha_{m+1} = \ldots = \alpha_n = 0$ wegen der Unabhängigkeit der u_j. ■

Eine erste Schlussfolgerung des Lemmas ist

$$m = \dim(U) \geq \dim(L[u_{m+1}, \ldots, u_n]) = n - m =: l.$$

Wir können nun die l Vektoren $f(u_{m+1}), \ldots, f(u_n)$ mit Vektoren $u'_{l+1}, \ldots, u'_m$ zu einer Basis $(f(u_{m+1}), \ldots, f(u_n), u'_{l+1}, \ldots, u'_m)$ in U ergänzen. Da $u_{m+1}, \ldots, u_n$ eine Basis in $L[u_{m+1}, \ldots, u_n]$ bilden und (7.7) gilt, folgt nach Korollar 6.1, dass $(u_{m+1}, \ldots, u_n, f(u_{m+1}), \ldots, f(u_n), u'_{l+1}, \ldots, u'_m)$ eine Basis in V ist. Wir brauchen diese nun nur noch umzunumerieren, dann haben wir die gewünschte Jordanbasis: $v_1 := u_{m+1}, v_2 := f(u_{m+1}), v_3 := u_{m+2}, v_4 := f(u_{m+2}), \ldots, v_{2l} := f(u_n), v_{2l+1} := u'_{l+1}, \ldots, v_n := u'_m$. Das Abbildungsverhalten von f ist dann genau durch das Schema (7.6) gegeben, d.h. die darstellende Matrix von f ist (7.5). Damit haben wir Satz 7.1 im Falle $k = 2$ bewiesen.

Wir beweisen den Satz 7.1 nun allgemein. Wir beginnen wieder mit der *Eindeutigkeit*. Seien

$$U_0 := \{0\} \subset U_1 := \ker(f) \subset U_2 := \ker\left(f^2\right) \subset \ldots \subsetneq U_k := \ker\left(f^k\right) = V.$$

Wir setzen $m_j := \dim U_j$. Falls wir ein Abbildungsverhalten gemäss dem Schema (7.2) haben, so ist die „unterste Schicht" vor 0 (d.h. $v_{d_1}, v_{d_1+d_2}, \ldots$) eine Basis von $\ker(f) = U_1$, die unterste und die zweitunterste Schicht zusammen eine Basis von $U_2 = \ker(f^2)$, etc. Die Anzahl der Vektoren in diesen Schichten legt jedoch das Schema bis auf die Reihenfolge der Basisvektoren eindeutig fest. Somit wird die Jordanmatrix (bis auf die Reihenfolge der Blöcke) eindeutig durch die Dimensionen der U_i festgelegt.

Nun zur *Existenz:* Für $1 \leq j \leq k$ setzen wir

$$r_j := m_j - m_{j-1}.$$

Wir beweisen mit Induktion nach k die folgende Aussage:

$\boldsymbol{A}_k$: Sei $0 \leq t \leq r_k$ und die Vektoren $u_1, \ldots, u_t$ seien linear unabhängig in $U_k \backslash U_{k-1}$ mit

$$L[u_1, \ldots, u_t] \cap U_{k-1} = \{0\}. \tag{7.8}$$

Dann lassen sich $u_1, \ldots, u_t$ zu einer Jordanbasis ergänzen, in der $u_1, \ldots, u_t$ in der „obersten Schicht" sind:

$$\begin{array}{ccccccc} u_1 & \cdots & u_t & \cdots & & \\ \downarrow & & \downarrow & & & \\ \vdots & & \vdots & & \vdots & \\ \downarrow & & \downarrow & & \downarrow & \\ 0 & \cdots & 0 & \cdots & 0 & \end{array}$$

Falls wir diese Aussagen bewiesen haben, so ist die Existenz einer Jordanbasis gezeigt, denn für $t = 0$ ist die Bedingung (7.8) leer. Die Aussage enthält daher die Existenz einer Jordanbasis als Spezialfall. Die allgemeinere Version der Aussage ist jedoch bequem für den Induktionsschluss.

$k = 1$ (d.h. $f = 0$) ist trivial.

Wir führen den Induktionsschluss $A_{k-1} \Longrightarrow A_k$, $k \geq 2$.

Nach Lemma 7.2 ergänzen wir zunächst u_1, …, u_t durch Vektoren u_{t+1}, …, u_{r_k} (wenn nötig), für die gilt:

(1) $u_1, \ldots, u_{r_k}$ sind linear unabhängig

(2)

$$L\left[u_1, \ldots, u_{r_k}\right] \cap U_{k-1} = \{0\}. \tag{7.9}$$

Wegen $m_{k-1} + r_k = m_k = \dim V$ folgt daraus $V = U_{k-1} \oplus L\left[u_1, \ldots, u_{r_k}\right]$.

Man beachte, dass $u_1, \ldots, u_{r_k} \notin U_{k-1}$ gilt. Wir betrachten die Vektoren $f(v_1), \ldots, f(u_{r_k})$.

Lemma 7.4 *a)* $f(u_1), \ldots, f(u_{r_k}) \in U_{k-1} \backslash U_{k-2}$.

b) $f(u_1), \ldots, f(u_{r_k})$ *sind linear unabhängig. Insbesondere sind sie alle verschieden.*

c) $L\left[f(u_1), \ldots, f(u_{r_k})\right] \cap U_{k-2} = \{0\}$.

Beweis. Der Beweis ist im wesentlichen eine Repetition des Beweises von Lemma 7.3.

a): Zunächst ist $f(u_i) \in U_{k-1}$, denn aus $f^k = 0$ folgt $f^{k-1}(f(u_i)) = 0$, d.h. $f(u_i) \in \ker\left(f^{k-1}\right) = U_{k-1}$. Andererseits gilt $f(u_i) \notin U_{k-2}$, denn aus $f(u_i) \in U_{k-2}$ würde $f^{k-1}(u_i) = f^{k-2}(f(u_i)) = 0$ folgen, es würde also gelten $u_i \in U_{k-1}$. Damit ist a) bewiesen.

b), c): Sei

$$\sum_{i=1}^{r_k} \alpha_i f(u_i) \in U_{k-2}. \tag{7.10}$$

Dann folgt

$$f^{k-1}\left(\sum_{i=1}^{r_k} \alpha_i u_i\right) = f^{k-2}\left(\sum_{i=1}^{r_k} \alpha_i f(u_i)\right) = 0,$$

d.h. $\sum_{i=1}^{r_k} \alpha_i u_i \in \ker f^{k-1} = U_{k-1}$. Andererseits gilt $\sum_{i=1}^{r_k} \alpha_i u_i \in L[u_1, \ldots, u_{r_k}]$. Wegen $U_{k-1} \cap L[u_1, \ldots, u_{r_k}] = \{0\}$ folgt $\sum_{i=1}^{r_k} \alpha_i u_i = 0$, und wegen der linearen Unabhängigkeit der u_i folgt $\alpha_1 = \ldots = \alpha_{r_k} = 0$, d.h. insbesondere $\sum_{i=1}^{r_k} \alpha_i f(u_i) = 0$. Dies beweist c). Das Argument liefert aber auch einen Beweis von b), denn aus $\sum_{i=1}^{r_k} \alpha_i f(u_i) = 0$ folgt natürlich (7.10) und somit $\alpha_1 = \ldots = \alpha_{r_k} = 0$, wie gerade gezeigt wurde. ■

Mit diesem Lemma können wir den Induktionsbeweis einfach zu Ende führen:

U_{k-1} ist natürlich invariant unter f. Wir bezeichnen die Einschränkung von f auf $V' := U_{k-1}$ mit f'. Natürlich gilt nun $f'^{k-1} = 0$. Ferner ist für $j \leq k-1$: $\ker(f'^j) = U_j \subset V'$. Nach dem Lemma sind $f(u_1), \ldots, f(u_{r_k})$ linear unabhängige Vektoren in $V' \backslash U_{k-2} = U_{k-1} \backslash U_{k-2}$ mit $L[f(u_1), \ldots, f(u_{r_k})] \cap U_{k-2} = \{0\}$. Nach Induktionsvoraussetzung können wir deshalb $f(u_1), \ldots, f(u_{r_k})$ zu einer Jordanbasis $\mathcal{J}'$ von f' in V' ergänzen mit $f(u_1), \ldots, f(u_{r_k})$ in der obersten Schicht des Schemas. Dann ist $\mathcal{J}'$ zusammen mit $u_1, \ldots, u_{r_k}$ wegen (7.9) eine Basis von V und ist dann offensichtlich eine Jordanbasis von f in V :

$$\begin{array}{ccccccc} u_1 & \cdots & u_{r_k} & & & & \\ \downarrow & & \downarrow & & & & \\ f(u_1) & \cdots & f(u_{r_k}) & \cdots & & & \\ \downarrow & \cdots & \downarrow & \cdots & & & \\ & & & & & & \\ \downarrow & \cdots & \downarrow & \cdots & \downarrow & & \\ 0 & \cdots & 0 & \cdots & 0 & & \end{array}$$

Um das Schema (7.2) zu erhalten, müssen wir die Basis nur noch umstellen: $v_1 := u_1$, $v_2 := f(u_1), \ldots, v_k := f^{k-1}(u_1)$, $v_{k+1} := u_2, \ldots$

Wir haben die Existenz einer Jordanbasis bewiesen.

Die Zusatzbehauptungen im Satz 7.1 folgen sehr einfach: Die Anzahl der Jordanblöcke ist per Konstruktion gleich $\dim(\ker f)$ und die maximale Blockgrösse ist gleich der maximalen Länge der Spalten im Schema (7.2) (ohne den Nullvektor am Schluss), also gleich der kleinsten Zahl k mit $f^k = 0$. Damit ist der Satz vollständig bewiesen.

Bemerkung 7.2 *Das obige Lemma impliziert, dass $r_1 \geq r_2 \geq \ldots \geq r_k \geq 1$ gilt, was von vornherein nicht selbstverständlich ist.*

Bemerkung 7.3 *Der Beweis liefert auch ein Konstruktionsschema für eine Jordanbasis. Man beginnt auf der höchsten Stufe, sucht also unabhängige Vektoren $u_{k,1}, \ldots, u_{k,r_k} \notin U_{k-1}$ mit*

$$L[u_{k,1}, \ldots, u_{k,r_k}] \cap U_{k-1} = \{0\}. \tag{7.11}$$

(Zur Hervorhebung der Schichten verwenden wir Doppelindizes). Falls $r_k = 1$ ist, muss man einfach einen Vektor $\notin U_{k-1}$ wählen. Für $r_k > 1$ muss man jedoch

etwas sorgfältiger vorgehen um $L[u_{k,1},\ldots,u_{k,r_k}]\cap U_{k-1}=\{0\}$ *zu garantieren. Am besten wählt man zunächst eine Basis in* U_{k-1} *und ergänzt sie dann durch* $u_{k,1},\ldots,u_{k,r_k}$ *zu einer Basis in* $U_k=V$*. Dann ist (7.11) garantiert. Die Basis von* U_{k-1} *kann man anschliessend wegwerfen.*

Nun bildet man die $u_{k,1},\ldots,u_{k,r_k}$ *mit* f *ab und ergänzt daraufhin* $u_{k-1,1}:=f(u_{k,1}),\ldots,u_{k-1,r_k}:=f(u_{k,r_k})$ *(die gemäss dem Lemma 7.4 unabhängig sind) so durch Vektoren* $u_{k-1,r_k+1},\ldots,u_{k-1,r_{k-1}}\in U_{k-1}$*, dass* $u_{k-1,1},\ldots,u_{k-1,r_{k-1}}$ *unabhängig sind und*

$$L\left[u_{k-1,1},\ldots,u_{k-1,r_{k-1}}\right]\cap U_{k-2}=\{0\}$$

gilt. Am besten wählt man zuerst eine Basis $\mathcal{U}_{k-2}$ *von* U_{k-2}*. Dann sind die Vektoren aus* $\mathcal{U}_{k-2}$ *und* $u_{k-1,1},\ldots,u_{k-1,r_k}$ *nach dem Lemma 7.4 unabhängig und wir können sie durch* $u_{k-1,r_k+1},\ldots,u_{k-1,r_{k-1}}$ *zu einer Basis von* U_{k-1} *ergänzen. Die Basis* $\mathcal{U}_{k-2}$ *von* U_{k-2} *kann man dann wieder verschrotten, und man fährt mit der* $(k-2)$*-ten Schicht weiter, indem man* $u_{k-2,1}:=f(u_{k-1,1}),\ldots,u_{k-2,r_{k-1}}:=f\left(u_{k-1,r_{k-1}}\right)$ *bildet, diese dann wieder ergänzt etc. Am Schluss muss man die gefundene Basis noch in der richtigen Reihenfolge aufschreiben um ein Schema der Form (7.2) zu erhalten.*

Der Satz 7.1 hat natürlich eine Formulierung mit Matrizen:

Satz 7.2 *Sie* A *eine* $n\times n$*-Matrix mit der Eigenschaft, dass* $k\in\mathbb{N}$ *existiert mit* $A^k=0$*. Dann existiert eine reguläre Matrix* S*, sodass* $S^{-1}AS$ *die Form (7.1) hat.*

Beispiel 7.1 *Wir betrachten die reelle* 5×5*-Matrix*

$$A:=\begin{pmatrix}1&1&0&0&0\\-1&0&1&0&0\\1&0&-1&0&0\\-1&0&1&1&1\\1&0&-1&-1&-1\end{pmatrix}.$$

Das charakteristische Polynom ist $\chi_A(x)=-x^5$*. Nach Cayley-Hamilton ist demzufolge* $A^5=0$*, d.h. die Matrix ist nilpotent. Der Rang von* A *ist 3 und demzufolge ist die geometrische Vielfachheit des Eigenwertes* 0 *gleich* 2*. Daraus folgt, dass zwei Jordanblöcke existieren. Nun gibt es noch zwei Möglichkeiten für die Blockgrössen, nämlich* 1 *&* 4 *oder* 2 *&* 3*. Um zu entscheiden, welcher Fall vorliegt, müssen wir* $U_2=\ker A^2$ *betrachten. Sind die Blockgrössen* 1 *&* 4*, so ist* $\dim(U_2)=3$ *und im anderen Fall* 4*.*

$$A^2=\begin{pmatrix}0&1&1&0&0\\0&-1&-1&0&0\\0&1&1&0&0\\0&-1&-1&0&0\\0&1&1&0&0\end{pmatrix}.$$

Der Rang ist offenbar gleich 1 *und damit ist* $\dim U_2 = 4$. *Wir sehen also, dass die Blockgrössen* 2 *&* 3 *sind. Es folgt also, dass eine reguläre Matrix* S *existiert mit*

$$S^{-1}AS = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{7.12}$$

Um S *zu bestimmen, müssen wir einfach eine Jordanbasis gemäss dem Beweis des Satzes 7.1 konstruieren. Offenbar ist* $r_1 = r_2 = 2$, $r_3 = 1$. *Wir wählen einfach einen Vektor* v_1, *der nicht in* $U_2 = \ker A^2$ *ist. (7.9) ist dann automatisch erfüllt, da* $r_3 = 1$ *gilt. Wir können z.B.*

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

nehmen. v_2 *und* v_3 *erhalten wir durch Anwendung von* A :

$$v_2 = Av_1 = A \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \; v_3 = Av_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \end{pmatrix}.$$

Etwas mehr Aufwand ist es, einen geeigneten Vektor $v_4 \in U_2$ *zu finden. Es reicht nicht, dass* v_2, v_4 *linear unabhängig und nicht in* U_1 *sind. Dann haben wir nämlich keine Garantie dafür, dass (7.9) erfüllt ist. Um* v_4 *zu finden, wählen wir eine beliegige Basis in* U_1, *z.B.* v_3 *und* $\overline{v} := \begin{pmatrix} -1 \\ 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$, *und ergänzen* $v_3, \overline{v}, v_2$ *zu einer Basis in* U_2. *Wegen* $\dim U_2 = 4$ *wird dafür noch ein Vektor benötigt, unser gewünschtes* v_4. *Eine Möglichkeit ist* $v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$. *Nun können wir* $\overline{v}$ *vergessen, er hat seine Schuldigkeit getan, nämlich ein geeigenetes* v_4 *zu finden. Die Konstruktion erzwingt, dass* $U_1 \cap L[v_2, v_4] = \{0\}$ *gilt. Nun ergibt sich* v_5 *als*

Av_4, also

$$v_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}.$$

Damit haben wir unsere Basis $(v_1, v_2, v_3, v_4, v_5)$ beisammen. Sie wird nach folgendem Schema abgebildet:

$$\begin{array}{ccccccc} v_1 & \to & v_2 & \to & v_3 & \to & 0 \\ & & v_4 & \to & v_5 & \to & 0 \end{array}.$$

Damit ist die darstellende Matrix bezüglich dieser Basis durch die rechte Seite von (7.12) gegeben. S ist einfach die Matrix der Basistransformation, d.h. wir schreiben einfach die v_i in die Spalten:

$$S := \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 1 \\ 0 & -1 & 1 & 0 & -1 \end{pmatrix}.$$

Wenn wir uns nicht verrechnet haben, gilt nun die Gleichung (7.12).

7.2 Die Jordansche Normalform

In diesem Abschnitt ist wieder $f : V \to V$ ein Endomorphismus. Wir setzen jedoch nun nur voraus, dass das Minimalpolynom $m_f(x)$ in Linearfaktoren zerfällt. Ist der Grundkörper K algebraisch abgeschlossen, so ist das stets der Fall, insbesondere also im Fall $K = \mathbb{C}$.

Das Ziel ist, f als direkte Summe von Endomorphismen auf invarianten Unterräumen darzustellen, wobei die Einschränkungen von f auf diese invarianten Unterräume dann mit Hilfe des Satzes aus dem letzten Unterkapitel diskutiert werden können.

Sei $\operatorname{spec}(f) = \{\lambda_1, \ldots, \lambda_s\}$. Da das Spektrum gleich der Nullstellenmenge des Minimalpolynoms ist, folgt, dass das Spektrum nicht leer ist. Ferner ist das Minimalpolynom $m(x)$ nach Voraussetzung gegeben durch

$$m(x) = \prod_{i=1}^{s} (x - \lambda_i)^{t_i}.$$

Der Eigenraum von λ_i ist gegeben durch $E(\lambda_i) = \ker(f - \lambda_i \operatorname{id}_V)$. Wir definieren nun eine Folge von Unterräumen durch

$$E_m(\lambda_i) := \ker\left((f - \lambda_i \operatorname{id}_V)^m\right),\ m \geq 1.$$

$E_1(\lambda_i)$ ist einfach der Eigenraum $E(\lambda_i)$.

Lemma 7.5 *a) Es gilt* $E_1(\lambda_i) \subset E_2(\lambda_i) \subset E_3(\lambda_i) \subset \ldots$

b) Sei m_i *die kleinste natürliche Zahl mit* $E_{m_i}(\lambda_i) = E_{m_i+1}(\lambda_i)$. *Dann gilt* $E_j(\lambda_i) = E_{m_i}(\lambda_i)$ *für alle* $j > m_i$.

Beweis. a) folgt unmittelbar aus der Definition der Unterräume. Man beachte, dass nicht alle Inklusionen $E_j \subset E_{j+1}$ echt sein können, sonst könnte V nicht endlichdimensional sein. Deshalb existiert eine kleinste Zahl m_i mit $E_{m_i}(\lambda_i) = E_{m_i+1}(\lambda_i)$. Ist $j \geq m_i + 2$ und $v \in E_j(v_i)$, so gilt

$$(f - \lambda_i \mathrm{id}_V)^j (v_i) = (f - \lambda_i \mathrm{id}_V)^{m_i+1} \left((f - \lambda_i \mathrm{id}_V)^{j-m_i-1} (v_i) \right) = 0,$$

Also ist $(f - \lambda_i \mathrm{id}_V)^{j-m_i-1} (v_i) \in E_{m_i+1}(\lambda_i) = E_{m_i}(\lambda_i)$, und wir erhalten

$$(f - \lambda_i \mathrm{id}_V)^{j-1} (v_i) = (f - \lambda_i \mathrm{id}_V)^{m_i} \left((f - \lambda_i \mathrm{id}_V)^{j-m_i-1} (v_i) \right) = 0,$$

d.h. $v_i \in E_{j-1}(\lambda_i)$. Wir haben also gezeigt, dass für alle $j \geq m_i + 2$ die Gleichung $E_j(\lambda_i) = E_{j-1}(\lambda_i)$ gilt. ■

Definition 7.3 $E_{m_i}(\lambda_i)$ *bezeichnet man als den* ***verallgemeinerten Eigenraum*** *des Eigenwertes* λ_i. *Wir schreiben ihn als* $\overline{E}(\lambda_i)$.

Lemma 7.6 *a) Die* $\overline{E}(\lambda_i)$ *sind invariant unter* f.

b) Für $i \neq j$ *gilt*

$$\overline{E}(\lambda_i) \cap \overline{E}(\lambda_j) = \{0\}.$$

Beweis. a): Sei $v \in \overline{E}(\lambda_i)$. Dann gilt

$$\begin{aligned}(f - \lambda_i \mathrm{id}_V)^{m_i} (f(v)) &= \left((f - \lambda_i \mathrm{id}_V)^{m_i} \circ f\right)(v) \\ &= \left(f \circ (f - \lambda_i \mathrm{id}_V)^{m_i}\right)(v) \\ &= f\left((f - \lambda_i \mathrm{id}_V)^{m_i} (v)\right) = 0.\end{aligned}$$

Daraus folgt $f(v) \in \overline{E}(\lambda_i)$.

b): Sei $v \in \overline{E}(\lambda_i)$, $v \neq 0$. Wir zeigen, dass für $j \neq i$ stets $(f - \lambda_j \mathrm{id}_V)^m (v) \neq 0$ für alle $m \in \mathbb{N}$ gilt.

Es existiert eine kleinste Zahl $r \in \mathbb{N}$ mit $(f - \lambda_i \mathrm{id}_V)^r (v) = 0$. Dann ist

$$\overline{v} := (f - \lambda_i \mathrm{id}_V)^{r-1} (v) \neq 0.$$

Daraus folgt aber $(f - \lambda_i \mathrm{id}_V)(\overline{v}) = 0$, d.h. $\overline{v}$ ist ein Eigenvektor zum Eigenwert λ_i. Einsetzen ergibt

$$(f - \lambda_j \mathrm{id}_V)^m (\overline{v}) = (\lambda_i - \lambda_j)^m \overline{v} \neq 0,$$

d.h.

$$\begin{aligned}(f - \lambda_i \mathrm{id}_V)^{r-1} \left((f - \lambda_j \mathrm{id}_V)^m (v)\right) &= (f - \lambda_j \mathrm{id}_V)^m \left((f - \lambda_i \mathrm{id}_V)^{r-1} (v)\right) \\ &= (f - \lambda_j \mathrm{id}_V)^m (\overline{v}) \neq 0.\end{aligned}$$

Dann muss jedoch auch $(f - \lambda_j \mathrm{id}_V)^m (v) \neq 0$ gelten. ■

Satz 7.3

$$V = \bigoplus_{i=1}^{s} \overline{E}(\lambda_i)$$

Beweis. Der Beweis besteht nach Satz 6.1 aus zwei Teilen:
A) Für jedes i gilt

$$\overline{E}(\lambda_i) \cap \left(\sum_{j:j\neq i} \overline{E}(\lambda_j) \right) = \{0\}.$$

B)

$$V = \sum_{i=1}^{s} \overline{E}(\lambda_i)$$

Beweis von A):
Wir müssen nachweisen, dass aus

$$\sum_{i=1}^{s} v_i = 0,\ v_i \in \overline{E}(\lambda_i)$$

folgt, dass alle $v_i = 0$ sind. Wir beweisen mit Induktion nach r, dass aus

$$\sum_{i=1}^{r} v_i = 0,\ v_i \in \overline{E}(\lambda_i) \tag{7.13}$$

folgt, dass alle $v_i = 0$ sind. Der Fall $r = 1$ ist trivial. Wir nehmen also $r \geq 2$ an. Anwendung von $(f - \lambda_r \operatorname{id}_V)^{m_r}$ auf die Summe ergibt (wegen $v_r \in \overline{E}(\lambda_r)$)

$$\sum_{i=1}^{r-1} (f - \lambda_r \operatorname{id}_V)^{m_r}(v_i) = 0.$$

Wegen der f-Invarianz der $\overline{E}(\lambda_i)$ ist $(f - \lambda_r \operatorname{id}_V)^{m_r}(v_i) \in \overline{E}(\lambda_i)$. Nach Induktionsvoraussetzung folgt also $(f - \lambda_r \operatorname{id}_V)^{m_r}(v_i) = 0$ und somit $v_i \in \overline{E}(\lambda_r)$ für alle $i = 1, \ldots, r-1$. Nach Lemma 7.6 b) gilt also $v_i = 0$ für $i = 1, \ldots, r-1$ und wegen (7.13) auch für $i = r$.

Beweis von B)

Nach der Generalvoraussetzung in diesem Unterkapitel zerfällt das Minimalpolynom in Linearfaktoren, ist also von der Form

$$m_f(x) = \prod_{i=1}^{s} (x - \lambda_i)^{t_i},\ t_i \in \mathbb{N}.$$

(Wir wissen schon aus dem letzten Kapitel (Satz 6.17), dass die Nullstellen des Minimalpolynoms genau die Eigenwerte sind. Das Minimalpolynom muss deshalb die obige Form haben.) Wir betrachten die Polynome

$$p_j(x) := \prod_{\substack{i=1 \\ i \neq j}}^{s} (x - \lambda_i)^{t_i}.$$

Diese Polynome sind teilerfremd. Nach Lemma 6.8 existieren Polynome $h_i(x)$ mit

$$1 = \sum_{i=1}^{s} p_i(x) h_i(x).$$

Daraus folgt $f = \sum_{i=1}^{s} p_i(f) \circ h_i(f)$. Sei $v \in V$. Dann gilt

$$v = \sum_{i=1}^{s} (p_i(f) \circ h_i(f))(v).$$

Wir setzen $v_i := (p_i(f) \circ h_i(f))(v)$. Nun folgt ganz einfach, dass $v_i \in \overline{E}(\lambda_i)$ ist:

$$\begin{aligned}(f - \lambda_i \operatorname{id}_V)^{t_i}(v_i) &= \left((f - \lambda_i \operatorname{id}_V)^{t_i} \circ p_i(f)\right)(h_i(f)(v)) \\ &= m_f(f)(h_i(f)(v)) = 0.\end{aligned}$$

Wir haben somit gezeigt, dass sich jeder Vektor in V als Summe von Vektoren aus den verallgemeinerten Eigenräumen darstellen lässt. Damit ist B) bewiesen. ■

Wir formulieren nun den „Hauptsatz" über die Jordanzerlegung:

Satz 7.4 *Sei V ein endlichdimensionaler K-Vektorraum und $f : V \to V$ ein Endomorphismus, dessen Minimalpolynom in Linearfaktoren zerfällt. Sei* $\operatorname{spec}(f) = \{\lambda_1, \ldots, \lambda_k\}$. *Dann existiert eine Basis von V, bezüglich der die darstellende Matrix A die folgende Gestalt hat:*

$$A = \begin{pmatrix} J(\lambda_1) & 0 & \cdots & 0 \\ 0 & J(\lambda_2) & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J(\lambda_k) \end{pmatrix}. \tag{7.14}$$

Dabei sind die $J(\lambda_i)$ quadratische $n_i \times n_i$-Matrizen, $n_i = \dim\left(\overline{E}(\lambda_i)\right)$, der folgenden Gestalt:

$$J(\lambda_i) = \begin{pmatrix} J^{\lambda_i}_{d_{i,1}} & 0 & \cdots & \cdots & 0 \\ 0 & J^{\lambda_i}_{d_{i,2}} & 0 & & \vdots \\ \vdots & 0 & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & J^{\lambda_i}_{d_{i,r_i}} \end{pmatrix}.$$

Dabei ist r_i (d.h. die Anzahl der Jordanblöcke für den Eigenwert λ_i) die geometrische Vielfachheit von λ_i und n_i ist die algebraische Vielfachheit von λ_i. Das Minimalpolynom von f ist

$$m_f(x) = \prod_{i=1}^{s} (x - \lambda_i)^{m_i}, \tag{7.15}$$

wobei $m_i := \min\left\{k : E_k(\lambda_i) = \overline{E}(\lambda_i)\right\}$ *gilt. Ferner ist* $m_i = \max\{d_{i,1}, \ldots, d_{i,r_i}\}$.

Beweis. Wir beweisen die Existenz.

Nach Lemma 7.6 a) sind die verallemeinerten Eigenräume $\overline{E}(\lambda_i)$ f-invariant. Wir können deshalb f auf die $\overline{E}(\lambda_i)$ einschränken. Diese Einschränkung bezeichnen wir mit f_i. Nach Satz 7.3 stellt sich f als direkte Summe der f_i dar, also $f = \bigoplus_{i=1}^{k} f_i$, wie im Abschnitt 6.2 eingeführt wurde. Nach der Diskussion in diesem Abschnitt benötigen wir nur Basen in den einzelnen Unterräumen $\overline{E}(\lambda_i)$, bezüglich welchen sich die f_i durch die $J(\lambda_i)$ darstellen. Denn wegen Satz 7.3 ist die Vereinigung dieser Basen der $\overline{E}(\lambda_i)$ eine Basis in V, und ferner ist die darstellende Matrix von f bezüglich dieser Basis in V durch (7.14) gegeben.

Wir betrachten nun die Endomorphismen

$$g_i := f_i - \lambda_i \operatorname{id}_{\overline{E}(\lambda_i)}$$

auf $\overline{E}(\lambda_i)$. Per Definition ist $g_i^{m_i} = 0$. Nach Satz 7.1 existiert eine Basis in $\overline{E}(\lambda_i)$, bezüglich der die darstellende Matrix von g_i von der Form (7.1) ist. Die darstellende Matrix von f_i gewinnt man einfach, indem man dazu $\lambda_i E_{n_i}$ addiert. Das ist jedoch nichts anderes als die Matrix $J(\lambda_i)$. Damit ist die Existenz einer Jordanbasis gezeigt. Man beachte, dass m_i die maximale Grösse der Jordanblöcke zu λ_i ist.

Die Zusatzbehauptungen folgen sehr einfach: Falls die darstellende Matrix durch (7.14) gegeben ist, so ist das charakteristische Polynom natürlich

$$\prod_{i=1}^{s} (\lambda_i - x)^{n_i}.$$

Somit sind die n_i die algebraischen Vielfachheiten der Eigenwerte.

Wegen $\ker(f - \lambda_i \operatorname{id}_V) \subset \overline{E}(\lambda_i)$ gilt $\ker(f - \lambda_i \operatorname{id}_V) = \ker\left(f_i - \lambda_i \operatorname{id}_{\overline{E}(\lambda_i)}\right)$. Demzufolge ist $\dim(\ker(f - \lambda_i \operatorname{id}_V))$ - also die geometrische Vielfachheit von λ_i - gleich der Anzahl der Jordanblöcke des nilpotenten Endomorphismus $f_i - \lambda_i \operatorname{id}_{\overline{E}(\lambda_i)}$, d.h. einfach gleich der Anzahl der Jordanblöcke in A für den Eigenwert λ_i.

Wir hatten schon oben bemerkt dass m_i die maximale Grösse der Jordanblöcke zum Eigenwert λ_i ist. Wir zeigen noch, dass das Minimalpolynom durch (7.15) gegeben ist. Bezeichnet $p(x)$ das Polynom auf der rechten Seite von (7.15), so

bildet $p(f)$ offensichtlich jeden Vektor der entsprechenden Jordanbasis nach Null ab, d.h. es gilt $p(f) = 0$. Daraus folgt, dass das Minimalpolynom $p(x)$ teilt. Andererseits gilt jedoch für jeden echten Teiler $q(x)$ von $p(x)$ die Ungleichung $q(f) \neq 0$, was man folgendermassen sieht:

Sei

$$q(x) = \prod_{j=1}^{s} (x - \lambda_j)^{t_j},$$

mit $t_j \leq m_j$ und $t_i < m_i$ für mindestens ein i. Dann wird die „oberste Schicht" der Jordanbasis in $\overline{E}(\lambda_i)$ unter $\left(f_i - \lambda_i \operatorname{id}_{\overline{E}(\lambda_i)}\right)^{t_i}$ nicht nach Null abgebildet, also auch nicht unter $(f - \lambda_i \operatorname{id}_V)^{t_i}$. Ist nun v ein solcher Vektor $\in \overline{E}(\lambda_i)$ mit $w := (f - \lambda_i \operatorname{id}_V)^{t_i}(v) \neq 0$. Wegen der Invarianz von $\overline{E}(\lambda_i)$ ist $(f - \lambda_j \operatorname{id}_V)^k (w) \in \overline{E}(\lambda_i)$ für jedes $k \in \mathbb{N}$. Für $j \neq i$ ist dann $(f - \lambda_j \operatorname{id}_V)^{t_j}(w) \neq 0$ wegen $\overline{E}(\lambda_i) \cap \overline{E}(\lambda_j) = \{0\}$.

Demzufolge ist

$$q(f)(v) = \left(\prod_{j=1,\, j\neq i}^{s} (f - \lambda_j)^{t_j} \right)(w) \neq 0.$$

Wir haben also gezeigt, dass jeder echter Teiler von $p(x)$ den Endomorphismus nicht anulliert. Demzufolge ist $p(x)$ das Minimalpolynom.

Der Beweis der Eindeutigkeit der Jordanmatrix (bis auf die Reihenfolge der Blöcke) sei dem Leser überlassen. (Man muss nur zeigen, dass jede Jordanbasis in Basen der $\overline{E}(\lambda_i)$ zerfällt. Anschliessend benützt man die Eindeutigkeit aus Satz 7.1. ■

8 Nicht negative reelle Matrizen, Markoff-Ketten

8.1 Einführende Begriffe, Beispiele

In diesem Kapitel ist $K = \mathbb{R}$. Wir bezeichnen mit $M^+(n, \mathbb{R})$ oder kurz $M^+(n)$ die Menge der $n \times n$-Matrizen $A = (a_{ij})$ mit $a_{ij} \geq 0$ für alle i, j. Diese Matrizen sind besonders wichtig und haben spezielle Eigenschaften, die wir in diesem Kapitel diskutieren werden.

Eine Matrix $A \in M^+(n)$ heisst **stochastisch**, wenn $\sum_{j=1}^{n} a_{ij} = 1$ für alle $1 \leq i \leq n$ gilt. Eine stochastische Matrix ist also einfach eine Matrix in $M^+(n)$, die den Vektor

$$\mathbf{1} := \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

als Eigenvektor zum Eigenwert 1 hat.

Für jede quadratische $n \times n$-Matrix A und $k \in \mathbb{N}_0$ bezeichnen wir wie üblich A^k die k-te Matrixpotenz von A, mit der Festlegung $A^0 := E_n$, und schreiben $a_{ij}^{(k)}$ für die Komponenten dieser Matrix.

Für viele Anwendungen ist es etwas unnatürlich, dass die Indizes der Matrizenelemente von 1 bis n laufen. Wir können statt dessen eine beliebige endliche Indexmenge I nehmen und dann quadratische Matrizen $(a_{ij})_{i,j \in I}$. Da wir die Indexmenge I natürlich einfach durchnumerieren können, spielt das hier keine Rolle.

Stochastische Matrizen schreiben wir meist als $P = (p_{ij})_{i,j \in I}$. Sie spielen in der Wahrscheinlichkeitstheorie eine grosse Rolle. p_{ij} wird dann als die Wahrscheinlichkeit interpretiert, mit der man in den „Zustand j" wechselt, falls man gerade „im Zustand i" ist. Die Bedingung $\sum_{j \in I} p_{ij} = 1$ ist die grundlegende Annahme der Wahrscheinlichkeitsrechnung. (Wir setzen voraus, dass einige Grundkenntnisse über Wahrscheinlichkeitsrechnung aus dem Gymnasium bekannt sind).

Ein wichtiges Problem ist die Untersuchung der Wahrscheinlichkeiten bei Iterationen des zufälligen Vorgangs. Man fragt sich, mit welcher Wahrscheinlichkeit man im Zustand j ist, wenn man in i startet, aber die „zufällige Bewegung" zwei Mal ausführt. Nach einer grundlegenden Regel der Wahrscheinlichkeitsrechnung muss man einfach über die Zustände k, die man nach dem ersten Schritt erreichen kann, summieren und dabei die Wahrscheinlichkeiten multiplizieren. Also: Nach zwei Schritten gelangt man von i nach j mit Wahrscheinlichkeit $\sum_k p_{ik} p_{kj}$. Das ist natürlich nichts anderes als die ij-te Komponente von P^2. Analog: Wenn man die Wahrscheinlichkeiten berechnen will, mit denen man nach n Schritten von i nach j gelangt, muss man einfach die Matrix P zur n-ten Potenz nehmen und dann die ij-te Komponente davon nehmen. Wir bezeichnen diese Komponente

in Zukunft mit $p_{ij}^{(n)}$. Natürlich ist P^n auch wieder eine stochastische Matrix.

Eine derartige Abfolge von Zufallsschritten nennt man in der Wahrscheinlichkeitstheorie eine Markoff-Kette. Von besonderem Interesse ist das Verhalten von solchen Markoff-Ketten für grosse n. Dies hängt eng mit den in der Physik besonders wichtigen Ergodensätzen zusammen. Wir können hier jedoch nur andeutungsweise darauf eingehen.

Wir betrachten einige Beispiele.

8.1.1 Irrfahrten auf Graphen

Ein (endlicher) Graph $\mathcal{G} = (E, K, \varphi)$ besteht aus einer endlichen Menge E von **Ecken** (englisch "vertices") und einer endlichen Menge K von **Kanten** (englisch "edges"). Jeder Kante $k \in K$ wird ein Paar $\varphi(k) = \{e, e'\}$ von Ecken zugeordnet. Es kann auch $e = e'$ gelten. In diesem Fall ist $\varphi(k)$ eine einelementige Menge. Formal ist φ einfach eine Abbildung von K in die Menge der ein- oder zweielementigen Teilmengen von E. Man sagt dann, dass die Kante k die Ecken e, e' „verbindet", wenn $\varphi(k) = \{e, e'\}$ gilt. Man beachte, dass wir zulassen, dass zwei verschiedene Kanten dieselben Ecken verbindet und dass eine Kante eine Ecke „mit sich selbst" verbindet.

Für jede Ecke $e \in E$ bezeichnen wir mit K_e die Menge der Kanten, die an e „anstossen", d.h.

$$K_e := \{k \in K : e \in \varphi(k)\}.$$

Analog bezeichen wir mit $K_{e,e'}$ die Menge der Kanten, die e mit e' verbinden:

$$K_{e,e'} := \{k \in K : \varphi(k) = \{e, e'\}\}.$$

Wir setzen nun voraus, dass der Graph $\mathcal{G} = (E, K, \varphi)$ die Eigenschaft hat, dass $K_e \neq \emptyset$ für jede Ecke e gilt, und definieren eine stochastische Matrix $(p_{e,e'})_{e,e' \in E}$ durch

$$p_{e,e'} := \frac{|K_{e,e'}|}{|K_e|}.$$

Wir setzen natürlich $p_{e,e'} := 0$, wenn $K_{e,e'} = \emptyset$ gilt. Es ist offensichtlich, dass $\sum_{e'} p_{e,e'} = 1$ für jede Ecke e ist. Zur Veranschaulichung stellt man sich diese sogenannte „Übergangsmatrix" wie folgt vor. Ein Wanderer bewegt sich zufällig auf dem Graphen. Befindet er sich zu einem Zeitpunkt in einer Ecke e, so wählt er unter den an e anstossenden Kanten zufällig (und mit gleicher Wahrscheinlichkeit) eine aus und bewegt sich dann auf dieser Kante zur nächsten Ecke.

Hier ein konkretes

Beispiel 8.1 *Wir nehmen* $E = \{1, 2, 3\}$ *und folgende Kanten: Eine Kante, die* 1 *mit sich verbindet, eine, die* 1 *mit* 2 *verbindet, zwei Kanten, die* 2 *mit* 3 *verbinden,*

und noch eine Kante, die 3 *mit sich verbindet. Dann ist die zugehörige Matrix gegeben durch*

$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \end{pmatrix}.$$

Interessiert man sich für die Übergangswahrscheinlichkeiten nach 3 *Schritten, so hat man*

$$P^3 = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \end{pmatrix}^3 = \begin{pmatrix} \frac{7}{24} & \frac{31}{72} & \frac{5}{18} \\ \frac{31}{108} & \frac{25}{108} & \frac{13}{27} \\ \frac{5}{27} & \frac{13}{27} & \frac{1}{3} \end{pmatrix}$$

zu berechnen. Bei Start in 1 *hat man also Wahrscheinlichkeit* $\frac{31}{72}$*, nach* 3 *Schritten in* 2 *zu sein. Nehmen wir* 20 *Schritte, so erhalten wir den komplizierten Ausdruck:*

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \end{pmatrix}^{20} = \begin{pmatrix} \frac{304\,686\,352\,736\,285}{1\,218\,719\,480\,020\,992} & \frac{456\,998\,388\,430\,463}{1\,218\,719\,480\,020\,992} & \frac{114\,258\,684\,713\,561}{304\,679\,870\,005\,248} \\ \frac{456\,998\,388\,430\,463}{1\,828\,079\,220\,031\,488} & \frac{685\,601\,424\,167\,221}{1\,828\,079\,220\,031\,488} & \frac{6347\,031\,550\,313}{16\,926\,659\,444\,736} \\ \frac{114\,258\,684\,713\,561}{457\,019\,805\,007\,872} & \frac{6347\,031\,550\,313}{16\,926\,659\,444\,736} & \frac{42\,847\,817\,108\,965}{114\,254\,951\,251\,968} \end{pmatrix}.$$

Nach Rundung ergibt sich jedoch ein ganz einfacher Ausdruck:

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \end{pmatrix}^{20} \simeq \begin{pmatrix} 0.250\,01 & 0.374\,98 & 0.375\,01 \\ 0.249\,99 & 0.375\,04 & 0.374\,97 \\ 0.250\,01 & 0.374\,97 & 0.375\,02 \end{pmatrix} \simeq \begin{pmatrix} \frac{1}{4} & \frac{3}{8} & \frac{3}{8} \\ \frac{1}{4} & \frac{3}{8} & \frac{3}{8} \\ \frac{1}{4} & \frac{3}{8} & \frac{3}{8} \end{pmatrix}.$$

Wir werden später verstehen, wieso die Übergangswahrscheinlichkeiten nach vielen Iterationen so einfach werden.

8.1.2 Irrfahrten auf Gruppen

G sei eine endliche Gruppe, und μ sei ein sogenannter Wahrscheinlichkeitsvektor auf G: μ ist einfach eine Abbildung von G nach $[0,1]$ mit $\sum_{g\in G}\mu(g) = 1$.

Lemma 8.1 *$P = (p_{g,h})_{g,h\in G}$ definiert durch*

$$p_{g,h} := \mu\left(hg^{-1}\right)$$

ist eine stochastische Matrix.

Beweis. Für jedes feste $g \in G$ definiert die Abbildung $\phi_g : G \to G$, $h \to hg^{-1}$ eine Bijektion. In der Tat: ϕ_g ist injektiv, denn aus $hg^{-1} = h'g^{-1}$ folgt $h = (hg^{-1})\,g = (h'g^{-1})\,g = h'$, sowie surjektiv, denn für jedes $h \in G$ gilt $h = hgg^{-1} = \phi_g(hg)$. Daraus folgt

$$\sum_{h\in G} p_{g,h} = \sum_{h\in G}\mu\left(hg^{-1}\right) = \sum_{h\in G}\mu(h) = 1$$

für jedes $g \in G$. ■

Man beachte, dass $p_{g,hg} = \mu(h)$ ist. $\mu(h)$ ist also einfach die Wahrscheinlichkeit, mit der man von einem beliebigen Element g nach hg springt. Man bezeichnet das deshalb auch als eine „Linksirrfahrt" auf G. Analog kann man die Rechtsirrfahrt durch $p_{g,h} = \mu(g^{-1}h)$ definieren.

Als Beispiel betrachten wir ein einfaches Modell dafür, einen Stapel Jasskarten zu mischen. Natürlich können wir (zu mathematischen Zwecken) einfach annehmen, dass die Karten von 1 bis 36 durchnumeriert sind. Die Menge I der möglichen Reihenfolgen der Karten ist dann einfach die Menge der Permutationen dieser 36 Zahlen. Wir definieren nun eine stochastische Matrix $P = (p_{\sigma,\pi})_{\sigma,\pi\in I}$, die eines der Standardverfahren modelliert, bei dem man einfach den Stapel 3 Mal überschlägt. (Im Englischen wird das „overhand shuffling" genannt. Wir beschränken uns auf dreimaliges Überschlagen nur der Einfachheit halber.) Mathematisch lässt sich das wie folgt formulieren: Wir wählen 3 Zahlen $1 \leq m_1 < m_2 < m_3 < 36$. Dann definieren wir eine Permutation π_m, $m = (m_1, m_2, m_3)$ wie folgt: Der Stapel $\{m_3 + 1, 36\}$ wird an die Spitze verschoben, der Stapel $\{m_2 + 1, m_3\}$ an die zweite Stelle etc, d.h.

$$\pi = \begin{pmatrix} 1 & \cdots & & & & & & & & \cdots & 36 \\ m_3+1 & \cdots & 36 & m_2+1 & \cdots & m_3 & m_1+1 & \cdots & m_2 & 1 & \cdots & m_1 \end{pmatrix}.$$

Nun geben wir unter μ jeder dieser speziellen Permutationen die gleiche Wahrscheinlichkeit. Es gibt offenbar so viele derartige Permutation, wie es Möglichkeiten gibt, 3 Zahlen aus den Zahlen $1, \ldots, 35$ auszuwählen, also $\binom{35}{3} = \frac{35\cdot 34\cdot 33}{6} = 6545$. Wir definieren daher $\mu(\pi) = 1/6545$, falls π von dieser Form ist, und andernfalls $\mu(\pi) = 0$. $p_{\sigma,\pi\sigma} = \mu(\pi)$ gibt dann einfach die Wahrscheinlichkeit an, mit der man von der Permutation σ zur Permutation $\pi\sigma$ gelangt.

Man beachte übrigens, dass es gigantisch viele Permutationen von 36 Elementen gibt, nämlich

$$36! = 371993326789901217467999448150835200000000.$$

Rechnet man das Alter des Universums zu 10 Milliarden Jahren, so ist das 10^{24} mal das Alter des Universums in Sekunden. Trotz dieser unvorstellbar grossen Zahl ist es das „Traumziel" des Kartenmischers, nach einigen wenigen Iterationen des Mischvorgangs jede dieser Möglichkeiten mit etwa gleicher Wahrscheinlichkeit zu erhalten. Für eine wirklich gute Durchmischung in diesem Sinne ist „overhand shuffling" nicht besonders gut geeignet. Man würde ca. 50 Iterationen benötigen. Das unter Pokerspielern üblichere „riffle shuffling" ist wesentlich besser und führt nach ca. 7 Iterationen (bei 52 Karten) zum Ziel. Wir werden hier jedoch nachweisen können, dass der Mischvorgang „im Prinzip" zum Ziel führt: dass nämlich nach n-facher Iteration für $n \to \infty$ sich asymptotisch die Gleichverteilung einstellt.

Als weiteres Beispiel betrachten wir noch die abelsche Gruppe $(\mathbb{Z}_n, +)$. Ist $\mu(1) = \mu(-1) = 1/2$, $\mu(i) = 0$ für alle anderen Elemente, so gilt einfach $p_{ij} = 1/2$

für $j = i \pm 1$, und 0 sonst. Dieses Beispiel können wir auch als Irrfahrt auf einem Graphen auffassen: Als Eckpunktmenge nehmen wir $\mathbb{Z}_n$, und $\{i, i+1\}$ sind jeweils durch Kanten verbunden. Bei einer anderen Wahl von μ ist dies jedoch i.allg. nicht mehr möglich (z.B. für $\mu(1) = p$, $\mu(-1) = 1-p$ und $p \neq 1/2$).

8.1.3 Gittermodelle der statistischen Physik

Wir betrachten ein ganz einfaches 1-dimensionales Modell der statistischen Physik, das sogenannte eindimensionale Ising-Modell. Allen Punkten i eines eindimensionalen Gitters $\{1, \ldots, n\}$ ordnen wir sogenannte „Spinvariablen" σ_i zu. Diese Spins können „up", d.h. $\sigma_i = +1$, oder „down", d.h. $\sigma_i = -1$ sein. Wir haben mathematisch also einfach eine Folge $\sigma_1, \ldots, \sigma_n$ von ± 1-Grössen.

Wir suchen nun ein Modell, bei dem sich benachbarte Spins beeinflussen. In der Physik wird das durch eine Energiefunktion H auf den Spinkonfigurationen beschrieben. Wir nehmen an, dass die Wechselwirkung anziehend, im physikalischen Jargon „ferromagnetisch" ist: Haben benachbarte Spins die gleiche Ausrichtung, so hat die Konfiguration eher tiefe Energie. Die einfachste Möglichkeit, dies zu realisieren, ist durch folgende Energiefunktion gegeben:

$$H(\sigma) := -J \sum_{i=1}^{n-1} \sigma_i \sigma_{i+1},$$

wobei J die Wechselwirkungsenergie ist. Nach einem fundamentalen Prinzip der statistischen Physik stellt sich bei einer Temperatur $T > 0$ (natürlich in Grad Kelvin gerechnet) die folgende Gleichgewichtsverteilung — die sogenannte Gibbs-Verteilung — auf den Spinkonfigurationen $\sigma = (\sigma_1, \ldots, \sigma_n)$ ein

$$G_T(\sigma) := \exp\left[-\frac{1}{kT} H(\sigma)\right] \Big/ Z_n(T).$$

Dabei ist k ein physikalische Konstante, die sogenannte Boltzmann-Konstante, und

$$Z_n(T) := \sum_{\sigma} \exp\left[-\frac{1}{kT} H(\sigma)\right]$$

ist die sogenannte Zustandssumme. Man beachte, dass $\sum_\sigma G_T(\sigma) = 1$ ist. Ferner ist natürlich $G_T(\sigma) > 0$ für alle σ. Wir können die $G_T(\sigma)$ daher als Wahrscheinlichkeiten interpretieren. Es sind die Wahrscheinlichkeiten, mit denen sich das System bei Temperatur T in der Konfiguration σ befindet. Diese Wahrscheinlichkeiten sind offenbar desto grösser, je stärker die Konfiguration σ ausgerichtet ist, d.h. je mehr Paare $(i, i+1)$ es gibt mit $\sigma_i = \sigma_{i+1}$. Wir setzen $\beta := J/kT$. Kleine β entsprechen dann hoher Temperatur und umgekehrt. Man beachte nun, dass sich $\exp[-\beta H(\sigma)]$ wie folgt schreiben lässt:

$$\exp[-\beta H(\sigma)] = \prod_{i=1}^{n-1} A_\beta(\sigma_i, \sigma_{i+1}),$$

wobei $A_\beta = (A_\beta(i,j))_{i,j=\pm 1}$ die folgende Matrix ist:

$$A_\beta := \begin{pmatrix} \mathrm{e}^{\beta} & \mathrm{e}^{-\beta} \\ \mathrm{e}^{-\beta} & \mathrm{e}^{\beta} \end{pmatrix} \in M^+(2)$$

Dies ist die sogenannte „Transfermatrix".

Von fundamentaler Bedeutung in der statistischen Physik ist das Verhalten der sogenannten freien Energie im Limes $n \to \infty$.

$$f(\beta) := \lim_{n\to\infty} \frac{1}{n} \log Z_n(\beta).$$

Nun gilt jedoch

$$Z_n(\beta) = \sum_{\sigma_1,\sigma_n=\pm 1} A_\beta^{n-1}(\sigma_1,\sigma_n), \tag{8.1}$$

so dass wir wieder darauf stossen, die Potenzen einer positiven Matrix zu berechnen. Wir werden $f(\beta)$ etwas später berechnen.

8.2 Irreduzibilität, Periodizität

Wir betrachten in diesem Abschnitt eine Matrix $A \in M^+(n)$, $A = (a_{ij})_{i,j\in I}$. Die n-te Potenz bezeichnen wir mit $A^n = \left(a_{ij}^{(n)}\right)_{i,j\in I}$. Wir führen einige Notationen ein. Seien $i,j \in I$, $n \in \mathbb{N}_0$. Wir schreiben:

$$i \overset{n}{\longrightarrow} j \overset{\text{Def}}{\Longleftrightarrow} a_{ij}^{(n)} > 0,$$

$$i \longrightarrow j \overset{\text{Def}}{\Longleftrightarrow} \exists n \in \mathbb{N}_0 \text{ mit } i \overset{n}{\longrightarrow} j,$$

$$i \sim j \overset{\text{Def}}{\Longleftrightarrow} i \longrightarrow j \text{ und } j \longrightarrow i.$$

Lemma 8.2 *a)* $i \overset{n}{\longrightarrow} j,\ j \overset{m}{\longrightarrow} k \Longrightarrow i \overset{n+m}{\longrightarrow} k$.
b) $i \longrightarrow j,\ j \longrightarrow k \Longrightarrow i \longrightarrow k$.
c) $\sim$ *ist eine Äquivalenzrelation auf* I.

Beweis. a) Aus $a_{ij}^{(n)} > 0$ und $a_{jk}^{(m)} > 0$ folgt

$$a_{ik}^{(n+m)} = \sum_{s\in I} a_{is}^{(n)} a_{sk}^{(m)} \geq a_{ij}^{(n)} a_{jk}^{(m)} > 0.$$

b) folgt sofort aus a).

c) Reflexivität folgt aus $a_{ii}^{(0)} = 1 > 0$. Die Symmetrie folgt aus der Definition. Die Transitivität folgt aus b). ■

Definition 8.1 *A heisst* ***irreduzibel****, wenn alle Paare $i, j \in I$ äquivalent sind, d.h. wenn für $i, j \in I$ stets ein $n \in \mathbb{N}_0$ existiert mit $a_{ij}^{(n)} > 0$.*

Ist $i \in I$, so betrachten wir die Menge $\Gamma_i := \left\{ n \in \mathbb{N} : i \xrightarrow{n} i \right\}$. Man beachte, dass $0 \notin \Gamma_i$ ($\mathbb{N} := \{1, 2, 3, \ldots\}$). $\pi(i) := \mathrm{ggT}(\Gamma_i)$ ist die sogenannte ***Periode*** *von i. Ist $\Gamma_i = \emptyset$, so setzen wir $\pi(i) := \infty$.*

Lemma 8.3 *Ist $\pi(i) < \infty$, so existiert ein $n_0 \in \mathbb{N}$ mit $n\pi(i) \in \Gamma_i$ für alle $n \geq n_0$.*

Beweis. Lemma 8.2 a) zeigt, dass Γ_i abgeschlossen unter der Addition ist: Sind $n, m \in \Gamma_i$, so gilt $n + m \in \Gamma_i$. Wir zeigen: Ist Γ eine beliebige nichtleere Teilmenge von $\mathbb{N}$ mit dieser Eigenschaft und $\pi := \mathrm{ggT}(\Gamma)$, so gilt $n\pi \in \Gamma$, wenn n gross genug ist. (Die genaue Herkunft von Γ spielt weiter keine Rolle; wir lassen deshalb den Index i weg).

Zunächst zeigen wir, dass eine endliche Teilmenge $\Gamma' \subset \Gamma$ existiert mit $\mathrm{ggT}(\Gamma') = \mathrm{ggT}(\Gamma) = \pi$. Dies sieht man wie folgt ein: Sei $\Gamma_n = \Gamma \cap \{1, \ldots, n\}$. Da Γ nicht leer ist, ist Γ_n nicht leer, wenn n gross genug ist. Sei $g_n := \mathrm{ggT}(\Gamma_n)$. Da g_{n+1} alle Elemente in Γ_{n+1} teilt, teilt es auch alle Elemente in Γ_n, und somit teilt g_{n+1} auch g_n. Insbesondere folgt $g_n \geq g_{n+1} \geq g_{n+2} \geq \ldots$. Nun kann aber nur endlich oft ein striktes Ungleichheitszeichen stehen, und somit existiert ein m mit $g_\ell = g_m$ für alle $\ell \geq m$. Daraus folgt aber sofort, dass g_m der grösste gemeinsame Teiler aller Elemente in Γ ist, also $g_m = \pi$.

Sei nun $\Gamma_m = \{n_1, n_2, \ldots, n_k\}$, d.h. $\pi = \mathrm{ggT}(n_1, \ldots, n_k)$. Dann existieren Zahlen $l_1, \ldots, l_k \in \mathbb{Z}$, so dass $\pi = \sum_{i=1}^{k} l_i n_i$ ist (vgl. Abschnitt 6.4.3). Weil alle n_j Vielfache von π sind, existiert ein $K \in \mathbb{N}$ mit

$$\sum_{j=1}^{k} n_j = K\pi.$$

Sei

$$L := (K-1)\left(\max_j |l_j|\right), \text{ und } n_0 := KL.$$

Sei $n \geq n_0$. Division durch K mit Rest ergibt

$$n = RK + r,\ R \geq L,\ 0 \leq r \leq K-1.$$

Demzufolge gilt

$$\begin{aligned} n\pi = RK\pi + r\pi &= \sum_{j=1}^{k} Rn_j + r\sum_{j=1}^{k} l_j n_j \\ &= \sum_{j=1}^{k} (R + rl_j)\, n_j. \end{aligned}$$

Wegen $R \geq L$ und der Definition von L folgt aber $R + rl_j \geq 0$, d.h. $R + rl_j \in \mathbb{N}_0$ für alle j. Aus der Abgeschlossenheit unter der Addition folgt dann aber $\sum_{j=1}^{k} (R + rl_j) n_j \in \Gamma$. Somit ist nachgewiesen, dass für alle $n \geq n_0$ die Zahl $n\pi$ in Γ ist. ■

Proposition 8.1 *Ist $i \sim j$ so gilt $\pi(i) = \pi(j)$.*

Beweis. Ist $i = j$, so folgt natürlich $\pi(i) = \pi(j)$. Wir können daher voraussetzen, dass $i \neq j$ gilt. Per Definition existieren dann $n, m \in \mathbb{N}$ mit $i \xrightarrow{n} j$ und $j \xrightarrow{m} i$. Wegen Lemma 8.2 a) folgt dann $i \xrightarrow{n+m} i$, $j \xrightarrow{n+m} j$. Somit sind $\pi(i), \pi(j) < \infty$. Nach Lemma 8.3 existiert $n_0 \in \mathbb{N}$ mit $j \xrightarrow{n_0\pi(j)} j$ und $j \xrightarrow{(n_0+1)\pi(j)} j$. Nochmals 8.2 a) angewandt ergibt:

$$i \xrightarrow{n+n_0\pi(j)+m} i,\ i \xrightarrow{n+(n_0+1)\pi(j)+m} i.$$

Daraus folgt $\pi(i) \mid n+n_0\pi(j)+m$ und $\pi(i) \mid n+(n_0+1)\pi(j)+m$, d.h. $\pi(i) \mid \pi(j)$. Analog zeigt man $\pi(j) \mid \pi(i)$. Daher gilt $\pi(i) = \pi(j)$. ■

Diese Proposition besagt also, dass die Periode eine Klassengrösse unter der obigen Äquivalenzrelation ist, d.h. die Periode ist auf jeder Äquivalenzklasse eine konstante Funktion. Insbesondere gilt für jede irreduzible Matrix, dass alle Elemente von I dieselbe Periode haben. Man spricht dann einfach von der Periode der Matrix.

Definition 8.2 *Eine irreduzible Matrix $A \in M^+(n)$ heisst **aperiodisch,** wenn die Periode der Matrix 1 ist.*

Wir zitieren ohne Beweis (der nicht sehr schwierig, aber etwas länglich und nicht allzu interessant ist), den folgenden Satz:

Satz 8.1 *Sei A irreduzibel mit Periode $p \geq 2$. Dann existiert eine Zerlegung von I in p disjunkte Teilmengen:*

$$I = I_1 \cup \ldots \cup I_p,\ I_i \cap I_j = \emptyset \text{ für } i \neq j,$$

mit der folgenden Eigenschaft: Für alle $k \in \{1, \ldots, p\}$ und alle $i \in I_k$ gilt $\left\{ j \in I : i \xrightarrow{1} j \right\} \subset I_{k+1}$ (mit der Konvention $I_{p+1} := I_i$). In Worten: Von I_k aus kann man in einem Schritt nur nach I_{k+1} gelangen.

Die Zerlegung $\{I_k : 1 \leq k \leq p\}$ ist die Zerlegung von I nach Äquivalenzklassen bezüglich der Matrix A^p.

Wir diskutieren noch kurz die Beispiele aus Abschnitt 8.1. Die Irrfahrt auf Graphen ist genau dann irreduzibel, wenn der Graph zusammenhängend ist.

Definition 8.3 *Ein Graph $\mathcal{G} = (E, K, \varphi)$ heisst **nicht zusammenhängend**, wenn es eine echte nichtleere Teilmenge $A \subset E$ gibt, sodass keine Ecke in A mit einer Ecke ausserhalb A durch eine Kante verbunden ist. Ein Graph der nicht nicht zusammenhängend ist heisst **zusammenhängend.***

Proposition 8.2 *Die stochastische Matrix aus Abschnitt 8.1.1 ist genau dann irreduzibel, wenn $\mathcal{G}$ zusammenhängend ist.*

Der sehr einfache Beweis sei dem Leser überlassen.

Periodiziät oder Aperiodizität für Irrfahrten auf Graphen zu entscheiden, ist i.allg. etwas schwieriger. Es ist jedoch evident, dass wenn in einem zusammenhängenden Graphen auch nur eine Ecke existiert, die mit sich selbst verbunden ist, die Matrix dann aperiodisch ist. Für eine Ecke e, die mit sich selbst verbunden ist, gilt nämlich $p_{e,e} > 0$ und damit $\pi(e) = 1$. Wenn der Graph zusammenhängend ist, folgt daraus jedoch, dass $\pi(e) = 1$ für alle e ist. Irreduzible Irrfahrten auf Graphen sind jedoch aperiodisch oder haben Periode 2. Es gilt nämlich stets $p_{e,e'} > 0 \Leftrightarrow p_{e',e} > 0$. Daraus folgt sofort $p^{(2)}_{e,e} > 0$.

Das Beispiel des „overhand shuffling“ in Abschnitt 8.1.2 ist irreduzibel und aperiodisch. Der Leser möge sich das selbst überlegen. Wir betrachten noch das Beispiel der Irrfahrt auf $(\mathbb{Z}_n, +)$. Die zugehörige Matrix ist offensichtlich irreduzibel, denn man kommt mit positiver Wahrscheinlichkeit von jedem Punkt zu jedem anderen Punkt nach genügend vielen Iterationen. Ebenfalls gilt $p^{(2)}_{i,i} > 0$ für jedes i. Die Periode ist somit 1 oder 2. Ferner ist $p^{(n)}_{i,i} > 0$, weil man in n Schritten einmal „um den Kreis“ laufen kann. Ist n ungerade, so ist die Matrix also aperiodisch (wegen $\mathrm{ggT}(n, 2) = 1$). Ist jedoch n gerade, so kann man die Elemente von $\mathbb{Z}_n$ in die Gruppen der geraden und der ungeraden Elemente aufteilen. Offensichtlich kann man dann in einem Schritt nur von der geraden Gruppe in die ungerade und von der ungeraden Gruppe in die gerade wechseln. Daraus folgt sofort, dass die Periode gleich 2 ist.

8.3 Der Perron-Frobenius Eigenwert

Wir führen die folgenden Bezeichnungen ein:

$$D := \{z \in \mathbb{C} : |z| \leq 1\},$$

$$S := \{z \in \mathbb{C} : |z| = 1\}.$$

Wir benötigen zwei vorbereitende Hilfssätze:

Lemma 8.4 *Seien $z_1, \ldots, z_n \in D$, $\lambda_1, \ldots, \lambda_n \in [0, 1]$ mit $\sum_{k=1}^n \lambda_k = 1$, $\overline{z} := \sum_{k=1}^n \lambda_k z_k \in S$. Dann gilt $z_j = \overline{z}$ für alle j mit $\lambda_j > 0$.*

Beweis. Wir können oBdA annehmen, dass alle $\lambda_k > 0$ sind. Wegen $\overline{z} \in S$ existiert ein $\varphi \in [0, 2\pi)$ mit $\overline{z} = \mathrm{e}^{i\varphi}$. Wir setzen $\widetilde{z}_k := \mathrm{e}^{-i\varphi} z_k$. Dann ist $\sum_{k=1}^n \lambda_k \widetilde{z}_k = 1$. Somit folgt $\sum_{k=1}^n \lambda_k \operatorname{Re}(\widetilde{z}_k) = 1$ oder

$$\sum_{k=1}^{n} \lambda_k \left(1 - \operatorname{Re}(\widetilde{z}_k)\right) = 0.$$

Nun sind jedoch die $\lambda_k > 0$ und die $\widetilde{z}_k$ haben nach wie vor Betrag ≤ 1. Demzufolge ist $\operatorname{Re}(\widetilde{z}_k) \leq 1$ oder $1 - \operatorname{Re}(\widetilde{z}_k) \geq 0$. Aus der obigen Gleichung folgt daher $1 - \operatorname{Re}(\widetilde{z}_k) = 0$ für alle k, d.h. $\operatorname{Re}(\widetilde{z}_k) = 1$, was wegen $\widetilde{z}_k \in D$ impliziert, dass die $\widetilde{z}_k$ alle gleich 1 sind. Das bedeutet aber nichts anderes als $z_k = \mathrm{e}^{i\varphi} = \overline{z}$ für alle k. ■

Lemma 8.5 *Sei A eine irreduzible aperiodische Matrix $\in M^+(n)$. Dann existiert $N \in \mathbb{N}$, sodass alle Matrixelemente von A^N strikt positiv sind.*

Beweis. Nach Lemma 8.3 existiert für jedes $i \in I$ eine natürliche Zahl n_i, sodass $a_{ii}^{(n)} > 0$ für alle $n \geq n_i$ gilt. Da I endlich ist, gilt für $n \geq M := \max_i n_i$: $a_{ii}^{(n)} > 0$ für alle $i \in I$ und $n \geq M$. Weiter gilt wegen der Irreduzibilität, dass für $i, j \in I$ ein $k_{ij} \in \mathbb{N}$ existiert mit $a_{ij}^{(k_{ij})} > 0$. Wieder mit Lemma 8.2 folgt nun $a_{ij}^{(n)} > 0$ für alle $n \geq M + k_{ij}$. Demzufolge gilt $a_{ij}^{(n)} > 0$ für alle $i, j \in I$ und alle $n \geq N := M + \max_{ij} k_{ij}$. ■

Wir formulieren nun den Hauptsatz der Perron-Frobenius-Theorie, aber zunächst nur für stochastische Matrizen $P = (p_{ij})$. Wenn wir nachfolgend von Eigenwerten sprechen, meinen wir immer (möglicherweise) komplexe Eigenwerte. Ist P stochastisch, so wissen wir, dass $1 \in \operatorname{spec}(P)$ gilt.

Satz 8.2 (Perron-Frobenius, stochastische Matrizen) *Sei P eine irreduzible stochastische Matrix. Dann gilt:*

a) Alle (eventuell komplexen) Eigenwerte haben Betrag ≤ 1.

b) 1 ist ein algebraisch (und deshalb auch geometrisch) einfacher Eigenwert.

c) P ist genau dann aperiodisch, wenn 1 der einzige Eigenwert vom Betrag 1 ist.

Beweis. a) Wir fassen P als lineare Abbildung von $\mathbb{C}^I \to \mathbb{C}^I$ auf. Sei $\lambda \in \operatorname{spec}_{\mathbb{C}}(P)$. $(z_i)_{i \in I}$, $z_i \in \mathbb{C}$ sei ein Eigenvektor, d.h. es gilt

$$\sum_j p_{ij}\, z_j = \lambda z_i, \ \forall i \in I.$$

Sei i_0 so gewählt, dass

$$|z_{i_0}| = \max_i |z_i| \tag{8.2}$$

gilt. Dann folgt aus der obigen Gleichung

$$|\lambda|\,|z_{i_0}| = \left|\sum_j p_{i_0 j}\, z_j\right| \le \sum_j p_{i_0 j}\ |z_j|$$
$$\le \sum_j p_{i_0 j}\ |z_{i_0}| = |z_{i_0}|\,.$$

Daraus folgt $|\lambda| \le 1$.

b) Wir zeigen zunächst, dass 1 geometrisch einfach ist. Sei $z \in \mathbb{C}^I$ ein Eigenvektor zum Eigenwert 1. Wir wählen wieder i_0 mit (8.2). Natürlich muss dann $z_{i_0} \neq 0$ gelten, sonst wäre z der Nullvektor. Wir setzen nun

$$x_i := z_i / z_{i_0}. \tag{8.3}$$

Dann ist $x = (x_i)_{i\in I}$ ebenfalls ein Eigenvektor zu 1, denn wir haben ja z nur mit einem Faktor multipliziert. Ferner gilt $x_i \in D$ für alle i. Aus der Gleichung $x = Px$ folgt $x = P^k x$ für alle k, d.h. insbesondere

$$1 = x_{i_0} = \sum_{j\in I} p^{(k)}_{i_0 j} x_j.$$

Nun gilt aber $\sum_j p^{(k)}_{i_0 j} = 1$. Aus Lemma 8.4 folgt daher, dass $x_j = 1$ für alle j mit $p^{(k)}_{i_0 j} > 0$ ist. Wegen der Irreduzibilität existiert jedoch für jedes j mindestens ein k mit $p^{(k)}_{i_0 j} > 0$. Demzufolge haben wir gezeigt, dass $x_j = 1$ für alle j gilt. Dies bedeutet jedoch nichts anderes als dass jeder Eigenvektor von 1 einfach ein Vielfaches des Vektors $\mathbf{1}$ ist. Wir haben also gezeigt, dass die geometrische Vielfachheit des Eigenwertes 1 gleich 1 ist.

Wir müssen nun noch zeigen, dass auch die algebraische Vielfachheit gleich 1 ist. Falls dies nicht der Fall ist, ist der Teil zum Eigenwert 1 in der Jordanmatrix ein Jordanblock der Grösse ≥ 2. Es existiert also eine reguläre Matrix S mit

$$S^{-1}PS = \begin{pmatrix} \boxed{\begin{matrix} 1 & 0 & \cdots & 0 \\ 1 & \ddots & & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & & 1 & 1 \end{matrix}} & & 0 \\ & & \\ 0 & & J \end{pmatrix}.$$

Nun hat die m-te Potenz dieses Jordanblockes in der ersten unteren Nebendiagonalen lauter m, wie man leicht nachrechnet. Demzufolge gilt

$$S^{-1}P^m S = \begin{pmatrix} \boxed{\begin{matrix} 1 & 0 & \cdots & 0 \\ m & \ddots & & \vdots \\ * & \ddots & \ddots & 0 \\ * & * & m & 1 \end{matrix}} & & 0 \\ & & \\ 0 & & J \end{pmatrix}.$$

Somit gilt

$$m = \sum_{j,k} s_{2j}^{(-1)} p_{jk}^{(m)} s_{k1}.$$

Daraus folgt

$$\begin{aligned} m &\leq \sum_j \left| s_{2j}^{(-1)} \right| \sum_k p_{jk}^{(m)} \max_l |s_{l1}| \\ &= \sum_j \left| s_{2j}^{(-1)} \right| \max_l |s_{l1}| , \end{aligned}$$

wegen $\sum_k p_{jk}^{(m)} = 1$ für alle j. Die obige Ungleichung müsste für alle $m \in \mathbb{N}$ gelten, was offensichtlich nicht möglich ist. Deshalb kann die algebraische Vielfachheit von 1 nicht grösser als 1 sein.

c) (I) Wir setzen zunächst voraus, dass P aperiodisch ist.

Sei $\lambda \in \operatorname{spec}_{\mathbb{C}} P$, $|\lambda| = 1$, und $z \in \mathbb{C}^I$ mit $Pz = \lambda z$. Wie üblich wählen wir i_0 mit (8.2) und definieren x durch (8.3). Nach Lemma 8.5 existiert ein N mit $p_{i_0 j}^{(N)} > 0$ für alle j. Nun gilt

$$1 = \left| \lambda^N x_{i_0} \right| = \left| \sum_j p_{i_0 j}^{(N)} x_j \right| .$$

Nach Lemma 8.4 folgt dann, dass alle x_j gleich sind. Daraus folgt insbesondere $\lambda = 1$.

(II) Wir beweisen nun die Umkehrung und zeigen, dass eine periodische (irreduzible) stochastische Matrix noch andere Eigenwerte ausser 1 auf dem Einheitskreis hat. Wir benützen dabei jedoch den hier nicht bewiesenen Satz über die Zyklenzerlegung, Satz 8.1.

Sei also $p \geq 2$ und $I = I_1 \cup \ldots \cup I_p$ die dort eingeführte Zerlegung. Wir definieren für $l \in \{0, 1, \ldots, p-1\}$ den Vektor $z^{(l)} \in \mathbb{C}^I$ durch

$$z_j^{(l)} := \mathrm{e}^{ikl/p},\ j \in I_k,\ 1 \leq k \leq p.$$

(i ist hier die imaginäre Einheit $\sqrt{-1}$.) Dann gilt für $s \in I_k$:

$$\sum_j p_{sj} z_j^{(l)} = \sum_{j \in I_{k+1}} p_{sj} z_j^{(l)} = \sum_{j \in I_{k+1}} p_{sj} \mathrm{e}^{i(k+1)l/p} = e^{il/p} e^{ikl/p},$$

d.h. es folgt

$$\sum_j p_{sj} z_j^{(l)} = \mathrm{e}^{il/p} z_s^{(l)},\ s \in I.$$

Somit gilt

$$1, \mathrm{e}^{i/p}, \mathrm{e}^{2i/p}, \ldots, \mathrm{e}^{(p-1)i/p} \in \operatorname{spec}(P) .$$

(Es ist nicht sehr schwierig zu zeigen, dass das alle Eigenwerte auf dem Einheitskreis sind. Wir wollen das jedoch hier nicht tun.) ■

Wir diskutieren den Satz von Perron-Frobenius nun im allgemeinen Fall positiver Matrizen, indem wir ihn auf den Fall von stochastischen Matrizen zurückführen.

Satz 8.3 (Perron-Frobenius, allgemein) *Sei $A \in M^+(n)$ irreduzibel. $\rho(A)$ sei der sogenannte Spektralradius*

$$\rho(A) := \max\{|\lambda| : \lambda \in \operatorname{spec}_{\mathbb{C}}(A)\}.$$

Dann gilt:

a) $\rho(A) > 0$, $\rho(A) \in \operatorname{spec}(A)$.

b) Es existiert ein Eigenvektor $y = (y_j)_{j\in I}$ zu $\rho(A)$ mit $y_j > 0$ für alle j.

c) $\rho(A)$ ist algebraisch (und geometrisch) einfach.

d) Ist A aperiodisch so gilt

$$\max\{|\lambda| : \lambda \in \operatorname{spec}_{\mathbb{C}}(A) \setminus \{\rho(A)\}\} < \rho(A).$$

Beweis. Sei

$$\Delta := \left\{ x \in \mathbb{R}^I : x_j \geq 0 \ \forall j,\ \sum_j x_j = 1 \right\}.$$

Δ ist ein kompakte Teilmenge von $\mathbb{R}^I$ (siehe Diff.-Int.). Für $x \in \Delta$ definieren wir

$$r_x := \sup\left\{ t \geq 0 : \sum_j a_{ij} x_j \geq t x_i,\ \forall i \right\},$$

und

$$r := \sup_{x\in\Delta} r_x.$$

Die Grundidee des Beweises besteht nun darin, dass man zeigt, dass $r \in \operatorname{spec}(A)$ gilt, und dass zu r ein Eigenvektor mit positiven Komponenten existiert. Damit kann dann der Satz sehr einfach auf den Spezialfall stochastischer Matrizen zurückgeführt werden.

Lemma 8.6 *Es gilt $0 < r < \infty$ und $r \in \operatorname{spec}(A)$. Ferner existiert ein Eigenvektor $y \in \mathbb{R}^I$ zu r mit $y_i > 0$ $\forall i$.*

Beweis. $r > 0$ folgt sehr einfach aus der Irreduzibilität. In der Tat ist offensichtlich $r_{\mathbf{1}} > 0$. Wir geben eine Abschätzung von r nach oben: Aus $t x_i \leq \sum_j a_{ij}\, x_j,\ \forall i$, folgt

$$\begin{aligned} t x_i &\leq \left(\sum\nolimits_j a_{ij}\right) \max_j x_j, \\ t \max_i x_i &\leq \max_i \left(\sum\nolimits_j a_{ij}\right) \max_j x_j, \\ t &\leq \max_i \left(\sum\nolimits_j a_{ij}\right) =: \|A\|. \end{aligned}$$

($\max_i x_i$ ist wegen $\sum_i x_i = 1$ natürlich > 0). Es folgt also $r_x \leq \|A\|$ für alle $x \in \Delta$ und damit $r \leq \|A\|$.

Wir wählen nun eine Folge $(x^{(n)})_{n\in\mathbb{N}}$ in Δ mit $r_{x^{(n)}} \to r$. Wegen der Kompaktheit von Δ können wir eine Teilfolge von $(x^{(n)})_{n\in\mathbb{N}}$ wählen, die in Δ konvergiert. Der Einfachheit halber bezeichnen wir diese ebenfalls mit $\left(x^{(n)}\right)_{n\in\mathbb{N}}$. Es gilt dann also $\lim_{n\to\infty} x_i^{(n)} = y_i$ für alle i, mit $y = (y_i) \in \Delta$. Aus

$$\sum_j a_{ij} x_j^{(n)} \geq r_{x^{(n)}} x_i^{(n)},\ \forall i$$

folgt

$$\sum_j a_{ij} y_j \geq r y_i,\ \forall i. \tag{8.4}$$

Daraus folgt $r \leq r_y$. Wegen $r = \sup_x r_x$ folgt dann aber $r = r_y$.

Wir zeigen nun, dass y ein Eigenvektor zu r ist. Wir zeigen (scheinbar) mehr: Nämlich dass jeder Vektor $y \in \Delta$, der (8.4) erfüllt, automatisch ein Eigenvektor sein muss. Wir bezeichnen mit Δ_r die Menge der Vektoren $\in \Delta$, die diese Ungleichungen erfüllen.

Wir führen den Beweis indirekt und nehmen an, dass $y \in \Delta_r$ existiert, der kein Eigenvektor ist. Für einen derartigen Vektor muss $\sum_j a_{ij} y_j > r y_i$ für mindestens ein $i \in I$ gelten. Andererseits ist jedoch leicht ersichtlich, dass diese Ungleichung nicht für alle i gelten kann. Andernfalls liesse sich ein $\varepsilon > 0$ finden, sodass auch noch $\sum_j a_{ij} y_j > (r+\varepsilon)\, y_i$ für alle i gelten würde. Dies widerspräche der Maximalität von r. Es muss daher eine nichtleere Menge $J \subsetneqq I$ geben mit der Eigenschaft, dass $y \in \Delta_r$ existiert mit $\sum_j a_{ij} y_j > r y_i$ für alle $i \in J$, dass aber kein $y \in \Delta_r$ existiert mit $\sum_j a_{ij} y_j > r y_i$ auf einer Menge, die J echt enthält. Wir führen diese Aussage nun zu einem Widerspruch.

Aus der Irreduzibilität von A folgt, dass ein $s \notin J$ und ein $t \in J$ existiert mit $a_{st} > 0$. Wäre nämlich $a_{st} = 0$ für alle $s \notin J,\ t \in J$, so folgt auch $a_{st}^{(n)} = 0$ für alle $s \notin J,\ t \in J$, was offensichtlich der Irreduzibilität widerspricht. Sei also $s \notin J$, $t \in J$ mit $a_{st} > 0$ und sei $y \in \Delta_r$ so, dass

$$\sum_j a_{ij} y_j \begin{cases} > r y_i & \text{für } i \in J \\ = r y_i & \text{für } i \notin J \end{cases}.$$

Wir können nun $\varepsilon > 0$ so klein wählen, dass auch noch $(r+\varepsilon)\, y_t < \sum_j a_{tj} y_j$ gilt. Wir definieren

$$z_i := \begin{cases} y_i + \varepsilon & \text{für } i = t \\ y_i & \text{für } i \neq t \end{cases}.$$

Dann gilt:

$$r z_i \leq \sum_j a_{ij} z_j,\ \forall i,$$

$$rz_i < \sum_j a_{ij} z_j,\ \forall i \in J,$$

$$\begin{aligned} rz_s = ry_s &= \sum_j a_{sj} y_j < \sum_j a_{sj} y_j + \varepsilon a_{st} \\ &= \sum_j a_{sj} z_j. \end{aligned}$$

Setzen wir

$$\overline{z}_i := \frac{z_i}{\sum_j z_j},$$

so erfüllt auch $\overline{z}$ die obigen Ungleichungen, ist daneben aber noch in Δ. Somit ist es in Δ_r. Ferner gilt

$$r\overline{z}_i < \sum_j a_{ij} \overline{z}_j,\ \forall i \in J \cup \{s\}.$$

Dies steht aber im Widerspruch zur Definition von J. Damit ist unsere Behauptung gezeigt und nachgewiesen, dass jeder Vektor in Δ_r ein Eigenvektor zum Eigenwert r ist. Insbesondere haben wir gezeigt, dass r ein Eigenwert ist.

Bisher haben wir gezeigt, dass $r \in \operatorname{spec}(A)$ und $0 < r < \infty$ gelten und dass ein Eigenvektor $y \in \Delta$ dazu existiert. Wir zeigen nun noch, dass $y_i > 0$ für alle i gilt. Damit ist dann das Lemma bewiesen.

Sei $J := \{i : y_i > 0\}$. Dann ist $J \neq \emptyset$, den sonst wäre $y = 0$ und nicht in Δ. Wir führen $J \neq I$ in ähnlicher (und einfacherer) Weise zu einem Widerspruch wie oben. In diesem Fall wäre nämlich für jedes Element $k \notin J : 0 = y_k = \sum_{j \in J} p_{kj} y_j$, d.h. $p_{kj} = 0$ für jedes Element $k \notin J$, $j \in J$. Das widerspricht jedoch offensichtlich der Irreduzibilität. ■

Schluss des Beweises von Satz 8.3.

Der Beweis kann nun sehr einfach zu Ende geführt werden: Wir nehmen r, y wie im Lemma. Dann definieren wir

$$p_{ij} := \frac{a_{ij} y_j}{r y_i}.$$

Dann ist $P = (p_{ij})$ ein stochastische Matrix. Offensichtlich ist sie irreduzibel und hat dieselben Periodizitätseigenschaften wie die Matrix A. Ferner lassen sich die charakteristischen Polynome sehr einfach ineinander überführen:

$$p_{ij} - x\delta_{ij} = \frac{(a_{ij} - rx\delta_{ij})\, y_j}{r y_i}.$$

Daraus folgt sehr einfach

$$\chi_P(x) = \det(P - xE) = \frac{\det(A - rxE)}{r^{|I|}} = \chi_A(rx)/r^{|I|}. \tag{8.5}$$

Hier haben wir benutzt, dass für jede quadratische Matrix (b_{ij}) und für jeden Vektor (z_i) mit allen Komponenten ungleich Null, (b_{ij}) dieselbe Determinante wie $(b_{ij}z_j/z_i)$ hat, was unmittelbar aus der Definition der Determinante folgt. Wir sehen also:

$$\operatorname{spec}(A) = \{r\lambda : \lambda \in \operatorname{spec}(P)\},$$

und ferner entsprechen sich die algebraischen Vielfachheiten. Somit ist gezeigt, dass r ein Eigenwert von A ist (was wir schon wussten), der die algebraische Vielfachheit 1 hat (was wir noch nicht wussten), ferner gilt

$$r = \max\{|\mu| : \mu \in \operatorname{spec}(A)\} = \rho(A).$$

Ferner ist y ein Eigenvektor von A, und wie wir aus dem Lemma wissen, hat er lauter positive Einträge. Somit sind a) und b) des Satzes bewiesen. c) folgt unmittelbar aus (8.5) und d) folgt aus der Tatsache, dass A genau dann aperiodisch ist, wenn P aperiodisch ist. ■

Wir diskutieren nun eine wichtige Anwendung auf stochastische Matrizen. Ist P eine stochastische Matrix, so ist natürlich P^T im allgemeinen keine stochastische Matrix, aber natürlich nach wie vor eine Matrix $\in M^+(n)$. Ferner stimmen die charakteristischen Polynome von P und P^T überein. Ist P irreduzibel, so ist auch P^T irreduzibel, und ist P aperiodisch, so ist P^T aperiodisch. Das folgt ganz einfach aus der Tatsache, dass die n-te Potenz von P^T die Transponierte der n-ten Potenz von P ist.

Ist P irreduzibel, so folgt also aus Satz 8.3 sofort:

Satz 8.4 *Sei P eine irreduzible stochastische Matrix. Dann existiert genau ein Vektor $\pi = (\pi_i)_{i\in I}$ mit den Eigenschaften:*

$$\pi_i > 0,\ \forall i,\ \sum_i \pi_i = 1,$$

$$\sum_i \pi_i p_{ij} = \pi_j,\ \forall j. \tag{8.6}$$

Beweis. (8.6) bedeutet, dass π, als Spaltenvektor geschrieben, ein Eigenvektor zum Eigenwert 1 von P^T ist. Wir wissen aber nach Satz 8.3, dass $1 \in \operatorname{spec}\left(P^T\right)$ gilt, mit einem Eigenvektor mit lauter positiven (reellen) Komponenten. Mit der Einschränkung $\sum_i \pi_i = 1$ wird dieser eindeutig festgelegt, da 1 geometrisch einfach ist. ■

Bemerkung 8.1 *Vektoren $\pi = (\pi_i)_{i\in I}$ mit $\pi_i \geq 0,\ \forall i,\ \sum_i \pi_i = 1$ nennt man aus naheliegenden Gründen **Wahrscheinlichkeitsvektoren.** Erfüllen sie für eine stochastische Matrix P die Gleichung (8.6), so nennt man sie **stationär** oder **invariant**.*

Für den Beweis des nachfolgenden Satzes (und auch später) benötigen wir das folgende Lemma:

Lemma 8.7 *Die n-te Potenz des Jordanblockes*

$$J_m^\lambda = \begin{pmatrix} \lambda & 0 & \cdots & & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \lambda & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}$$

ist gegeben durch die Matrix

$$\left(J_m^\lambda\right)^n = \sum_{s=0}^{\min(n,m-1)} \binom{n}{s} \lambda^{n-s} F_s.$$

Dabei ist $F_s = \left(f_{ij}^{(s)}\right)$ *die Matrix gegeben durch* $f_{j+s,j}^{(s)} = 1$ *und* 0 *für die anderen Komponenten, d.h.* F_s *hat Einsen in der s-ten unteren Nebendiagonalen und Nullen sonst (*$F_0 = E$, $F_1 = J_m^0$*).*

Beweis. Wir schreiben $J_m^\lambda = \lambda E_m + J_m^0$. Nun multiplizieren wir die Potenz aus, wobei wir berücksichtigen, dass E_m mit allen anderen Matrizen natürlich vertauscht:

$$\left(J_m^\lambda\right)^n = \sum_{s=0}^{n} \binom{n}{s} \lambda^{n-s} \left(J_m^0\right)^s.$$

Nun beachte man, dass $\left(J_m^0\right)^s = F_s$ gilt, wobei $F_s = 0$ für $s \geq m$ ist. ■

Satz 8.5 *Sei P stochastisch, irreduzibel und aperiodisch. Dann gilt für alle* $i, j \in I$

$$\lim_{n\to\infty} p_{ij}^{(n)} = \pi_j.$$

Anders formuliert: $\lim_{n\to\infty} P^n$ *existiert und ist eine Matrix vom Rang* 1 *mit allen Zeilen gegeben durch den stationären Vektor* π*.*

Beweis. Nach dem Hauptsatz über die Jordanzerlegung existiert eine reguläre (möglicherweise komplexe) Matrix S mit

$$P = S \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & J_{m_1}^{\lambda_1} & 0 & \cdots & 0 \\ \vdots & 0 & J_{m_2}^{\lambda_2} & & \vdots \\ & \vdots & & & 0 \\ 0 & 0 & \cdots & 0 & J_{m_k}^{\lambda_k} \end{pmatrix} S^{-1}$$

mit Jordanblöcken $J_{m_i}^{\lambda_i}$. Die λ_i sind möglicherweise nicht alle verschieden, aber alle vom Betrag < 1. Damit gilt

$$P^n = S \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & \left(J_{m_1}^{\lambda_1}\right)^n & 0 & \cdots & 0 \\ \vdots & 0 & \left(J_{m_2}^{\lambda_2}\right)^n & & \vdots \\ & \vdots & & & 0 \\ 0 & 0 & \cdots & 0 & \left(J_{m_k}^{\lambda_k}\right)^n \end{pmatrix} S^{-1}.$$

Aus Lemma 8.7 folgt

$$\lim_{n\to\infty} \left(J_{m_i}^{\lambda_i}\right)^n = 0.$$

Somit gilt

$$\lim_{n\to\infty} P^n = S \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} S^{-1} = \left(a_i b_j\right)_{i,j\in I},$$

wobei (a_i) die erste Spalte von S und (b_j) die erste Zeile von S^{-1} ist. Die erste Spalte von S ist ein Eigenvektor zum Eigenwert 1 von P, d.h. wir können $a_i = 1\ \forall i$, setzen.

Nun gilt

$$\sum_k \pi_k p_{kj} = \pi_j \quad \forall j,$$

und damit gilt auch für alle n

$$\sum_k \pi_k p_{kj}^{(n)} = \pi_j \quad \forall j,$$

und mit einem Limesübergang in dieser Gleichung folgt

$$b_j = \left(\sum_k \pi_k\right) b_j = \lim_{n\to\infty} \sum_k \pi_k p_{kj}^{(n)} = \pi_j.$$

Damit ist der Satz bewiesen. ■

Eine wichtige (und vielfach nicht ganz einfache) Aufgabe ist die Bestimmung des stationären Vektors π. Dazu muss natürlich einfach ein Gleichungssystem gelöst werden, was aber bei sehr grossen Systemen natürlich fast unmöglich ist (Denken Sie an die Indexmenge bei dem Problem der Mischung von Kartenstapeln). In wichtigen Fällen hat man jedoch „Glück“ und man findet einen Vektor, der die sogenannte „detailed balance“ Bedingung erfüllt:

$$\pi_i p_{ij} = \pi_j p_{ji},\ \forall i, j. \tag{8.7}$$

Es ist natürlich klar, dass dieses Gleichungssystem im allgemeinen keine Lösung hat, denn es sind n^2 Gleichungen für n Unbekannte. Wir werden jedoch gleich sehen, dass unsere Beispiele von früher einen Vektor besitzen, der diese Bedingung erfüllt. Wir werden auch später sehen, dass eine stochastische Matrix P, die einen derartigen Vektor besitzt, automatisch diagonalisierbar ist.

Lemma 8.8 *Sei P eine stochastische Matrix und π ein Vektor, der die Bedingung (8.7) erfüllt. Dann ist π stationär.*

Beweis.

$$\sum_i \pi_i p_{ij} = \sum_i \pi_j p_{ji} = \pi_j.$$

■

Beispiel 8.2 *Wir betrachten die Irrfahrt auf einem endlichen Graphen $\mathcal{G} = (E, K, \varphi)$ aus Abschnitt 8.1.1. Die zugehörige Irrfahrt hatte die stochastische Matrix*

$$p_{e,e'} = \frac{|K_{e,e'}|}{|K_e|}.$$

Nun ist offensichtlich $K_{e,e'} = K_{e',e}$. Demzufolge erfüllt der Vektor $(|K_e|)_{e\in E}$ die Bedingung (8.7). Nach Normierung erhalten wir den stationären Wahrscheinlichkeitsvektor

$$\pi_e = \frac{|K_e|}{\sum_{e'} |K_{e'}|}.$$

Nehmen wir etwa das konkrete Beispiel 8.1, so gilt $|K_1| = 2$, $|K_2| = 3$, $|K_3| = 3$. Daher ist der (eindeutige) stationäre Wahrscheinlichkeitsvektor gegeben durch $\left(\frac{1}{4}, \frac{3}{8}, \frac{3}{8}\right)$, und da das Beispiel offensichtlich aperiodisch ist, folgt

$$\lim_{n\to\infty} p^{(n)}_{e,e'} = \pi_{e'}.$$

Beispiel 8.3 *Als weiteres Beispiel betrachten wir Irrfahrten auf Gruppen. In diesem Fall ist die Gleichverteilung ein stationärer Wahrscheinlichkeitsvektor: $\pi_g = 1/|G|$: Es gilt*

$$\sum_g \frac{1}{|G|} p_{g,h} = \frac{1}{|G|} \sum_g \mu\left(hg^{-1}\right) = \frac{1}{|G|} \sum_g \mu(g) = \frac{1}{|G|}.$$

Wenn man zusätzlich weiss, dass die Matrix irreduzibel und aperiodisch ist (was in der Regel nicht sehr schwierig zu entscheiden ist), so folgt

$$\lim_{n\to\infty} p^{(n)}_{g,h} = \frac{1}{|G|}$$

für alle g, h. Das Beispiel erfüllt übrigens nur in den seltensten Fällen die Bedingung (8.7). Betrachten wir etwa die Irrfahrt auf der abelschen Gruppe $(\mathbb{Z}_n, +)$ mit $\mu(1) = p \in (0, 1)$, $\mu(-1) = 1 - p$. Dann ist offensichtlich (8.7) genau dann erfüllt, wenn $p = 1/2$ ist.

Zum Schluss berechnen wir noch die freie Energie für das Ising-Modell aus Abschnitt 8.1.3. Dazu brauchen wir die hier vorgestellte Theorie nicht wirklich, denn es handelt sich ja bei

$$A_\beta = \begin{pmatrix} \mathrm{e}^{\beta} & \mathrm{e}^{-\beta} \\ \mathrm{e}^{-\beta} & \mathrm{e}^{\beta} \end{pmatrix},$$

nur um eine 2×2-Matrix, die wir natürlich bequem von Hand diagonalisieren können. Transfermatrizen (die i.allg. nicht stochastische Matrizen sind), treten jedoch in der Physik sehr häufig auf und können nur in den wenigsten Fällen explizit diagonalisiert werden. Das charakteristische Polynom ist

$$\det \begin{pmatrix} \mathrm{e}^{\beta} - x & \mathrm{e}^{-\beta} \\ \mathrm{e}^{-\beta} & \mathrm{e}^{\beta} - x \end{pmatrix} = x^2 - 2\mathrm{e}^{\beta} x + \mathrm{e}^{2\beta} - \mathrm{e}^{-2\beta},$$

was auf die beiden Eigenwerte $\lambda_1 = 2\cosh\beta > \lambda_2 = 2\sinh\beta$ führt. In Übereinstimmung mit unserer allgemeinen Theorie ist λ_1 ein reeller, positiver und einfacher Eigenwert. Die freie Energie berechnet sich nun sofort mit Hilfe von (8.1) als Logarithmus des grösseren der Eigenwerte:

$$f(\beta) = \lim_{n\to\infty} \frac{1}{n} \log Z_n(\beta) = \log(2\cosh\beta).$$

9 Lineare Differentialgleichungen mit konstanten Koeffizienten

9.1 Das Exponential einer Matrix

Wir betrachten in diesem Kapitel entweder reelle oder komplexe Lösungen von speziellen Differentialgleichungen. Um die beiden Fälle in den Notationen nicht stets doppelt auszuführen, verwenden wir $\mathbb{K}$ für $\mathbb{R}$ oder für $\mathbb{C}$. Sei $A = (a_{ij})$ eine quadratische Matrix $\in M_{\mathbb{K}}(n)$. Wir definieren eine Norm durch

$$\|A\| := \max_i \sum_j |a_{ij}| .$$

Lemma 9.1 *Die obige Norm hat die folgenden Eigenschaften:*
a) Für $A \in M_{\mathbb{K}}(n)$, $\lambda \in \mathbb{K}$ gilt

$$\|\lambda A\| = |\lambda| \, \|A\| .$$

b) Für $A, B \in M_{\mathbb{K}}(n)$ gilt

$$\|A + B\| \leq \|A\| + \|B\| .$$

c) Für $A, B \in M_{\mathbb{K}}(n)$ gilt

$$\|AB\| \leq \|A\| \, \|B\| .$$

Beweis. a) ist evident.
b)

$$\begin{aligned} \max_i \sum_j |a_{ij} + b_{ij}| &\leq \max_i \sum_j (|a_{ij}| + |b_{ij}|) \\ &\leq \max_i \sum_j |a_{ij}| + \max_i \sum_j |b_{ij}| . \end{aligned}$$

c)

$$\|AB\| = \max_i \sum_j \left| \sum_k a_{ik} b_{kj} \right| \leq \max_i \sum_k |a_{ik}| \max_i \sum_j |b_{ij}| = \|A\| \, \|B\| .$$

■

Aus Teil c) des obigen Lemmas folgt insbesondere:

$$\|A^n\| \leq \|A\|^n .$$

Wir definieren nun das Exponential einer quadratischen, reellen oder komplexen Matrix A einfach durch die entsprechende Potenzreihe, wobei wir nachweisen müssen, dass diese konvergiert.

Lemma 9.2 *Sei $A \in M_{\mathbb{K}}(n)$. Dann konvergiert die Reihe $\sum_{n=0}^{\infty} \frac{1}{n!} A^n$ in $\mathbb{K}^{n^2}$, d.h. für jedes Paar i, j von Indizes konvergiert die Reihe $\sum_{n=0}^{\infty} \frac{1}{n!} a_{ij}^{(n)}$ absolut. ($a_{ij}^{(n)}$ ist wie üblich die i,j-te Komponente von A^n).*

Beweis.

$$\frac{1}{n!} \left| a_{ij}^{(n)} \right| \leq \frac{1}{n!} \|A^n\| \leq \frac{1}{n!} \|A\|^n .$$

Aber wie in Diff-Int gelernt, konvergiert die Reihe $\sum_{n=0}^{\infty} \frac{1}{n!} \|A\|^n$. ■

Definition 9.1 *Ist $A \in M_{\mathbb{K}}(n)$, so ist*

$$\exp(A) := \sum_{n=0}^{\infty} \frac{1}{n!} A^n$$

das Exponential der Matrix A. (Wie üblich ist $A^0 = E_n$).

Eine wichtige Eigenschaft der üblichen Exponentialfunktion im Reellen oder Komplexen ist die Gleichung $\exp(a+b) = \exp(a) + \exp(b)$. Dies ist für Matrizen im allgemeinen nicht richtig, wie man leicht an Beispielen nachprüfen kann:

Beispiel 9.1 *Sei $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Dann ist A^2 die Nullmatrix. Demzufolge ist $\exp(A) = E + A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Ferner sei $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Dann ist $B^n = B$ für $n \geq 1$ und alle B und demzufolge $\exp(B) = \begin{pmatrix} \mathrm{e} & 0 \\ 0 & 1 \end{pmatrix}$. Nun ist $A + B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, und $(A+B)^n = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ für $n \geq 1$. Demzufolge gilt $\exp(A+B) = \begin{pmatrix} \mathrm{e} & \mathrm{e} \\ 0 & 1 \end{pmatrix} \neq \exp(A)\exp(B) = \begin{pmatrix} \mathrm{e} & 1 \\ 0 & 1 \end{pmatrix}$.*

Es gilt jedoch der folgende wichtige

Satz 9.1 *Seien $A, B \in M_{\mathbb{K}}(n)$ mit $AB = BA$. Dann gilt*

$$\exp(A+B) = \exp(A)\exp(B) .$$

Beweis. Die Doppelreihe $\sum_{n,m=0}^{\infty} \frac{1}{n!m!} A^n B^m$ ist (komponentenweise) absolut konvergent wegen

$$\left\| \frac{1}{n!m!} A^n B^m \right\| \leq \frac{1}{n!m!} \|A\|^n \|B\|^m$$

und $\sum_{n,m=0}^{\infty} \frac{1}{n!m!} \|A\|^n \|B\|^m < \infty$. Deshalb darf man die Reihe beliebig umsummieren. Dies sollte aus der Vorlesung Diff-Int bekannt sein. Wir erhalten somit einerseits

$$\sum_{n,m=0}^{\infty} \frac{1}{n!m!} A^n B^m = \sum_{n=0}^{\infty} \frac{1}{n!} A^n \sum_{m=0}^{\infty} \frac{1}{m!} B^m = \exp(A) \exp(B)$$

und andererseits

$$\begin{aligned}
\sum_{n,m=0}^{\infty} \frac{1}{n!m!} A^n B^m &= \sum_{k=0}^{\infty} \left(\sum_{n=0}^{k} \frac{1}{n!\,(k-n)!} A^n B^{k-n} \right) \\
&= \sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{n=0}^{k} \binom{k}{n} A^n B^{k-n} \right) \\
&= \sum_{k=0}^{\infty} \frac{1}{k!} (A+B)^k = \exp(A+B),
\end{aligned}$$

wobei wir

$$\sum_{n=0}^{k} \binom{k}{n} A^n B^{k-n} = (A+B)^k$$

benutzt haben, was aus $AB = BA$ folgt. ■

Korollar 9.1 *Für jede quadratische Matrix A ist $\exp(A)$ regulär.*

Beweis. Da A mit $(-A)$ vertauscht folgt $\exp(A)\exp(-A) = \exp(A-A) = \exp(0) = E$. ■

Beispiel 9.2 *Wir betrachten einen Jordanblock $J_m^\lambda = \lambda E_m + J_m^0$. Da E_m mit jeder Matrix vertauscht, folgt*

$$\exp\left(J_m^\lambda\right) = \exp(\lambda E_m) \exp\left(J_m^0\right).$$

Nun ist $\exp(\lambda E_m)$ offensichtlich $e^{\lambda} E_m$. Ferner ist $\left(J_m^0\right)^k = 0$ falls $k \geq m$ ist, und für $k < m$ ist $\left(J_m^0\right)^k$ die Matrix die in der k-ten unteren Nebendiagonalen Einsen hat und sonst überall Nullen. Demzufolge ist

$$\exp\left(J_m^0\right) = \begin{pmatrix}
1 & 0 & \cdots & & \cdots & 0 \\
1 & 1 & 0 & \cdots & & 0 \\
\frac{1}{2!} & 1 & 1 & 0 & \cdots & 0 \\
\frac{1}{3!} & \frac{1}{2!} & 1 & 1 & 0 & \vdots \\
\vdots & & & & \ddots & \vdots \\
\frac{1}{(m-1)!} & \frac{1}{(m-2)!} & \cdots & \frac{1}{2!} & 1 & 1
\end{pmatrix}.$$

$\exp\left(J_m^\lambda\right)$ *ist dann gleich* $e^{\lambda} \exp\left(J_m^0\right)$.

Eine wichtige Bemerkung ist, dass sich die Ähnlichkeitstransformation auf die Exponentialfunktion überträgt: Ist S eine reguläre Matrix und $B = S^{-1}AS$, so gilt auch

$$\exp(B) = S^{-1} \exp(A) S. \tag{9.1}$$

Dies folgt einfach durch die Tatsache, dass $B^n = S^{-1}A^nS$ ist. Daraus folgt sofort für jedes $N \in \mathbb{N}$:

$$\sum_{n=1}^{N} \frac{1}{n!} B^n = S^{-1} \left(\sum_{n=1}^{N} \frac{1}{n!} A^n \right) S,$$

und mit einem Grenzübergang $N \to \infty$ folgt die entsprechende Aussage über Exponentiale.

9.2 Lineare Systeme von Differentialgleichungen

Wir betrachten ein System von Differentialgleichungen der folgenden Form:

$$y_i'(t) = \sum_{j=1}^{n} a_{ij}\, y_j(t)\,,\ t \in \mathbb{R},\ 1 \le i \le n.$$

Die quadratische Matrix $A = (a_{ij})_{1 \le i,j \le n}$ ist dabei eine vorgegebene reelle oder komplexe Matrix. Dabei sollen die Funktionen y_i differenzierbare Abbildungen $\mathbb{R} \ni t \to y_i(t) \in \mathbb{K}$ sein. Der Vektor $y(t) = (y_i(t))_{1 \le i \le n}$ definiert dann eine differenzierbare Abbildung $\mathbb{R} \to \mathbb{K}^n$. Eine Funktion y, die das obige Gleichungssystem erfüllt, heisst Lösung dieses Systems. Wir betrachten derartige Lösungen als Elemente des Vektorraums $C(\mathbb{R}, \mathbb{K}^n)$ der stetigen Funktionen.

Das obige Gleichungssystem lässt sich in Matrizenschreibweise wie folgt darstellen:

$$y'(t) = Ay(t)\,, \tag{9.2}$$

$$y(t) := \begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_n(t) \end{pmatrix}.$$

Die Menge von Lösungen von (9.2) bezeichnen wir mit L_A.

Lemma 9.3 *L_A ist ein Unterraum von $C(\mathbb{R}, \mathbb{K}^n)$.*

Beweis. Seien $y, z \in L_A$ und $\alpha, \beta \in \mathbb{K}$. Dann gilt

$$\begin{aligned}(\alpha y + \beta z)'(t) &= \alpha y'(t) + \beta z'(t) = \alpha A\, y(t) + \beta A\, z(t) \\ &= A(\alpha y(t) + \beta z(t))\,.\end{aligned}$$

■

Lemma 9.4 *Die matrizenwertige Funktion* $\mathbb{R} \ni t \to \exp(tA) \in M_{\mathbb{K}}(n)$ *ist stetig differenzierbar und erfüllt die Gleichung*

$$\frac{d}{dt}\exp(tA) = A\exp(tA)$$

Beweis. Wir zeigen zunächst, dass $t \to \exp(tA)$ stetig ist. Man beachte, dass für $s, t \in \mathbb{R}$ die Matrizen sA und tA vertauschen. Daraus folgt:

$$\exp((t+s)A) = \exp(sA)\exp(tA).$$

Nun gilt

$$\exp(sA) = E + \sum_{j=1}^{\infty} \frac{s^j}{j!} A^j.$$

Für $|s| \leq 1$ gilt $\|(s^j/j!)\,A^j\| \leq \|A\|^j/j!$, d.h. die Reihe oben konvergiert absolut, gleichmässig in $|s| \leq 1$. Demzufolge gilt

$$\begin{aligned}\lim_{s\to 0}\exp((t+s)A) &= \exp(tA)\lim_{s\to 0}\exp(sA)\\ &= \exp(tA)\left[E + \sum_{j=1}^{\infty}\lim_{s\to 0}\frac{s^j}{j!}A^j\right] = \exp(tA).\end{aligned}$$

Damit ist gezeigt, dass die Exponentialfunktion stetig ist. Die Differenzierbarkeit folgt nun in ähnlicher Weise: Für $s \neq 0$:

$$\begin{aligned}\frac{1}{s}\left[\exp((t+s)A) - \exp(tA)\right] &= \frac{\exp(sA) - E}{s}\exp(tA)\\ &= \left(\sum\nolimits_{j=1}^{\infty}\frac{1}{j!}s^{j-1}A^j\right)\exp(tA),\end{aligned}$$

woraus in analoger Weise wie oben

$$\begin{aligned}\lim_{s\to 0}\frac{1}{s}\left[\exp((t+s)A) - \exp(tA)\right] &= \left(\sum\nolimits_{j=1}^{\infty}\frac{1}{j!}\lim_{s\to 0}s^{j-1}A^j\right)\exp(tA)\\ &= A\exp(tA)\end{aligned}$$

folgt. ■

Für $y_0 \in \mathbb{K}^n$ sei

$$z_{y_0}(t) := \exp(tA)\ y_0.$$

z_{y_0} ist offenbar eine stetig differenzierbare Funktion $\mathbb{R} \to \mathbb{K}^n$, also insbesondere ein Element in $C(\mathbb{R}, \mathbb{K}^n)$.

Satz 9.2

$$L_A = \{z_{y_0} : y_0 \in \mathbb{K}^n\}.$$

Beweis. Aus dem vorangegangenen Lemma folgt, dass für jeden Vektor $y_0 \in \mathbb{K}^n$, die Funktion z_{y_0} das Differentialgleichungssystem (9.2) löst.

Wir müssen nun noch nachweisen, dass dies alle Lösungen sind. Sei $y : \mathbb{R} \to \mathbb{K}^n$ eine beliebige Lösung. Wir betrachten die Funktion $t \to z(t) := \exp(-At)\, y(t)$. Differenzieren und Anwendung der Produktregel - zusammen mit dem vorangegangenen Lemma impliziert:

$$\begin{aligned} z'(t) &= -A\exp(-At)\, y(t) + \exp(-At)\, y'(t) \\ &= -A\exp(-At)\, y(t) + \exp(-At)\, A\, y(t) = 0. \end{aligned}$$

Daraus folgt, dass $z(t)$ konstant in t ist, d.h. $z(t) = z(0) = y(0)$. Somit folgt

$$y(t) = \exp(At)\, y(0),$$

d.h. $y = z_{y(0)}$. ■

Korollar 9.2

$$\dim(L_A) = n.$$

Beweis. Wir betrachten die lineare Abbildung $\mathbb{K}^n \ni y_0 \to z_{y_0} \in C(\mathbb{R}, \mathbb{K}^n)$. Diese Abbildung ist injektiv, denn z_{y_0} ist nur die Nullfunktion, wenn $y_0 = 0$ gilt. Demzufolge hat nach Satz 4.18 das Bild dieser Abbildung die Dimension $\dim(\mathbb{K}^n) = n$. Nach Satz 9.2 ist dieses Bild aber L_A. ■

Die gesamte Menge der Lösungen bezeichnet man oft auch als die „allgemeine Lösung“. In vielen Fällen ist man nicht an der gesamten Lösungsmenge, d.h. an der allgemeinen Lösung interessiert, sondern an der „partikulären“ Lösung, die einer bestimmten Anfangsbedingung genügt. Sucht man etwa nach einer Lösung von (9.2), die für $t = 0$ fest vorgegeben ist: $y(0) = y_0$, so ist die eindeutige Lösung mit dieser Anfangsbedingung dann einfach $y(t) = \exp(tA)\, y_0$. Dies lässt sich wie folgt verallgemeinern:

Satz 9.3 *Seien $t_0 \in \mathbb{R}$ und $y_0 \in \mathbb{K}^n$. Dann hat das Gleichungssystem (9.2) genau eine Lösung, die der Anfangsbedingung $y(t_0) = y_0$ genügt. Sie ist gegeben durch*

$$y(t) = \exp((t - t_0)\, A)\, y_0.$$

Beweis. Wir suchen eine Lösung des Gleichungssystems der Form $y(t) = \exp(tA)\, z$ mit der Eigenschaft $y(t_0) = y_0$. Einsetzen ergibt $z = \exp(-t_0 A)\, y_0$. Demzufolge ist $t \to \exp((t - t_0)\, A)\, y_0$ die eindeutige Lösung unseres Problems. ■

Die effektive Berechnung von $\exp(tA)$ ist in der Regel nicht ganz einfach. Der einfachste Fall ist, wenn A diagonalisierbar ist, d.h. wenn eine reguläre Matrix S existiert mit

$$S^{-1}AS = D := \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

Dann ist einfach

$$\exp(tA) = S\exp(tD)S^{-1} = S\begin{pmatrix} \mathrm{e}^{\lambda_1 t} & 0 & \cdots & 0 \\ 0 & \mathrm{e}^{\lambda_2 t} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \mathrm{e}^{\lambda_n t} \end{pmatrix} S^{-1}$$

Ist A nicht diagonalisierbar, jedoch $\mathbb{K} = \mathbb{C}$, so können wir A durch eine Ähnlichkeitstransformation auf Jordansche Normalform bringen und dann die Exponentialfunktion gemäss Beispiel 9.2 ausrechnen. So ist nach diesem Beispiel

$$\exp\left(tJ_m^\lambda\right) = \mathrm{e}^{\lambda t}\begin{pmatrix} 1 & 0 & \cdots & & 0 \\ t & 1 & \ddots & & \\ \frac{t^2}{2!} & t & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \frac{t^{m-1}}{(m-1)!} & \cdots & \frac{t^2}{2!} & t & 1 \end{pmatrix}. \tag{9.3}$$

Der reelle Fall erfordert einige zusätzliche Überlegungen (falls nicht alle Eigenwerte reell sind). Wir wollen das jedoch nicht systematisch diskutieren.

Beispiel 9.3 $n = 3$.

$$y'(t) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & -1 \end{pmatrix} y(t).$$

Man berechnet sofort, dass es drei verschiedene Eigenwerte gibt, nämlich $1, 2$ *und* -1. *Die zugehörige Ähnlichkeitstransformation ist*

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

Demzufolge ist die allgemeine Lösung im Komplexen (oder im Reellen)

$$\begin{pmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} \mathrm{e}^t & 0 & 0 \\ 0 & \mathrm{e}^{2t} & 0 \\ 0 & 0 & \mathrm{e}^{-t} \end{pmatrix}\underbrace{S^{-1}\begin{pmatrix} y_{01} \\ y_{02} \\ y_{03} \end{pmatrix}}_{=:z_0}$$

$$= \begin{pmatrix} 2 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} z_{01}\mathrm{e}^t \\ z_{02}\mathrm{e}^{2t} \\ z_{03}\mathrm{e}^{-t} \end{pmatrix}$$

$$= \begin{pmatrix} 2z_{01}\mathrm{e}^t \\ -2z_{01}\mathrm{e}^t + z_{02}\mathrm{e}^{2t} \\ z_{01}\mathrm{e}^t + z_{03}\mathrm{e}^{-t} \end{pmatrix},\ z_0 \in \mathbb{C}^3 \text{ bzw. } \mathbb{R}^3.$$

Wir diskutieren noch die Differentialgleichung n-ter Ordnung für *eine* Funktion $y : \mathbb{R} \to \mathbb{K}$ (also nicht für einen Vektor), der Form

$$y^{(n)}(t) + a_{n-1}y^{(n-1)}(t) + \ldots + a_0 y(t) = 0. \tag{9.4}$$

Das ist die sogenannte homogene lineare Differentialgleichung n-ter Ordnung mit konstanten Koeffizienten $a_0, \ldots, a_{n-1} \in \mathbb{K}$. $y^{(k)}$ bezeichnet dabei die k-te Ableitung von y. Die inhomogene Gleichung, die wir hier nicht diskutieren, ist von der Form

$$y^{(n)}(t) + a_{n-1}y^{(n-1)}(t) + \ldots + a_0 y(t) = f(t),$$

mit einer vorgegebenen Funktion f.

Wir können die Gleichung (9.4) auf unser Gleichungssystem (9.2) zurückführen, indem wir die n Funktionen $y_1, \ldots, y_n$ wie folgt definieren:

$$\begin{aligned} y_1 &:= y \\ y_2 &:= y' \\ &\vdots \\ y_n &:= y^{(n-1)}. \end{aligned}$$

Dann erhalten wir das System

$$\begin{pmatrix} y_1' \\ y_2' \\ \vdots \\ y_{n-1}' \\ y_n' \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & & \ddots & \ddots & \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & \cdots & -a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n-1} \\ y_n \end{pmatrix}. \tag{9.5}$$

Um Verwechslungen zu vermeiden, bezeichnen wir n-Tupel von Funktionen mit grossen Buchstaben: $Y = (y_i)_{1 \le i \le n}$. Wir bezeichnen mit L die Menge der Funktionen $\mathbb{R} \to \mathbb{K}$, die (9.4) erfüllen, und mit $\widetilde{L}$ die Lösungsmenge der Funktionen $\mathbb{R} \to \mathbb{K}^n$ von (9.5). L ist ebenfalls ein Vektorraum, wie man auf die gleiche Weise wie in Lemma 9.3 sofort nachprüft. Wir definieren die lineare Abbildung

$$p : C(\mathbb{R}, \mathbb{K}^n) \to C(\mathbb{R}, \mathbb{K}), \quad Y = (y_i)_{1 \le i \le n} \to y_1.$$

p ordnet also einem n-Tupel von Funktionen einfach die erste dieser Funktionen zu. Nach der obigen Konstruktion ist eine Funktion $y \in C(\mathbb{R}, \mathbb{K})$ genau dann in L, wenn sie die erste Komponente eines $Y \in \widetilde{L}$ ist. Demzufolge ist die Einschränkung $p|_{\widetilde{L}}$ von p auf $\widetilde{L}$ nach L surjektiv. Andererseits ist diese Einschränkung auch injektiv, denn wenn wir die erste Komponente einer Lösung von (9.5) kennen, können wir die anderen Komponenten einfach durch Ableiten gewinnen. $p|_{\widetilde{L}}$ ist also ein Isomorphismus. (Es mag etwas merwürdig erscheinen,

dass die Abbildung, die einem n-Tupel eine einzige Komponente zuordnet, ein Isomorphismus ist, aber dies liegt einfach daran, dass das ganze n-Tupel durch seine erste Komponente vollständig bestimmt ist.) man muss sich vor Augen halten, dass das L und $\widetilde{L}$ ohnehin „kleine“ Teilräume von unendlichdimensionalen Vektorräumen sind). Aus Korollar 9.2 folgt nun sofort:

Satz 9.4 *Die Dimension des Lösungsraumes L von (9.4) ist n.*

Wir wollen nun eine Basis dieses Lösungsraumes finden. Dazu wollen wir die Eigenwerte von

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & & & & \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & \cdots & -a_{n-1} \end{pmatrix}$$

etwas genauer unter die Lupe nehmen.

Lemma 9.5 *a) Alle (möglicherweise komplexen) Eigenwerte von A sind geometrisch einfach.*

b) Das Minimalpolynom von A ist (bis auf das Vorzeichen) gleich dem charakteristischen Polynom, und dieses ist gegeben durch

$$\chi_A(x) = (-1)^n \left(a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n\right).$$

Beweis. Es ist etwas bequemer, mit der Transponierten von A zu arbeiten. Ist $\mathcal{V} = (v_1, \ldots, v_n)$ die Standardbasis von $\mathbb{C}^n$, so wird diese mit $B := A^T$ nach dem folgenden Schema abgebildet:

$$v_1 \to v_2 \to \ldots \to v_n \to -a_0 v_1 - a_1 v_2 - \ldots - a_{n-1} v_n.$$

Definieren wir das Polynom $p(x) := a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$, so ergibt sich unmittelbar

$$p(B) v_1 = a_0 v_1 + a_1 v_2 + \ldots + a_{n-1} v_n + (-a_0 v_1 - a_1 v_2 - \ldots - a_{n-1} v_n) = 0,$$

und demzufolge

$$p(B) v_k = p(B) B^{k-1} v_1 = B^{k-1} p(B) v_1 = 0$$

für alle $1 \leq k \leq n$. Demzufolge annulliert $p(B)$ sämtliche Basisvektoren, woraus folgt, dass $p(B)$ die Nullmatrix ist. Das Minimalpolynom von B teilt also $p(x)$. Andererseits ergibt sich jedoch sehr einfach, dass kein Polynom $\neq 0$ vom Grade $< n$ die Matrix annulliert. Sei $q(x) = b_0 + b_1 x + \ldots + b_m x^m$ ein derartiges Polynom, $m < n$. Dann ist

$$q(B) v_1 = b_0 v_1 + b_1 v_2 + \ldots + b_m v_{m+1} \neq 0$$

wegen der linearen Unabhängigkeit der Basisvektoren. Wir haben somit gezeigt, dass $p(x)$ das Minimalpolynom von $B = A^T$ ist. Damit ist es natürlich auch (bis aufs Vorzeichen) das charakteristische Polynom, denn letzteres hat Grad n und wird vom Minimalpolynom geteilt. Da das charakteristische Polynom von A mit dem von A^T übereinstimmt, haben wir b) bewiesen. Aus der Diskussion des Minimalpolynoms der Jordanschen Normalform folgt nun sofort, dass alle Eigenwerte von B geometrisch einfach sind. Dies bedeutet natürlich einfach, dass für jeden Eigenwert λ die Matrix $A^T - \lambda E_n$ Rang $n-1$ hat. Dann hat aber auch $A - \lambda E_n$ Rang $n-1$, denn der Rang einer Matrix ist gleich dem Rang der Transponierten. Somit ist jedes $\lambda \in \operatorname{spec}(A) = \operatorname{spec}\left(A^T\right)$ geometrisch einfach für A. Damit ist das Lemma bewiesen.

(Tatsächlich ist das Minimalpolynom von A stets gleich dem Minimalpolynom von A^T, was wir jedoch nicht bewiesen und hier auch nicht benutzt haben). ■

Mit der Information aus diesem Lemma können wir nun den Lösungsraum L von (9.4) bestimmen. Wir betrachten zunächst den Fall $\mathbb{K} = \mathbb{C}$. Seien $\lambda_1, \ldots, \lambda_k$ die verschiedenen Eigenwerte von A, d.h. die verschiedenen Nullstellen von $p(x)$. Aus dem Lemma wissen wir, dass alle diese Eigenwerte geometrisch einfach sind. Die Jordansche Normalform hat deshalb zu jedem Eigenwert nur einen Jordanblock, dessen Grösse gleich der algebraischen Vielfachheit des Eigenwertes ist. Sind $m_1, \ldots, m_k$ die algebraischen Vielfachheiten der Eigenwerte, so existiert also eine reguläre Matrix S mit

$$A = S \begin{pmatrix} J_{m_1}^{\lambda_1} & 0 & \cdots & 0 \\ 0 & J_{m_2}^{\lambda_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_{m_k}^{\lambda_k} \end{pmatrix} S^{-1}.$$

Demzufolge ist

$$\exp(tA) = S \begin{pmatrix} \exp\left(tJ_{m_1}^{\lambda_1}\right) & 0 & \cdots & 0 \\ 0 & \exp\left(tJ_{m_2}^{\lambda_2}\right) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \exp\left(tJ_{m_k}^{\lambda_k}\right) \end{pmatrix} S^{-1}.$$

$\exp\left(tJ_{m_i}^{\lambda_i}\right)$ kennen wir jedoch schon und haben es in (9.3) berechnet. Ist $y_0 \in \mathbb{C}^n$ beliebig, so sehen wir, dass jede Komponente von $Y(t) = \exp(tA)\, y_0$ eine Linearkombination der folgenden Funktionen ist:

$$z_{i,j}(t) = t^{j-1} \mathrm{e}^{\lambda_i t},\ 1 \leq j \leq m_i,\ 1 \leq i \leq k.$$

Dies gilt insbesondere auch für die erste Komponente $y(t) = y_1(t)$, an der wir eigentlich nur interessiert sind. Diese Überlegungen führen nun sehr leicht zum folgenden

Satz 9.5 *Sie $\mathbb{K} = \mathbb{C}$. Die Funktionen $z_{i,j},\ 1 \leq j \leq m_i,\ 1 \leq i \leq k$, bilden eine Basis von L, dem Lösungsraum von (9.4).*

Beweis. Wir haben gesehen, dass sich jede Lösung als Linearkombination der $z_{i,j}$ darstellen lässt. Nun bezeichnen wir mit M die lineare Hülle der $z_{i,j}$. Nach der vorangegangenen Überlegung gilt $L \subset M$. M kann aber höchstens Dimension n haben, denn es gibt insgesamt genau $n = m_1 + \ldots + m_k$ der $z_{i,j}$. Somit muss wegen Satz 9.4 $M = L$ gelten. Insbesondere sind also die $z_{i,j}$ auch tatsächlich alles Lösungen. Andererseits müssen die $z_{i,j}$ linear unabhängig sein, denn sonst wäre $\dim(M) < n$, was wiederum Satz 9.4 widerspräche. ■

Der Fall $\mathbb{K} = \mathbb{R}$ erfordert einige kleine Modifikationen, die wir ohne Beweise vorstellen. Wir berechnen nach wie vor die Eigenwerte von A, d.h. die Nullstellen des charakteristischen Polynoms. Diese können natürlich komplex sein. Da das charakteristische Polynom jedoch reell ist, müssen die komplexen Nullstellen in konjugiert komplexen Paaren vorkommen. Genauer:

Lemma 9.6 *Sei $p(x)$ ein Polynom mit reellen Koeffizienten und sei $\lambda = \alpha + i\beta$ eine komplexe Nullstelle des Polynoms mit algebraischer Vielfachheit m. Dann ist auch die konjugiert komplexe Zahl $\overline{\lambda} := \alpha - i\beta$ eine Nullstelle mit derselben algebraischen Vielfachheit.*

Beweis. Falls nicht aus Diff.-Int. bekannt: Übungsaufgabe. ■

Wenn wir nach den komplexen Lösungen von (9.4) suchen, so müssen wir einfach die Funktionen $t^j \exp(\lambda t),\ \lambda \in \operatorname{spec}_{\mathbb{C}}(A),\ 0 \leq j <$ alg.Vielfachheit von λ, betrachten. Ist λ komplex, $\lambda = \alpha + i\beta$, so sind also $t^j \exp(\alpha t) \exp(i\beta t)$ und $t^j \exp(\alpha t) \exp(-i\beta t)$, also auch

$$t^j \mathrm{e}^{\alpha t} \cos(\beta t) = t^j \mathrm{e}^{\alpha t} \frac{1}{2} \left[\mathrm{e}^{i\beta t} + \mathrm{e}^{-i\beta t}\right]$$

und

$$t^j \mathrm{e}^{\alpha t} \sin(\beta t) = t^j \mathrm{e}^{\alpha t} \frac{1}{2i} \left[\mathrm{e}^{i\beta t} - \mathrm{e}^{-i\beta t}\right].$$

Es ist dann nicht schwierig zu zeigen, dass die Funktionen, die man auf diese Weise bilden kann, eine Basis des (reellen) Lösungsraumes bilden:

Satz 9.6 *Sei $\mathbb{K} = \mathbb{R}$. Wir nehmen an, dass das charakteristische Polynom von A r reelle Eigenwerte $\lambda_1, \ldots, \lambda_r$ hat mit algebraischen Vielfachheiten $m_1, \ldots, m_r$ und $2s$ komplexe $\lambda_{r+1} = \alpha_1 + i\beta_1, \ldots, \lambda_{r+s} = \alpha_s + i\beta_s$, $\lambda_{r+s+1} = \overline{\lambda}_{r+1}, \ldots, \lambda_{r+2s} = \overline{\lambda}_{r+s}$, mit algebraischen Vielfachheiten $n_1, \ldots, n_s$. (Die zweite Hälfte hat dieselben algebraischen Vielfachheiten). Dann bilden die Funktionen*

$$t^j \mathrm{e}^{\lambda_k t},\ 0 \leq j < m_j,\ 1 \leq k \leq r,$$

$$t^j \mathrm{e}^{\alpha_k t} \cos(\beta_k t),\ t^j \mathrm{e}^{\alpha_k t} \sin(\beta_k t),\ 0 \leq j < m_j,\ 1 \leq k \leq s,$$

eine Basis von L.

10 Bilinearformen und Isometrien

Wir setzen in diesem Kapitel generell voraus, dass $\operatorname{char} K \neq 2$ ist und dass V endlichdimensional ist (obwohl wir das nicht überall wirklich brauchen würden).

10.1 Spezielle Typen von Bilinearformen, Gramsche Matrix

Wir erinnern an die Definition der Multilinearformen aus Kapitel 5.2. Sei V ein K-Vektorraum. Eine k-Linearform ist eine Abbildung $\varphi : V^k \to K$, die linear in jedem Argument ist. Wie wir gesehen hatten, ist die Menge der k-linearen Formen in natürlicher Weise ein K-Vektorraum. Der Raum der 1-Linearformen, kurz der Linearformen, ist einfach der Dualraum V^*. Wir diskutieren in diesem Kapitel fast ausschliesslich den Fall $k = 2$, und bezeichnen die Formen dann als Bilinearformen. Wie in Kapitel 5 bezeichnen wir den Vektorraum der Bilinearformen mit $M_2(V)$.

Sind $f, g \in V^*$, so können wir das sogenannte Tensorprodukt von f und g, $f \otimes g \in M_2(V)$ wie folgt definieren:

$$(f \otimes g)(u, v) = f(u)\, g(v).$$

Man prüft sofort nach, dass das eine Bilinearform ist.

Bemerkung 10.1 *$M_2(V)$ ist ein Beispiel eines Tensorproduktes von zwei Vektorräumen, nämlich von V^* mit sich selbst. Man schreibt daher auch $V^* \otimes V^*$ für $M_2(V)$.*

Eine Bilinear- (und allgemeiner Multilinear-)Form ist eindeutig durch ihre Werte auf einer Basis festgelegt: Ist $\varphi \in M_2(V)$ und ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V, so gilt für Vektoren $v, w \in V$, $v = \sum_{i=1}^n x_i v_i$, $w = \sum_{j=1}^n y_j v_j$:

$$\varphi(v, w) = \sum_{i,j=1}^{n} x_i y_j \varphi(v_i, v_j). \tag{10.1}$$

Definition 10.1 *Ist $\varphi \in M_2(V)$ und ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V, so heisst die Matrix*

$$G = (\varphi(v_i, v_j))_{1 \leq i,j \leq n}$$

*die **Grammatrix** von φ bezüglich der Basis $\mathcal{V}$.*

Wir haben also gesehen, dass eine Basis von V und die Grammatrix die Bilinearform φ eindeutig festlegen. Umgekehrt definiert für jede $n \times n$-Matrix $G = (g_{ij})$ und für jede Basis $\mathcal{V} = (v_1, \ldots, v_n)$ die durch

$$\varphi\left(\sum\nolimits_{i=1}^n x_i v_i, \sum\nolimits_{j=1}^n y_j v_j\right) = \sum_{i,j=1}^{n} x_i y_j g_{ij}$$

definierte Abbildung $V \times V \to K$ eine Bilinearform auf V. Somit werden, analog wie bei den linearen Abbildungen, Bilinearformen durch Matrizen beschrieben, wobei die Zuordnung von der gewählten Basis abhängt.

Schreiben wir die Koordinatenvektoren (wie üblich) als Spaltenvektoren, so lässt sich das in kompakter Weise wie folgt schreiben:

$$\varphi(v, w) = x^T G y,$$

wobei x der Koordinatenvektor von v und y der Koordinatenvektor von w ist.

Wir untersuchen nun, wie sich die Grammatrix transformiert, wenn man die Basis wechselt: Sei $\mathcal{W} = (w_1, \ldots, w_n)$ eine zweite („neue“) Basis, mit Matrix der Basistransformation $S = (s_{ij})$:

$$w_j = \sum_i s_{ij} v_i.$$

Dann berechnet sich die Grammatrix G' derselben Bilinearform φ bezüglich der neuen Basis als

$$\begin{aligned} g'_{ij} = \varphi(w_i, w_j) &= \varphi\left(\textstyle\sum_k s_{ki} v_k, \sum_l s_{lj} v_l\right) \\ &= \sum_{k,l} s_{ki}\, s_{lj}\, \varphi(v_k, v_l) = \sum_{k,l} s_{ki}\, s_{lj}\, g_{kl}. \end{aligned}$$

Somit haben wir das folgende Resultat bewiesen:

Satz 10.1 *Sei φ eine Bilinearform, G die Grammatrix bezüglich einer Basis $\mathcal{V}$ und G' die Grammatrix bezüglich einer Basis $\mathcal{W}$. Sei S die Matrix der Basistransformation, die $\mathcal{W}$ durch $\mathcal{V}$ darstellt. Dann gilt*

$$G' = S^T G S.$$

Korollar 10.1 *Der Rang der Grammatrix wird durch die Bilinearform φ festgelegt und hängt nicht von der speziellen Basis ab.*

Beweis. Es gilt für jede reguläre Matrix S und für jede quadratische Matrix G : $\operatorname{rang}\left(S^T G S\right) = \operatorname{rang} G$. ■

Als nächstes wollen wir eine Basis von $M_2(V)$ bestimmen. Wir erinnern daran, dass zu einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$ von V die Dualbasis $(f_1, \ldots, f_n)$ in V^* eindeutig durch die Festlegung

$$f_i(v_j) = \delta_{ij}$$

definiert ist.

Lemma 10.1 *Sei $v_1, \ldots, v_n$ eine Basis von V und $f_1, \ldots, f_n$ die zugehörige Dualbasis von V^*. Dann ist $(f_i \otimes f_j)_{1 \le i,j \le n}$ eine Basis von $M_2(V)$.*

Beweis. Wir zeigen zunächst die lineare Unabhängigkeit. Sind $\alpha_{ij} \in K$ mit $\sum_{ij} \alpha_{ij} (f_i \otimes f_j) = 0$ (als Element von $M_2(V)$), so folgt für alle $1 \leq k, l \leq n$:

$$\begin{aligned} 0 &= \left(\sum\nolimits_{i,j} \alpha_{ij} (f_i \otimes f_j)\right)(v_k, v_l) = \sum\nolimits_{i,j} \alpha_{ij} (f_i \otimes f_j)(v_k, v_l) \\ &= \sum\nolimits_{i,j} \alpha_{ij} f_i(v_k) f_j(v_l) = \alpha_{kl}. \end{aligned}$$

Wir zeigen nun noch, dass $L\left[(f_i \otimes f_j)_{1 \leq i,j \leq n}\right] = M_2(V)$ gilt. Sei $\psi \in M_2(V)$ beliebig. Dann gilt

$$\psi = \sum\nolimits_{i,j} \psi(v_i, v_j)\ f_i \otimes f_j.$$

Um dies nachzuweisen, müssen wir wegen der Bilinearität nur nachprüfen, dass die Gleichung gilt, wenn wir links und rechts beliebige Paare (v_k, v_l) einsetzen:

$$\begin{aligned} \left(\sum\nolimits_{i,j} \psi(v_i, v_j)\ f_i \otimes f_j\right)(v_k, v_l) &= \sum\nolimits_{i,j} \psi(v_i, v_j)\ (f_i \otimes f_j)(v_k, v_l) \\ &= \psi(v_k, v_l). \end{aligned}$$

Damit ist das Lemma bewiesen. ■

Korollar 10.2 *Ist* $\dim(V) = n$, *so ist* $\dim(M_2(V)) = n^2$.

Eine wichtige Rolle spielen Bilinearformen, die spezielle Eigenschaften haben:

Definition 10.2 *Eine Bilinearform* $\varphi \in M_2(V)$ *heisst* ***symmetrisch,*** *wenn* $\varphi(u, v) = \varphi(v, u)$ *für alle* $u, v \in V$ *gilt. Sie heisst* ***antisymmetrisch, alternierend, oder symplektisch*** *(alle diese Begriffe sind gleichbedeutend), wenn* $\varphi(u, v) = -\varphi(v, u)$ *für alle* $u, v \in V$ *gilt.*

Wir hatten schon in Kapitel 5.2 gesehen, dass die Menge der symmetrischen Bilinearformen ein Unterraum von $M_2(V)$ ist. Das gleiche gilt für die Menge der antisymmetrischen Bilinearformen.

Bemerkung 10.2 *Offensichtlich ist eine Bilinearform genau dann symmetrisch, wenn die Grammatrix (bezüglich einer beliebigen Basis) symmetrisch ist, und symplektisch genau dann, wenn die Grammatrix schiefsymmetisch ist, d.h. dass* $G^T = -G$ *gilt.*

Beispiel 10.1 *a) Auf* $\mathbb{R}^n$ *ist das übliche Skalarprodukt*

$$(x, y) \to \sum_{i=1}^{n} x_i y_i$$

eine symmetrische Bilinearform.

b) Von besonderer Bedeutung in der Physik ist die folgende Bilinearform auf dem vierdimensionalen Raum $\mathbb{R}^4$. Wir schreiben die Vektoren von $\mathbb{R}^4$ als $(x,t) = (x_1,x_2,x_3,t)$, d.h. als „Raum-Zeit-Vektoren". Wir definieren

$$\varphi\left((x,t),(y,s)\right) := \sum_{i=1}^{3} x_i y_i - c^2 ts,$$

wobei c eine Konstante, die Lichtgeschwindigkeit ist. $\mathbb{R}^4$ versehen mit dieser Bilinearform nennt man den Minkowski-Raum. (c spielt natürlich mathematisch gar keine Rolle: Man könnte genau so gut auch $c = 1$ nehmen.)

c) Eine einfache symplektische Bilinearform auf $\mathbb{R}^2$ ist

$$(x,y) \to x_1 y_2 - x_2 y_1 = \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}.$$

Die obigen Definitionen gelten in Vektorräumen über beliebigen Körpern. Für komplexe Vektorräume betrachtet man oft eine Modifikation:

Definition 10.3 *Sei V ein $\mathbb{C}$-Vektorraum. Eine Abbildung $\varphi : V \times V \to \mathbb{C}$ heisst* ***Sesquilinearform,*** *wenn sie die beiden folgenden Bedingungen erfüllt:*

a) φ ist linear im ersten Argument:

$$\varphi\left(\alpha u + \beta v, w\right) = \alpha\varphi\left(u,w\right) + \beta\varphi\left(v,w\right),\ \forall \alpha,\beta \in \mathbb{C},\ \forall u,v,w \in V,$$

b) φ ist „konjugiert linear" im zweiten Argument:

$$\varphi\left(w, \alpha u + \beta v\right) = \overline{\alpha}\varphi\left(w,u\right) + \overline{\beta}\varphi\left(w,v\right),\ \forall \alpha,\beta \in \mathbb{C},\ \forall u,v,w \in V.$$

Die Sesquilinearform heisst ***Hermitesch*** *wenn*

$$\varphi\left(u,v\right) = \overline{\varphi\left(v,u\right)},\ \forall u,v \in V$$

gilt. Eine Hermitesche Sesquilinearform bezeichnen wir auch einfach als Hermitesche Form.

Das Standardbeispiel einer Hermiteschen Form in $\mathbb{C}^n$ ist

$$\varphi\left(x,y\right) = \sum_{j=1}^{n} x_i \overline{y_i}.$$

Man beachte, dass für eine Hermitesche Form stets $\varphi\left(v,v\right) \in \mathbb{R}$ gilt (wegen $\varphi\left(v,v\right) = \overline{\varphi\left(v,v\right)}$), obwohl natürlich i.allg. $\varphi\left(u,v\right)$ komplexe Werte annimmt.

Wir können natürlich auch für Sesquilinearformen die Grammatrix definieren: Ist $\mathcal{V} = (v_1,\ldots,v_n)$ eine Basis im komplexen Vektorraum V, so setzen wir

$$g_{ij} := \varphi\left(v_i,v_j\right).$$

Ist $v = \sum_i x_i v_i$, $w = \sum_i y_i v_i$, so gilt dann

$$\varphi(v,w) = \sum\nolimits_{i,j} g_{ij}\, x_i\, \overline{y_j},$$

oder in Kurzschreibweise

$$\varphi(v,w) = x^T G \overline{y}.$$

Offensichtlich ist eine Sesquilinearform genau dann Hermitesch, wenn

$$G^T = \overline{G} \tag{10.2}$$

gilt.

Definition 10.4 *Eine komplexe quadratische Matrix, die (10.2) erfüllt, heisst* ***Hermitesche Matrix.***

10.2 Normalformen

Wir betrachten in diesem Abschnitt Bilinearformen φ, wobei wir jedoch voraussetzen, dass φ entweder symmetrisch oder symplektisch ist. Im Falle $K = \mathbb{C}$ werden wir auch Hermitesche Formen zulassen. Die für uns in diesem Kapitel wichtige Voraussetzung ist, dass $\varphi(u,v) = 0$ genau dann wenn $\varphi(v,u) = 0$ gilt. Dies ist im allgemeinen für Bilinearformen nicht richtig, gilt jedoch offensichtlich für symmetrische und auch für symplektische Formen und natürlich auch für Hermitesche Formen. Wir definieren

$$\ker\varphi := \{v \in V : \varphi(v,w) = 0 \quad \forall w \in V\}.$$

Definition 10.5 *φ heisst* ***nichtdegeneriert,*** *wenn $\ker\varphi = \{0\}$ ist. Sonst heisst φ* ***degeneriert****.*

Hat V die Dimension 1, so ist eine Bilinearform φ natürlich genau dann nichtdegeneriert, wenn sie nicht die Nullform ist. Ist φ nicht die Nullform, so ist in diesem einfachen Fall $\varphi(v,w) \neq 0$ falls beide Vektoren $\neq 0$ sind. Ist $\dim(V) \geq 2$, so gibt es jedoch auch für nichtdegenerierte Formen „viele“ Paare von Vektoren, für die $\varphi(v,w) = 0$ ist.

Lemma 10.2 *Sei $\mathcal{V} = (v_1, \ldots, v_n)$ eine beliebige Basis in V. Dann ist φ genau dann nichtdegeneriert, wenn die Grammatrix regulär ist.*

Beweis. Offensichtlich ist

$$\ker\varphi = \{v \in V : \varphi(v, v_i) = 0 \quad \forall i\}.$$

Somit ist $v = \sum_j x_j v_j$ genau dann im Kern, wenn das homogene Gleichungssystem

$$\sum\nolimits_j x_j\, \varphi(v_j, v_i) = \sum\nolimits_j x_j\, g_{ji} = 0 \quad \forall i$$

erfüllt ist. Dieses Gleichungssystem hat genau dann nur die triviale Lösung, wenn G regulär ist. ■

Ist φ eine Bilinearform und U ein Unterraum von V, so können wir φ sehr einfach auf U einschränken: Wir definieren $\varphi_U : U \times U \to K$ durch $\varphi_U(u_1, u_2) := \varphi(u_1, u_2)$ für $u_1, u_2 \in U$. Offensichtlich ist φ_U eine Bilinearform auf U.

Beispiel 10.2 *a) Wir betrachten auf K^2 die Bilinearform $\varphi(x, y) := x_1y_2 - x_2y_1$. Diese Bilinearform ist natürlich nichtdegeneriert, denn die Grammatrix ist $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Man beachte, dass stets $\varphi(x, x) = 0$ gilt. Die Einschränkung von φ auf jeden eindimensionalen Unterraum von K^2 ist also die Nullform. Die Einschränkung einer nichtdegenerierten Bilinearform kann also durchaus degeneriert sein.*

b) Auch symmetrische nichtdegenerierte Bilinearformen können nichttriviale Unterräume haben, auf denen die Bilinearform degeneriert ist. Betrachte z.B. wieder auf K^2 $\varphi(x, y) := x_1y_1 - x_2y_2$. Hier ist die Einschränkung von φ auf den eindimensionalen Unterraum, der aufgespannt wird durch $(1, 1)$, die Nullform. Dasselbe gilt für den Unterraum, der von $(1, -1)$ aufgespannt wird.

Wir nennen einen Unterraum $U \subset V$ **nichtdegeneriert** (bezüglich einer Bilinearform φ), wenn φ_U nichtdegeneriert ist. Wie wir in den Beispielen oben gesehen haben, können nichtdegenerierte Bilinearformen durchaus nichttriviale degenerierte Unterräume haben.

Für einen Unterraum U definieren wir das **Komplement** von U bezüglich φ durch

$$U^\perp := \{v \in V : \varphi(v, u) = 0 \quad \forall u \in U\}.$$

Da wir vorausgesetzt haben, dass $\varphi(v, u) = 0$ genau dann gilt, wenn $\varphi(u, v) = 0$ ist, spielt es keine Rolle, in welcher Reihenfolge u und v in der obigen Definition von $U^\perp$ stehen. Hat φ diese Eigenschaft nicht, muss man zwischen zwei Komplementen unterscheiden und die nachfolgende Diskussion würde ein gutes Stück umständlicher.

Lemma 10.3 *a) $U^\perp$ ist ein Unterraum von V.*

b) Ist U nichtdegeneriert, so gilt $V = U \oplus U^\perp$.

c) Sind U und $U^\perp$ nichtdegeneriert, so gilt $\left(U^\perp\right)^\perp = U$.

Beweis. a) ist sehr einfach und soll dem Leser überlassen sein.

b) Der Beweis spaltet sich in zwei Teile. Wir zeigen zunächst, dass $U \cap U^\perp = \{0\}$ gilt. Sei $v \in U \cap U^\perp$. Wegen $v \in U^\perp$ folgt $\varphi(v, w) = 0$ für alle $w \in U$. Da v auch in U ist folgt $v \in \ker(\varphi_U)$. Daraus folgt $v = 0$ wegen der Voraussetzung, dass U nichtdegeneriert ist. Wir haben somit gezeigt, dass

$$U + U^\perp = U \oplus U^\perp$$

gilt.

Wir müssen nun noch zeigen, dass $U + U^\perp = V$ ist. Dazu reicht es aus, nachzuweisen, dass

$$\dim(U) + \dim\left(U^\perp\right) \geq \dim(V)$$

gilt. Sei $v_1, \ldots, v_m$ eine Basis von U. Wir ergänzen das zu einer Basis in V durch $v_{m+1}, \ldots, v_n$. Dann ist $v = \sum_{j=1}^n x_j v_j$ genau dann in $U^\perp$, wenn $\varphi(v, u) = 0$ für alle $u \in U$ ist, d.h. dass $\varphi(v, v_i) = 0$ für $i = 1, \ldots, m$ ist. Dies ist aber gleichbedeutend damit, dass

$$\sum_{j=1}^n x_j \varphi(v_j, v_i) = 0,\ i = 1, \ldots, m$$

gilt. Das ist ein homogenes lineares Gleichungssystem mit m Gleichungen und n Unbekannten. Deshalb ist die Dimension des Lösungsraumes mindestens $n - m$. Somit gilt $\dim\left(U^\perp\right) \geq n - m = \dim(V) - \dim(U)$.

c) folgt nun sehr einfach: Sind U und $U^\perp$ nichtdegeneriert, so gilt

$$V = U \oplus U^\perp \text{ und } V = U^\perp \oplus \left(U^\perp\right)^\perp.$$

Daraus folgt $\dim U = \dim\left(U^\perp\right)^\perp$. Andererseits ist jedoch $U \subset \left(U^\perp\right)^\perp$, denn für $u \in U$ gilt $\varphi(u, v) = 0$ für alle $v \in U^\perp$. Somit folgt $U = \left(U^\perp\right)^\perp$. ■

Definition 10.6 *φ sei eine Bilinearform auf V. Zwei Unterräume U_1, U_2 heissen **orthogonal** bezüglich φ, wenn $\varphi(u_1, u_2) = 0$ für alle $u_1 \in U_1$ und alle $u_2 \in U_2$ ist.*

Wir diskutieren als nächstes das Normalformenproblem für Bilinearformen. Es geht dabei darum, eine Basis zu finden, bezüglich der eine Bilinearform eine besonders einfache Grammatrix hat. Wir diskutieren die drei Fälle von symmetrischen, symplektischen und Hermiteschen Formen separat. Zunächst der symmetrische Fall.

Satz 10.2 *Sei φ eine symmetrische Bilinearform auf einem endlichdimensionalen Vektorraum V. Sei ferner $n = \dim V$ und $l = \dim(\ker\varphi)$. Dann existieren $m := n - l$ eindimensionale nichtdegenerierte Unterräume $U_1, \ldots, U_m$, die paarweise orthogonal sind, sodass*

$$V = U_1 \oplus U_2 \oplus \ldots \oplus U_m \oplus \ker\varphi$$

gilt.

Bevor wir den Satz beweisen, soll zunächst bemerkt werden, dass wir damit auch eine Basis gefunden haben, bezüglich der die Grammatrix eine sehr einfache

Gestalt hat. Wählen wir nämlich Vektoren $v_i \in U_i$, $v_i \neq 0$, $1 \leq i \leq m$, und eine Basis $v_{m+1}, \ldots, v_n$ in $\ker \varphi$, so ist $v_1, \ldots, v_n$ eine Basis in V. Andererseits gilt $\varphi(v_i, v_j) = 0$ falls $i \neq j$ ist, und $\varphi(v_i, v_i) = 0$ für $i \geq m+1$, da die Vektoren $v_{m+1}, \ldots, v_n$ im Kern sind. Für $i \leq m$ gilt jedoch $\alpha_i := \varphi(v_i, v_i) \neq 0$. Damit folgt aus dem obigen Satz das folgende

Korollar 10.3 *Unter den gleichen Voraussetzungen an φ wie oben existiert eine Basis von V, bezüglich der die Grammatrix die folgende Gestalt hat*

$$\begin{pmatrix} \alpha_1 & 0 & \cdots & & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & & 0 \\ \vdots & & \ddots & & & \vdots \\ & & & \alpha_m & & \\ 0 & & & & 0 & \vdots \\ 0 & \cdots & & & \cdots & 0 \end{pmatrix}.$$

Vorsicht: Die α_i brauchen nichts mit irgendwelchen Eigenwerten zu tun zu haben.

Beweis von Satz 10.2. Wir führen eine Induktion nach $n = \dim V$ durch. $n = 1$ ist trivial.

Wir setzen also $n \geq 2$ voraus. Ist $\ker \varphi = V$, so ist ebenfalls nichts mehr zu zeigen. Wir setzen also voraus, dass $\ker \varphi \neq V$ gilt. Dann existieren Vektoren $v, w \in V$ mit $\varphi(v, w) \neq 0$. Wegen der Symmetrie und $\operatorname{char} K \neq 2$ folgt

$$\varphi(v+w, v+w) - \varphi(v, v) - \varphi(w, w) = 2\varphi(v, w) \neq 0.$$

Daraus folgt, dass ein $x \in V$ existiert mit $\varphi(x, x) \neq 0$. Dann ist der Unterraum

$$U_1 := L[x]$$

nichtdegeneriert. Nach Lemma 10.3 folgt

$$V = U_1 \oplus V'$$

mit $V' := U_1^{\perp}$. φ' sei die Einschränkung von φ auf V'.

Wir zeigen zunächst

$$\ker \varphi = \ker \varphi'. \tag{10.3}$$

Jeder Vektor $v \in V$ hat eine eindeutige Darstellung $v = \alpha x + v'$ mit $\alpha \in K$ und $v' \in V'$. Dann gilt

$$\begin{aligned} \varphi(v, x) &= \varphi(\alpha x + v', x) = \alpha\varphi(x, x) + \varphi(v', x) \\ &= \alpha\varphi(x, x) \text{ wegen } v' \in U_1^{\perp}. \end{aligned}$$

$\varphi(x,x)$ ist $\neq 0$. Demzufolge folgt aus $v \in \ker\varphi$ dass $\alpha = 0$ ist, d.h. $v \in V'$. Wir haben also

$$\ker\varphi \subset V' = U_1^\perp$$

gezeigt. Somit gilt:

$$\begin{aligned} v \in \ker\varphi &\iff v \in U_1^\perp \text{ und } \varphi(v, \alpha x + v') = 0 \ \forall \alpha \in K,\ v' \in U_1^\perp \\ &\iff v \in U_1^\perp \text{ und } \varphi(v, v') = 0 \ \forall v' \in U_1^\perp \\ &\iff v \in U_1^\perp \text{ und } v \in \ker(\varphi') \iff v \in \ker\varphi'. \end{aligned}$$

Damit ist (10.3) gezeigt.

Wir können nun die Induktionsvoraussetzung auf V' anwenden und erhalten die Zerlegung

$$V' = U_2 \oplus \ldots \oplus U_m \oplus \ker\varphi' = U_2 \oplus \ldots \oplus U_m \oplus \ker\varphi,$$

wobei $U_2, \ldots, U_m$ eindimensionale nichtdegenerierte Unterräume von φ' sind. Nun ist jedoch offensichtlich jeder nichtdegenerierte Unterraum $U' \subset V'$ von φ' auch ein nichtdegenerierter Unterraum von φ. Somit sind $U_2, \ldots, U_m$ eindimensionale nichtdegenerierte Unterräume $\subset V$ von φ und es gilt

$$V = U_1 \oplus U_2 \oplus \ldots \oplus U_m \oplus \ker\varphi.$$

■

Eine weitere Vereinfachung gibt es im Spezialfall $K = \mathbb{C}$ (oder in jedem Körper, in dem man stets Quadratwurzeln ziehen kann): Ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis mit $\varphi(v_i, v_j) = \alpha_i \delta_{ij}$, $\alpha_i = 0$ für $i > m$, $\alpha_i \neq 0$ für $i \leq m$, so definieren wir $v_i' := v_i/\beta_i$, mit $\beta_i^2 = \alpha_i$ für $i \leq m$ und $v_i' := v_i$ für $i > m$. Dann gilt $\varphi(v_i', v_j') = \delta_{ij}$ für $i \leq m$ und $\varphi(v_i', v_j') = 0$ sonst. Wir haben also den folgenden Satz bewiesen:

Satz 10.3 *Sei $K = \mathbb{C}$ und φ sei eine symmetrische Bilinearform. Dann existiert eine Basis, bezüglich der die Grammatrix die folgende Gestalt hat:*

$$\begin{pmatrix} E_m & 0 \\ 0 & 0_{n-m} \end{pmatrix}$$

(0_{n-m} bezeichnet die $(n-m)\times(n-m)$-Nullmatrix). m ist eindeutig durch φ bestimmt, hängt nicht von der speziellen Basis ab und ist durch $m = n - \dim(\ker\varphi)$ gegeben.

Beweis. Die Existenz einer derartigen Basis haben wir schon gezeigt. Dass m eindeutig ist, folgt einfach daraus, dass der Rang einer Grammatrix eindeutig durch die Bilinearform gegeben ist (Korollar 10.1). ■

Es sollte jedoch bemerkt werden, dass für $K = \mathbb{C}$ symmetrische Bilinearformen nicht sehr wichtig sind. Wesentlich wichtiger sind Hermitesche Formen. Wir bleiben jedoch zunächst beim symmetrischen Fall und diskutieren die besonders wichtige Situation für $K = \mathbb{R}$. In diesem Fall können wir nur aus positiven Körperelementen Wurzeln ziehen. Wir verfahren deshalb wie bei $K = \mathbb{C}$ mit der kleinen Modifikation, dass wir $v_i' = v_i/\sqrt{\alpha_i}$ nur für die i mit $\alpha_i > 0$ setzen. Für diese i gilt dann nach wie vor $\varphi(v_i', v_i') = 1$. Für $\alpha_i < 0$ setzen wir $v_i' := v_i/\sqrt{-\alpha_i}$. Dann ist offenbar $\varphi(v_i', v_i') = -1$.

Satz 10.4 (Trägheitssatz von Sylvester) *Sei $K = \mathbb{R}$ und φ sei eine symmetrische Bilinearform. Dann existiert eine Basis $\mathcal{V} = (v_1, \ldots, v_{n_+}, v_{n_+1}, \ldots, v_{n_+n_-}, \ldots, v_{n_+n_-n_0})$ $(n = n_+ + n_- + n_0)$, bezüglich der die Grammatrix die folgende Gestalt hat:*

$$\begin{pmatrix} E_{n_+} & 0 & 0 \\ 0 & -E_{n_-} & 0 \\ 0 & 0 & 0_{n_0} \end{pmatrix}. \tag{10.4}$$

(n_+, n_-, n_0) ist dabei eindeutig durch φ festgelegt.

Definition 10.7 *Das Tripel (n_+, n_-, n_0) heisst die **Signatur** der symmetrischen Bilinearform. Eine reelle symmetrische Bilinearform mit $n_+ = \dim V$ (d.h. $n_- = n_0 = 0$) heisst **positiv definit**.*

Beweis des Trägheitssatzes. Die Existenz haben wir schon bewiesen. Wir müssen noch zeigen, dass die Signatur nicht von der speziellen Basis abhängt. Seien $\mathcal{V} = (v_1, \ldots, v_n)$ und $\mathcal{V}' = (v_1', \ldots, v_n')$ zwei Basen bezüglich denen die Grammatrix die obige Form hat mit Signaturen (n_+, n_-, n_0) bzw. $\left(n_+', n_-', n_0'\right)$. Der Rang der Grammatrix ist wegen Korollar 10.1 durch die Bilinearform festgelegt, und somit gilt $n_0 = n_0'$. Seien

$$V_+ := L\left[v_1, \ldots, v_{n_+}\right],\ V_- := L\left[v_{n_+1}, \ldots, v_{n_+n_-}\right],$$

und analog V_+', V_-'. Man beachte, dass die letzten n_0 Vektoren beider Basen auf jeden Fall $\ker\varphi$ aufspannen: In der Tat gilt $v = \sum_{j=1}^n \alpha_j v_j \in \ker\varphi$ genau dann, wenn $\varphi(v, v_i) = 0$ für alle i gilt, d.h. genau dann, wenn $\alpha_i = 0$ für $i \le n_+ + n_-$ ist. D.h. $\ker\varphi = L\left[v_{n_+n_-+1}, \ldots, v_n\right]$. Gleiches gilt natürlich für die zweite Basis.

Nun gilt

$$V = V_+ \oplus V_- \oplus \ker\varphi = V_+' \oplus V_-' \oplus \ker\varphi.$$

Wenn wir annehmen, dass $n_+ > n_+'$ gilt, so folgt

$$\dim V_+ + \dim\left(V_-' \oplus \ker\varphi\right) > n.$$

Daraus folgt

$$V_+ \cap \left(V_-' \oplus \ker\varphi\right) \neq \{0\}.$$

Ist $x \in V_+ \cap \left(V'_- \oplus \ker\varphi\right)$, $x \neq 0$, so gilt einerseits $\varphi(x,x) > 0$ wegen $x \in V_+$, $x \neq 0$ und andererseits $\varphi(x,x) \leq 0$ wegen $x \in V'_- \oplus \ker\varphi$. Dies ist offenbar nicht möglich, und wir können daher schliessen, dass $n_+ > n'_+$ nicht möglich ist. Analog schliesst man $n'_+ > n_+$ aus. Daraus folgt $n_+ = n'_+$, woraus auch $n_- = n'_-$ folgt. ■

Die vorangegangenen Sätze kann man auch in Matrizensprache ausdrücken: Sei G eine symmetrische Matrix. Dann existiert eine reguläre Matrix S, sodass S^TGS eine Diagonalmatrix ist. Ist $K = \mathbb{C}$, so kann man S so wählen, dass in der Diagonalen nur Nullen und Einsen stehen. Im Fall $K = \mathbb{R}$ kann man S so wählen, dass in der Diagonalen nur ± 1 oder 0 vorkommt. Die Anzahlen von $+1$, -1 und 0 sind dabei durch G festgelegt.

Wir diskutieren als nächstes den besonders wichtigen Fall, wo $K = \mathbb{C}$ und φ eine Hermitesche Form ist.

Satz 10.5 *Sei $K = \mathbb{C}$ und φ eine Hermitesche Sesquilinearform. Dann existiert eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$, bezüglich der die Grammatrix von der Form (10.4) ist. (n_+, n_-, n_0) ist dabei eindeutig durch φ festgelegt.*

Definition 10.8 *Das Tripel (n_+, n_-, n_0) heisst die **Signatur** der Hermiteschen Form. Eine Hermitesche Form mit $n_+ = \dim V$ (d.h. $n_- = n_0 = 0$) heisst **positiv definit**.*

Beweis von Satz 10.5. Der Beweis geht völlig analog zu den entsprechenden Sätzen 10.2 und 10.4. Ein Punkt im Beweis von Satz 10.2 erfordert jedoch eine etwas genauere Überlegung: Wir hatten dort verwendet, dass für eine symmetrische Bilinearform φ mit $\varphi \neq 0$, ein Vektor v existiert mit $\varphi(v,v) \neq 0$. Wir zeigen nun die gleiche Aussage im Hermiteschen Fall:

Wir zeigen, dass aus $\varphi(v,v) = 0\ \forall v$ folgt, dass $\varphi = 0$ ist, d.h. dass $\varphi(u,v) = 0$ für alle $v, v \in V$ gilt. Zunächst folgt für beliebige u, v :

$$\begin{aligned} 0 &= \varphi(u+v, u+v) = \varphi(u,u) + \varphi(u,v) + \varphi(v,u) + \varphi(v,v) \\ &= \varphi(u,v) + \varphi(v,u) = \varphi(u,v) + \overline{\varphi(u,v)}. \end{aligned}$$

Daraus folgt, dass $\varphi(u,v)$ für beliebige $u, v \in V$ stets rein imaginär ist. Somit folgt, dass für beliebige u, v auch $\varphi(iu, v) = i\varphi(u,v)$ rein imaginär ist, wobei jedoch auch $\varphi(u,v)$ rein imaginär ist. Dies geht jedoch nur, wenn $\varphi(u,v) = 0$ für alle $u, v \in V$ ist.

Der Rest des Beweises von Satz 10.2 führt nun in einer trivialen Reformulierung sofort zur Aussage, dass eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$ existiert, bezüglich der die Grammatrix eine Diagonalmatrix ist: $G = (\alpha_i \delta_{ij})$. Die α_i sind dabei $\in \mathbb{R}$, da für eine Hermitesche Form stets $\varphi(v,v) \in \mathbb{R}$ gilt. Ersetzen wir die Basiselemente $v_i / \sqrt{|\alpha_i|}$ falls $\alpha_i \neq 0$ ist, so erhalten wir wie im Fall reeller symmetrischer Bilinearformen eine Grammatrix mit ± 1 und 0 in der Diagonalen. Das Argument im

Satz von Sylvester geht genau gleich durch und zeigt, dass die Anzahlen von ± 1 und 0 durch φ festgelegt sind. ■

Wir diskutieren zum Schluss den symplektischen Fall.

Satz 10.6 *Sei φ symplektisch. Ist $\varphi \neq 0$ so existieren 2-dimensionale, nichtdegenerierte, paarweise orthogonale Unterräume $U_1, \ldots, U_m$ ($2m \leq n = \dim V$) mit*

$$V = U_1 \oplus \ldots \oplus U_m \oplus \ker \varphi.$$

Beweis. Wir führen wiederum eine Induktion nach n durch. Ist $\dim V = 1$, so ist nichts zu zeigen, da dann $\varphi = 0$ sein muss (wegen $\varphi(v,v) = 0$ im symplektischen Fall). Ist $n \geq 2$ und $\varphi \neq 0$, so existieren Vektoren $u, v \in V$ mit $\varphi(u,v) \neq 0$. u, v müssen linear unabhängig sein. (Sind u, v linear abhängig, so folgt $\varphi(u,v) = 0$). Wir betrachten $U_1 := L[u,v]$ und setzen wieder $V' := U_1^{\perp}$. Dann gilt $V = U_1 \oplus V'$. Der Rest des Arguments ist wieder völlig analog zum Satz 10.2: Wir betrachten die Restriktion φ' von φ auf V' und wenden die Induktionsvoraussetzung auf φ' an. Natürlich muss man wieder zunächst zeigen, dass $\ker \varphi = \ker \varphi'$ ist. Wir überlassen die Details dem Leser. ■

Korollar 10.4 *Sei wieder φ symplektisch (und* $\operatorname{char} K \neq 2$*). Dann existiert eine Basis, bezüglich der die Grammatrix die folgende Gestalt hat:*

$$\begin{pmatrix}
\boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & 0 & \cdots & & \cdots & 0 \\
0 & \ddots & 0 & & & \vdots \\
\vdots & 0 & \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & 0 & & \\
 & & & 0 & & \\
\vdots & & & & \ddots & \vdots \\
0 & \cdots & & & \cdots & 0
\end{pmatrix}.$$

Beweis. Nach dem vorangegangen Satz existiert eine Basis

$$\mathcal{V} = (v_1, v_2, \ldots, v_{2m-1}, v_{2m}, v_{2m+1}, \ldots, v_n),$$

wobei v_1, v_2 eine Basis von U_1, v_3, v_4 eine Basis von U_2 etc., und $v_{2m+1}, \ldots, v_n$ eine Basis von $\ker \varphi$ ist. Setzen wir $\alpha_i := \varphi(v_{2i-1}, v_{2i}) \neq 0$, so gilt $\varphi\left(v_{2i}, v_{2i-1}\right) = -\alpha_i$. Damit hat die Grammatrix schon fast die obige Gestalt, nur dass die Zweierkästchen noch $\boxed{\begin{matrix} 0 & \alpha_i \\ -\alpha_i & 0 \end{matrix}}$ anstelle von $\boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}}$ sind. Wir ersetzen nun noch die Basis durch die Basis

$$\frac{v_1}{\alpha_1}, v_2, \frac{v_3}{\alpha_2}, v_4, \ldots, \frac{v_{2m-1}}{\alpha_m}, v_{2m}, v_{2m+1}, \ldots, v_n.$$

Dann ist die Grammatrix offenbar von der gewünschten Form. ■

Bemerkung 10.3 *Nach dem vorangegangenen Satz existieren nichtdegenerierte symplektische Formen nur auf Vektorräumen gerader Dimension.*

Im Gegensatz zu symplektischen Formen sind symmetrische und Hermitesche Formen durch ihre Werte auf der „Diagonalen“ eindeutig festgelegt:

Definition 10.9 *Sei φ eine symmetrische Bilinearform oder eine Hermitesche Form. Dann heisst die Abbildung $q : V \to K$ (bzw $V \to \mathbb{R}$), definiert durch $q(v) := \varphi(v, v)$, die zu φ gehörige* ***quadratische Form.*** *(Für eine Hermitesche Form ist $\varphi(v, v)$ stets reell).*

Satz 10.7 *Symmetrische Bilinearformen und Hermitesche Formen sind durch ihre zugehörigen quadratischen Formen eindeutig festgelegt.*

Beweis. Wir beweisen zunächst den symmetrischen Fall: Wegen

$$\varphi(u+v, u+v) = \varphi(u, u) + 2\varphi(u, v) + \varphi(v, v)$$

folgt

$$\varphi(u, v) = \frac{1}{2}\left[q(u+v) - q(v) - q(u)\right].$$

Der Hermitesche Fall ist leicht komplizierter; man rechnet jedoch sofort nach, dass

$$\varphi(u, v) = \frac{1}{2i}\left[-(1+i)\, q(u) - (1+i)\, q(v) + q(iu+v) + iq(u+v)\right]$$

gilt. ■

Wir diskutieren die Sache noch kurz in Koordinaten. Ist φ eine symmetrische Bilinearform und $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V, so stellt sich die Bilinearform in Koordinaten wie folgt dar: Sind $u, v \in V$ mit Koordinatenvektoren $x, y \in K^n$, so ist

$$\varphi(u, v) = \sum_{i,j=1}^{n} g_{ij} x_i y_j,$$

wobei $G = (g_{ij})$ die symmetrische Grammatrix ist. Natürlich ist die rechte Seite dieser Gleichung einfach eine symmetrische Bilinearform auf K^n. Die quadratische Form q ist in Koordinaten dann einfach durch

$$q(u) = \sum_{i,j=1}^{n} g_{ij} x_i x_j$$

gegeben. Die Sätze über Normalformen stellen sich in Koordinaten dann wie folgt dar: Zu jeder symmetrischen Bilinearform existiert eine Koordinatentransformation

$$x_i = \sum_{j=1}^{n} s_{ij} x'_j,$$

$S = (s_{ij})$ regulär, sodass

$$\sum_{i,j=1}^{n} g_{ij} x_i y_j = \sum_{i=1}^{n} \alpha_i x'_i y'_i$$

ist. Auf der Diagonalen gibt das einfach

$$\sum_{i,j=1}^{n} g_{ij} x_i x_j = \sum_{i=1}^{n} \alpha_i \left(x'_i\right)^2 .$$

Man beachte, dass S die Matrix ist, die die „alten" Koordinaten durch die „neuen" ausdrückt, d.h. die Matrix, die die neue Basis durch die alte via

$$v'_j = \sum_{i=1}^{n} s_{ij} v_i$$

bestimmt. Ist $K = \mathbb{C}$, so lässt sich S so wählen, dass alle α_i Null oder Eins sind. Im reellen Fall muss man auch -1 zulassen. Im Reellen lässt sich also jede quadratische Form als Differenz von Summen von Quadraten der Koordinaten schreiben:

$$q(v) = \varphi(v) = \sum_{i=1}^{n_+} x_i^2 - \sum_{i=n_+ +1}^{n_+ + n_-} x_i^2 \tag{10.5}$$

Im Spezialfall einer positiv definiten symmetrischen Bilinearform existiert eine Basis $\mathcal{V}$, bezüglich der die Grammatrix die Einheitsmatrix ist. Das bedeutet für die quadratische Form, dass

$$q(v) = \sum_{i=1}^{n} x_i^2 \tag{10.6}$$

ist.

Lemma 10.4 *Eine symmetrische reelle Bilinearform φ ist genau dann positiv definit, wenn $q(v) := \varphi(v, v) > 0$ für alle $v \neq 0$ ist.*

Beweis. Ist φ positiv definit, so existiert eine Basis, bezüglich der sich φ gemäss (10.6) darstellt. Daraus folgt $q(v) > 0$, falls $v \neq 0$ und damit der Koordinatenvektor $x \neq 0$ ist.

Ist φ nicht positiv definit, so hat man die Darstellung (10.5) mit $n_+ < n$. Dann existieren offensichtlich Vektoren $v \neq 0$ mit $q(v) \leq 0$. ∎

Der Hermitesche Fall geht wie üblich analog zum rellen symmetrischen Fall: In Koordinaten drückt sich eine Hermitesche Form durch

$$\varphi(u, v) = \sum_{i,j=1}^{n} g_{ij} x_i \overline{y_j}$$

aus, bzw. die quadratische Form durch

$$q(u) = \sum_{i,j=1}^{n} g_{ij} x_i \overline{x_j}.$$

Dabei ist G eine Hermitesche Matrix: $G^T = \overline{G}$. Durch eine geeignete Koordinatensubstitution $x_i = \sum_{j=1}^{n} s_{ij} x'_j$ lässt sich diese quadratische Form als Differenz von Summen von Quadraten der Absolutwerte der Koordinaten schreiben:

$$\sum_{i,j=1}^{n} g_{ij} x_i \overline{x_j} = \sum_{i=1}^{n_+} |x'_i|^2 - \sum_{i=n_++1}^{n_++n_-} |x'_i|^2 .$$

Für eine positiv definite Hermitesche Form existiert eine Basis $\mathcal{V}$, bezüglich der die Grammatrix die Einheitsmatrix ist. Das bedeutet für die quadratische Form, dass

$$q(v) = \sum_{i=1}^{n} |x_i|^2 \tag{10.7}$$

ist. Analog wie im reellen symmetrischen Fall zeigt man:

Lemma 10.5 *Eine Hermitesche Form φ ist genau dann positiv definit, wenn $q(v) := \varphi(v,v) > 0$ für alle $v \neq 0$ ist.*

10.3 Das Gram-Schmidtsche Orthogonalisierungsverfahren

Wir betrachten in diesem Abschnitt nur symmetrische Bilinearformen oder Hermitesche Formen.

Das im letzten Abschnitt vorgestellte Verfahren zur Orthogonalisierung ist nicht sehr konstruktiv, hat aber den Vorteil, dass es immer funktioniert. Wir stellen in diesem Abschnitt ein Verfahren vor, das „konstruktiver“ ist, das jedoch an eine Voraussetzung gebunden ist.

Definition 10.10 *φ sei eine symmetrische Bilinearform (oder eine Hermitesche Form). Ein Satz von Vektoren $v_1, \ldots, v_n$ heisst* ***orthogonal,*** *wenn $\varphi(v_i, v_j) = 0$ für $i \neq j$ gilt.*

Lemma 10.6 *Sind $v_1, \ldots, v_n$ orthogonal und gilt $\varphi(v_i, v_i) \neq 0$ für alle i, so sind diese Vektoren linear unabhängig.*

Beweis. Sei $\sum_{i=1}^{n} \alpha_i v_i = 0$. Dann folgt für $1 \leq k \leq n$:

$$0 = \varphi\left(v_k, \sum\nolimits_{i=1}^{n} \alpha_i v_i\right) = \alpha_k \varphi(v_k, v_k),$$

woraus sich $\alpha_k = 0$ für $1 \leq k \leq n$ ergibt. ■

Das Gram-Schmidtsche Orthogonalisierungsverfahren besteht nun darin, dass man eine beliebige Basis $\mathcal{V} = (v_1, \ldots, v_n)$ schrittweise orthogonalisiert. Wir müssen jedoch eine Voraussetzung an die Basis machen:

Bedingung 10.1 *Alle Unterräume $U_i := L[v_1, \ldots, v_i]$, $1 \leq i \leq n$, sind nichtdegeneriert.*

Die Bedingung besagt insbesondere, dass V selbst nichtdegeneriert ist, d.h. dass $\ker \varphi = \{0\}$ ist. Das ist jedoch nicht die entscheidende Einschränkung, denn man kann ja den Kern erst abspalten, wie wir das schon früher gemacht haben: $V = V' \oplus \ker \varphi$ und die Einschränkung von φ auf V' betrachten. Im allgemeinen gibt es jedoch auch im Fall, dass $\ker \varphi = \{0\}$ ist, durchaus degenerierte Unterräume, vgl. Beispiel 10.2 b).

Die obige Bedingung 10.1 ist stets erfüllt, wenn φ positiv definit ist: Nach Lemma 10.4 bzw. 10.5 ist dann stets $\varphi(v, v) > 0$ für $v \neq 0$, und deshalb ist in diesem Fall jeder nichttriviale Unterraum nichtdegeneriert.

Hier nun das Orthogonalisierungsverfahren: Wir starten mit einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$, die die Bedingung 10.1 erfüllt und konstruieren eine neue orthogonale Basis $\mathcal{U} = (u_1, \ldots, u_n)$ rekursiv. Sind $u_1, \ldots, u_{i-1}$ schon konstruiert, so bestimmen wir u_i so, dass die folgenden Eigenschaften gelten:

(i) $\varphi(u_i, u_i) \neq 0$.

(ii) $L[u_1, \ldots, u_i] = U_i$.

(iii) u_i ist orthogonal zu allen Vektoren in U_{i-1}.

(ii) kann man etwas anders formulieren: Er besagt, dass sich u_i der „neuen" Basis aus den ersten i Vektoren der alten Basis darstellen lässt. Dies ist gleichbedeutend damit, dass die Matrix S der Basistransformation von $\mathcal{V}$ nach $\mathcal{U}$ eine obere Dreiecksmatrix ist.

Wir beginnen mit $i = 1$ und setzen $u_1 := v_1$. Dann sind offenbar (i) und (ii) erfüllt und (iii) ist leer. Wir nehmen nun an, dass $i \geq 2$ ist und $u_1, \ldots, u_{i-1}$ schon konstruiert sind, wobei (i)-(iii) für Indizes $< i$ erfüllt sind. (Insbesondere sind $u_1, \ldots, u_{i-1}$ orthogonal). Wir bemerken zuerst, dass $u_1, \ldots, u_{i-1}, v_i$ linear unabhängig sind. Wenn (ii) erfüllt sein soll, können wir u_i in der folgenden Weise ansetzen:

$$u_i = \lambda_i v_i + \sum_{k=1}^{i-1} \lambda_k v_k, \ \lambda_k \in K. \tag{10.8}$$

Weil jedoch $L[u_1, \ldots, u_{i-1}] = U_{i-1}$ schon gilt, können wir $\sum_{k=1}^{i-1} \lambda_k v_k$ durch einen Ausdruck $\sum_{k=1}^{i-1} \alpha_k u_k$ ersetzen, und wir versuchen nun, die α's so zu bestimmen, dass (i)-(iii) erfüllt sind. Wir beachten zunächst, dass wir u_i noch mit einem beliebigen Faktor $\neq 0$ skalieren können, ohne dass das etwas an (i)-(iii) ändert.

Wir können deshalb $\lambda_i = 1$ ansetzen und bestimmen $\alpha_1, \ldots, \alpha_{i-1}$ so, dass

$$u_i = v_i + \sum_{k=1}^{i-1} \alpha_k u_k$$

die gewünschten Eigenschaften hat. Wir setzen das in die Orthogonalitätsbedingung (iii) ein: Es soll ja $\varphi(u_i, u_j) = 0$ für $j \leq i-1$ sein. Dies führt auf $i-1$ Gleichungen für die noch unbekannten α's:

$$\begin{aligned} 0 &= \varphi\left(v_i + \sum\nolimits_{k=1}^{i-1} \alpha_k u_k, u_j\right) = \varphi(v_i, u_j) + \sum_{k=1}^{i-1} \alpha_k \varphi(u_k, u_j) \\ &= \varphi(v_i, u_j) + \alpha_j \varphi(u_j, u_j), \ 1 \leq j \leq i-1. \end{aligned}$$

Nun beachten wir, dass wir (i) für Indizes $< i$ vorausgesetzt haben. Wir können die α's also nun einfach ausrechnen:

$$\alpha_j = -\frac{\varphi(v_i, u_j)}{\varphi(u_j, u_j)}, \ 1 \leq j \leq i-1.$$

Damit ist (iii) erfüllt, und wir haben nachgewiesen, dass mit dieser Wahl von u_i die u_k für $k \leq i$ orthogonal sind. Wir müssen nun noch die Eigenschaften (i) und (ii) nachweisen.

Beweis von (i): Zunächst bemerken wir, dass wegen der Unabhängigkeit von $u_1, \ldots, u_{i-1}, v_i$ der Vektor $u_i \neq 0$ ist. Wäre $\varphi(u_i, u_i) = 0$, so ist $\varphi(u_i, u_j) = 0$ für alle $j \leq i$. Damit folgt $\varphi(u_i, v) = 0$ für alle $v \in U_i$. Das bedeutet aber $u_i \in \ker(\varphi|_{U_i})$, d.h. der Unterraum U_i wäre degeneriert, was wir durch Bedingung 10.1 ausgeschlossen hatten.

Beweis von (ii): Da u_i eine Linearkombination von $u_1, \ldots, u_{i-1}$ und v_i ist, folgt $u_i \in L[u_1, \ldots, u_{i-1}, v_i] = U_i$. Daraus folgt $L[u_1, \ldots, u_i] \subset U_i$. Da sich jedoch auch v_i als Linearkombination von $u_1, \ldots, u_i$ darstellen lässt, folgt die Gleichheit dieser Unterräume.

Bemerkung 10.4 *a) Überzeugen Sie sich durch genaues Durchlesen der obigen Konstruktion, dass die u_i bis auf einen Streckungsfaktor eindeutig durch die Eigenschaften (i)-(iii) und die Basis $\mathcal{V}$ festgelegt sind. Tatsächlich war die einzige „Willkür" in der Konstruktion die Festlegung $\lambda_i = 1$ in (10.8).*

b) Um nachzuweisen, dass eine Folge $u_1, \ldots, u_n$ durch Gram-Schmidt (bis auf Streckungsfaktoren) aus einer Folge $v_1, \ldots, v_n$ hervorgeht, muss man nur (i), (ii) nachweisen und dass für jedes i der Vektor u_i orthogonal zu $v_1, \ldots, v_{i-1}$ ist. (i) ist für positiv definites φ automatisch durch $u_i \neq 0$ gegeben.

c) Ob die Bedingung 10.1 erfüllt ist, „merkt" man einfach im Laufe des Verfahrens: Die Bedingung ist genau dann erfüllt, wenn man bei der Konstruktion auf keinen Vektor u_i stösst, für den $\varphi(u_i, u_i) = 0$ ist.

d) Das Gram-Schmidt Verfahren kann in beliebigen Körpern verwendet werden. In den meisten Büchern wird es jedoch nur für reelle, positiv definite Formen vorgestellt.

Beispiel 10.3 *Wir betrachten die symmetrische Bilinearform auf* $\mathbb{R}^3$ *mit der Grammatrix (bezüglich der Standardbasis)*

$$G = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix}.$$

Die zugehörige quadratische Form ist einfach

$$q(x) = x_1^2 + 4x_1x_2 + 6x_1x_3 + x_2^2 + 2x_2x_3 + x_3^2. \tag{10.9}$$

Wir wissen natürlich nicht, ob die Form positiv definit ist (sie ist es auch nicht). Dennoch wenden wir Gram-Schmidt an in der Hoffnung, dass die Sache „gut geht". Die Ausgangsbasis ist einfach die Standardbasis $\mathcal{V} = (v_1, v_2, v_3)$. *Wir nehmen* $u_1 := v_1$. *Für* u_2 *machen wir den Ansatz*

$$u_2 = v_2 + \alpha u_1.$$

Mit der Bedingung $\varphi(u_1, u_2) = 0$ *ergibt sich* $2 + \alpha = 0$, *d.h.* $\alpha = -2$. *Damit ist*

$$u_2 = \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}.$$

Nun müssen wir noch u_3 *finden mit dem Ansatz*

$$u_3 = v_3 + \alpha_1 u_1 + \alpha_2 u_2.$$

Wir erhalten

$$\alpha_1 = -\frac{\varphi(v_3, u_1)}{\varphi(u_1, u_1)} = -3,\ \alpha_2 = -\frac{\varphi(v_3, u_2)}{\varphi(u_2, u_2)} = -\frac{5}{3}.$$

Damit erhalten wir

$$u_3 = \begin{pmatrix} 1/3 \\ -5/3 \\ 1 \end{pmatrix}.$$

Die Grammatrix bezüglich der neuen orthogonalen Basis ergibt sich dann durch $\varphi(u_1, u_1) = 1$, $\varphi(u_2, u_2) = -3$, $\varphi(u_3, u_3) = 1/3$ *und* $\varphi(u_i, u_j) = 0$ *für* $i \neq j$. *Die Signatur ist offenbar* $(2, 1, 0)$.

Die Matrix der Basistransformation ist

$$S = \begin{pmatrix} 1 & -2 & 1/3 \\ 0 & 1 & -5/3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Die zugehörige Koordinatentransformation (x für die alte Basis, y für die neue) ist:

$$\begin{aligned} x_1 &= y_1 - 2y_2 + \frac{1}{3}y_3 \\ x_2 &= y_2 - \frac{5}{3}y_3 \\ x_3 &= y_{3.} \end{aligned}$$

Einsetzen in (10.9) ergibt die quadratische Form ausgedrückt durch die y_i :

$$q(x) = y_1^2 - 3y_2^2 + \frac{1}{3}y_3^2.$$

Eine nach dem Gram-Schmidt Verfahren gefundene orthogonale Basis lässt sich je nach Körper noch normieren. Ist φ positiv definit, so können wir jede orthogonale Basis $\mathcal{U} = (u_1, \ldots, u_n)$ noch durch

$$u_i' := \frac{u_i}{\sqrt{\varphi(u_i, u_i)}}$$

ersetzen. Dann gilt einfach $\varphi\left(u_i', u_j'\right) = \delta_{ij}$.

Definition 10.11 *Ist φ eine positiv definite reelle symmetrische Bilinearform oder eine positiv definite Hermitesche Form, so heisst eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$ mit $\varphi(v_i, v_j) = \delta_{ij}$* ***orthonormiert.***

Zum Schluss noch ein Beispiel über Polynome. Das Gram-Schmidt Verfahren führt auf eine Vielzahl von orthogonalen Systemen von Polynomen, indem man eine vorgegebene Folge von Polynomen, meist $1, x, x^2, x^3, \ldots$, nach Gram-Schmidt bezüglich einer bestimmten Bilinearform orthogonalisiert. Als eines von vielen Beispielen führen wir die Legendre Polynome ein.

Wir betrachten dazu den (unendlichdimensionalen) Vektorraum $C([-1, 1], \mathbb{R})$ der stetigen Abbildungen $[-1, 1] \to \mathbb{R}$ und versehen diesen Raum mit der positiv definiten Bilinearform

$$\varphi(f, g) := \int_{-1}^{1} f(x)\, g(x)\, dx.$$

Wir wenden nun das Gram-Schmidt Verfahren auf die Folge der Polynome 1, x, x^2, x^3, ... an. Dass der Vektorraum hier unendlichdimensional ist, braucht uns

nicht weiter zu stören. Wir können einfach für jedes n den $(n+1)$-dimensionalen Unterraum $L[1, x, \ldots, x^n]$ von $C([-1,1], \mathbb{R})$ betrachten. Die Polynome 1, x, …, x^n sind linear unabhängig (Beweis als Übungsaufgabe: wieder einmal van der Monde). Wir können dann Gram-Schmidt auf diese endliche Folge anwenden, können aber natürlich genausogut ad infinitum weiterfahren. Das Ergebnis ist die Folge der Legendre Polynome $P_0(x) = 1, P_1(x), P_2(x), \ldots$. Wie schon erwähnt, liefert Gram-Schmidt die Vektoren eindeutig bis auf einen Normierungsfaktor. Die Legendre Polynome werden üblicherweise so normiert, dass $P_n(1) = 1$ ist, und nicht, dass $\varphi(P_n(x), P_n(x)) = 1$ gilt, was vielleicht natürlicher wäre.

Satz 10.8

$$P_n(x) = \frac{1}{2^n n!} \frac{d^n}{dx^n} \left(x^2 - 1\right)^n$$

Beweis. Zunächst beachte man, dass $(x^2-1)^n$ ein Polynom von Grad $2n$ ist. Demzufolge ist $P_n(x)$ ein Polynom von Grad n. Damit ist (ii) nachgewiesen. (i) folgt aus der Tatsache, dass unser φ positiv definit ist. Wir wenden nun Bemerkung 10.4 b) an und weisen nach, dass für $k < n$ die Gleichung

$$\int_{-1}^{1} x^k \frac{d^n}{dx^n} \left(x^2 - 1\right)^n \, dx = 0 \tag{10.10}$$

gilt. Einmalige partielle Integration liefert

$$\int_{-1}^{1} x^k \frac{d^n}{dx^n}(x^2-1)^n \, dx = x^k \frac{d^{n-1}}{dx^{n-1}}(x^2-1)^n \Big|_{-1}^{1} - k \int_{-1}^{1} x^{k-1} \frac{d^{n-1}}{dx^{n-1}}(x^2-1)^n \, dx.$$

Der erste Summand verschwindet, denn nach $(n-1)$-facher Differentiation von $(x^2-1)^n$ erhält man eine Summe von Polynomen, von denen jedes den Faktor (x^2-1) noch mindestens ein Mal enthält. Setzt man ± 1 sein, so erhält man 0. Nun fahren wir mit dem zweiten Summanden in gleicher Weise weiter. Nach k-maliger partieller Integration erhält man

$$\begin{aligned} \int_{-1}^{1} x^k \frac{d^n}{dx^n} \left(x^2-1\right)^n \, dx &= (-1)^k \, k! \int_{-1}^{1} \frac{d^{n-k}}{dx^{n-k}} \left(x^2-1\right)^n \, dx \\ &= (-1)^k \, k! \, \frac{d^{n-k-1}}{dx^{n-k-1}} \left(x^2-1\right)^n \Big|_{-1}^{1} = 0. \end{aligned}$$

Damit ist (10.10) gezeigt. Nach der Bemerkung 10.4 sind die $P_n(x)$ bis auf eine Streckung die Polynome, die man aus dem Gram-Schmidt Verfahren erhält, wenn man dieses auf die Folge $1, x, x^2, \ldots$ anwendet. Der Vorfaktor $\frac{1}{2^n n!}$ ist die richtige Normierung, damit $P_n(1) = 1$ gilt. Der Leser möge das selbst überprüfen. ∎

10.4 Positiv definite Bilinearformen und Matrizen

Wir betrachten in diesem Abschnitt reelle oder komplexe Vektorräume und φ sei eine symmetrische Bilinearform bzw. eine Hermitesche Form.

Ist $G = (g_{ij})$ eine Grammatrix bezüglich irgendeiner Basis, so ist φ genau dann positiv definit, wenn für alle $x \in \mathbb{R}^n \setminus \{0\}$ bzw. $x \in \mathbb{C}^n \setminus \{0\}$

$$\sum_{i,j} g_{ij} x_i x_j > 0,$$

bzw.

$$\sum_{i,j} g_{ij} x_i \overline{x_j} > 0,$$

gilt. Eine symmetrische (bzw. Hermitesche) Matrix G mit dieser Eigenschaft nennt man **positiv definit.**

Lemma 10.7 *a) Eine reelle Matrix G ist genau dann symmetrisch und positiv definit, wenn es eine reguläre Matrix S gibt mit $G = S^T S$.*

b) Eine komplexe Matrix G ist genau dann Hermitesch und positiv definit, wenn es eine reguläre Matrix S gibt mit $G = S^T \overline{S}$.

Beweis. Wir beweisen a). b) geht völlig analog.

Jede Matrix der Form $S^T S$ ist offensichtlich symmetrisch. Ist $\mathcal{V}$ die Standardbasis von $\mathbb{R}^n$, so ist $G := S^T S$ die Grammatrix der Form $\varphi(x, y) = \sum_{i=1}^n x_i y_i$ bezüglich der Basis die aus den Spalten von S besteht. Damit folgt, dass G die Grammatrix einer positiv definiten symmetrischen Bilinearform ist. Demzufolge ist G positiv definit. (Man kann das natürlich auch sofort direkt nachrechnen.) Ist andererseits G positiv definit, so wissen wir nach Satz 10.4, dass eine reguläre Matrix U existiert mit $E_n = U^T G U$, d.h. $G = S^T E_n S = S^T S$ mit $S = U^{-1}$. ■

In der Regel ist es nicht ganz einfach zu entscheiden, ob eine symmetrische (oder Hermitesche) Matrix positiv definit. Ein Kriterium basiert auf Determinanten. Es reicht jedoch nicht aus, nur die Determinante von G zu berechnen.

Ist $G = (g_{ij})$ eine $n \times n$-Matrix, so bezeichnen wir mit $G^{(m)} = (g_{ij})_{1 \le i,j \le m}$, für $m = 1, \ldots, n$ die sogenannten **Hauptminoren.** Man beachte, dass mit G auch die Hauptminoren symmetrisch sind. Ist G Hermitesch, so sind es auch die Hauptminoren. Die Determinante einer Hermiteschen Matrix ist stets reell, denn es gilt

$$\det G = \det G^T = \det\left(\overline{G}\right) = \overline{\det G}.$$

Satz 10.9 *a) Sei G reell und symmetrisch. Dann ist G genau dann positiv definit, wenn* $\det\left(G^{(m)}\right) > 0$ *für $m = 1, \ldots, n$ gilt.*

b) Sei G komplex und Hermitesch. Dann ist G genau dann positiv definit, wenn $\det\left(G^{(m)}\right) > 0$ *für $m = 1, \ldots, n$ gilt.*

Beweis. Wir beweisen den reellen Fall. Der Hermitesche geht völlig analog.

(I) Wir setzen zunächst voraus, dass G positiv definit ist. Dann existiert eine reguläre Matrix S mit $G = S^T S$. Demzufolge gilt

$$\det(G) = \det\left(S^T S\right) = \det\left(S^T\right)\det(S) = \det(S)^2 > 0.$$

Ist G positiv definit, so sind offensichtlich auch alle Hauptminoren positiv definit und wir erhalten $\det\left(G^{(m)}\right) > 0$ für alle m.

(II) Die Umkehrung ist etwas delikater. Wir setzen voraus, dass $\det(G^{(m)}) > 0$ für alle m gilt. Sei $\mathcal{V} = (v_1, \ldots, v_n)$ die Standardbasis von $\mathbb{R}^n$. Wir setzen $U_m := L[v_1, \ldots, v_m]$. Sei φ die zu G gehörende symmetrische Bilinearform. Dann ist $G^{(m)}$ die Grammatrix von $\varphi_m := \varphi|_{U_m}$. Aus $\det\left(G^{(m)}\right) > 0$ folgt, dass $G^{(m)}$ regulär ist. Somit ist φ_m nichtdegeneriert, d.h. alle unsere Unterräume U_m sind nichtdegeneriert. Wir können also das Gram-Schmidtsche Orthogonalisierungsverfahren auf die Standardbasis anwenden, d.h. wir können eine orthogonale Basis $\mathcal{U} = (u_1, \ldots, u_n)$ finden mit $U_m = L[u_1, \ldots, u_m]$ für alle m. Ist S die Matrix der Basistransformation

$$u_j = \sum_{i=1}^{n} s_{ij} v_i,$$

so sind, nach der Konstruktion bei Gram-Schmidt, die $s_{ij} = 0$ für $i > j$ (u_j wird linear aus $v_1, \ldots, v_j$ kombiniert). Setzen wir $\alpha_i := \varphi(u_i, u_i)$, so erhalten wir für jedes $m \leq n$:

$$\begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \alpha_m \end{pmatrix} = \left(S^{(m)}\right)^T G^{(m)} S^{(m)},$$

wobei $S^{(m)}$ die Hauptminoren von S sind. Daraus folgt

$$\alpha_1 \cdot \ldots \cdot \alpha_m = \det\left(\left(S^{(m)}\right)^T G^{(m)} S^{(m)}\right) = \det\left(S^{(m)}\right)^2 \det\left(G^{(m)}\right) > 0$$

für $1 \leq m \leq n$. Daraus folgt $\alpha_i > 0$ für alle i, woraus sich ergibt, dass die Signatur von φ gleich $(n, 0, 0)$ ist, was bedeutet, dass φ und damit G positiv definit sind. ■

10.5 Isometrien

Ein Vektorraum V, der versehen ist mit einer Bilinearform φ, fasst man am besten als einen Raum mit einer zusätzlichen Struktur auf. Wir schreiben dies dann als Paar (V, φ). Ein Vektorraum ist per Definition schon versehen mit einer Addition und einer Multiplikation mit Skalaren. Ein Vektorraum mit einer Bilinear-

oder Sesquilinearform hat einfach eine zusätzliche Verknüpfung $\varphi : V \times V \to K$. Einige dieser Paare haben besondere Namen: Ein reeller Vektorraum versehen mit einer positiv definiten symmetrischen Bilinearform heisst **Euklidscher Vektorraum** (was nicht heissen soll, dass Euklid das schon so formuliert hat). Ein komplexer Vektorraum versehen mit einer positiv definiten Hermiteschen Form heisst **unitärer Vektorraum**. Ein **symplektischer Vektorraum** ist einfach versehen mit einer symplektischen Bilinearform. Von besonderer Bedeutung für die Physik ist ein 4-dimensionaler reeller Vektorraum versehen mit einer symmetrischen Bilinearform der Signatur $(3, 1, 0)$. Dies ist der sogenannte **Minkowski-Raum,** der in der speziellen Relativitätstheorie eine besondere Rolle spielt.

Für Vektorräume ohne zusätzliche Struktur hatten wir bisher mit einigem Aufwand die Abbildungen zwischen Vektorräumen, die die Vektorraumstrukturen respektieren, untersucht, d.h. einfach die linearen Abbildungen. Von besonderem Interesse waren dabei die linearen Selbstabbildungen eines Vektorraums, die Endomorphismen. Wir beginnen nun in diesem Unterkapitel mit der Diskussion von linearen Abbildungen, die die zusätzliche Struktur invariant lassen.

V, W seien zwei Vektorräume. Ferner sei φ eine Bilinearform auf V und ψ eine Bilinearform auf W. (bzw. φ und ψ sind Sesquilinearformen). Wir setzen nicht notwendigerweise voraus, dass φ und ψ symmetrisch sind. Wir setzen jedoch stets voraus, dass sie entweder beide symmetrisch, beide symplektisch, oder beide Hermitesch sind.

Definition 10.12 *Eine linearer Isomorphismus $f : V \to W$ heisst eine **Isometrie,** wenn für alle $u, v \in V$*

$$\psi\left(f\left(u\right), f\left(v\right)\right) = \varphi\left(u, v\right) \tag{10.11}$$

*gilt. (V, φ) und (W, ψ) heissen **isometrisch**, wenn es eine Isometrie $f : V \to W$ gibt.*

Im Prinzip kann man natürlich auch allgemeine lineare Abbildungen $f : V \to W$ betrachten, für die (10.11) gilt. Man beachte jedoch, dass für $u \in \ker f$ dann $\varphi\left(u, v\right) = 0$ für alle $v \in V$ gilt, d.h. dass $u \in \ker \varphi$ ist. Wir werden in der Regel jedoch nur nichtdegenerierte Bilinearformen betrachten, sodass man sich dann auf jeden Fall auf injektive Abbildungen beschränken muss. Eine injektive Abbildung $f : V \to W$ definiert einen Isomorphismus $V \to \operatorname{Im} f$. Wir schränken uns daher von vornherein auf Isomorphismen ein. Man beachte insbesondere, dass ein Endomorphismus $f : V \to V$, der (10.11) für eine nichtdegenerierte Form erfüllt, ein Isomorphismus sein muss (falls V endlichdimensional ist).

Ist $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V und $f : V \to W$ ein Isomorphismus, so ist $\mathcal{W} = (w_1, \ldots, w_n) := (f\left(v_1\right), \ldots, f\left(v_n\right))$ eine Basis von W. Die Bedingung der Isometrie besagt dann einfach, dass die Grammatrix von φ bezüglich $\mathcal{V}$ gleich der Grammatrix von ψ bezüglich $\mathcal{W}$ ist. Daraus und aus den Sätzen der letzten Abschnitte lassen sich die folgenden Aussagen herleiten:

Satz 10.10 *a) Sei $K = \mathbb{R}$ und seien φ, ψ symmetrisch. Dann sind (V, φ) und (W, ψ) genau dann isometrisch, wenn die Signaturen von φ und ψ übereinstimmen.*

b) Sei $K = \mathbb{C}$ und seien φ, ψ Hermitesch. Dann sind (V, φ) und (W, ψ) genau dann isometrisch, wenn die Signaturen von φ und ψ übereinstimmen.

c) Sei $K = \mathbb{C}$ und seien φ, ψ symmetrisch. Dann sind (V, φ) und (W, ψ) genau dann isometrisch, wenn $\dim(V) = \dim(W)$ *und* $\dim(\ker\varphi) = \dim(\ker\psi)$ *gelten.*

d) Seien φ, ψ symplektisch. Dann sind (V, φ) und (W, ψ) genau dann isometrisch, wenn $\dim(V) = \dim(W)$ *und* $\dim(\ker\varphi) = \dim(\ker\psi)$ *gelten.*

Beweis. Die Beweise gehen alle parallel. Wir beweisen a).

I) Wir setzen zunächst voraus, dass φ und ψ dieselbe Signatur (n_+, n_-, n_0) haben. Dann muss $\dim V = \dim W$ gelten $(= n := n_+ + n_- + n_0)$. Nach Satz 10.4 existieren Basen

$$\mathcal{V} = \left(v_1, \ldots, v_{n_+}, v_{n_+ + 1}, \ldots, v_{n_+ + n_-}, \ldots, v_{n_+ + n_- + n_0}\right)$$
$$\mathcal{W} = \left(w_1, \ldots, w_{n_+}, w_{n_+ + 1}, \ldots, w_{n_+ + n_-}, \ldots, w_{n_+ + n_- + n_0}\right)$$

von V bzw. W mit

$$\varphi(v_i, v_j) = \psi(w_i, w_j) = \begin{cases} 1 & \text{für } i = j \leq n_+ \\ -1 & \text{für } n_+ < i = j \leq n_+ + n_- \\ 0 & \text{für } i \neq j \text{ oder } i = j > n_+ + n_- \end{cases} . \qquad (10.12)$$

Wir definieren eine Isomorphismus durch $f(v_i) = w_i$, $1 \leq i \leq n$. Dies ist offensichtlich eine Isometrie.

II) Sei $f : V \to W$ eine Isometrie und (n_+, n_-, n_0) sei die Signatur von (V, φ). Wir wählen eine entsprechende Basis in V wie oben und definieren $w_i := f(v_i)$. $(w_1, \ldots, w_n)$ ist wegen der angenommenen Isomorphie eine Basis von W. Wegen der Isometriebedingung ist dann $\psi(w_i, w_j)$ wie in (10.12). Daraus folgt jedoch, dass ψ dieselbe Signatur hat. ■

Bemerkung 10.5 *Ist $f : V \to W$ eine Isometrie, so ist auch die inverse Abbildung $f^{-1} : W \to V$ eine Isometrie. Das einfache Argument sei dem Leser überlassen.*

Von besonderer Bedeutung sind isometrische Selbstabbildung $V \to V$ eines Raumes (V, φ), d.h. die Isomorphien $f : V \to V$, für die $\varphi(f(u), f(v)) = \varphi(u, v)$ für alle $u, v \in V$ gilt. Die Menge dieser Isometrien bezeichnen wir mit $\mathrm{Iso}(V, \varphi)$.

Satz 10.11 $\mathrm{Iso}(V, \varphi)$ *ist unter der Operation der Komposition eine Gruppe. Das Neutralelement ist* id_V.

Beweis. Dass id_V eine Isometrie ist, ist offensichtlich.
Seien $f, g \in \mathrm{Iso}(V, \varphi)$. Dann ist für alle $u, v \in V$:

$$\begin{aligned}\varphi((g \circ f)(u), (g \circ f)(v)) &= \varphi(g(f(u)), g(f(v))) \\ &= \varphi(f(u), f(v)) = \varphi(u, v).\end{aligned}$$

Somit ist $g \circ f \in \mathrm{Iso}(V, \varphi)$.

Ist $f \in \mathrm{Iso}(V, \varphi)$, so gilt für alle $u, v \in V$:

$$\varphi(u, v) = \varphi\left(f\left(f^{-1}(u)\right), f\left(f^{-1}(v)\right)\right) = \varphi\left(f^{-1}(u), f^{-1}(v)\right).$$

Somit ist $f^{-1} \in \mathrm{Iso}(V, \varphi)$. ■

Lemma 10.8 *Sei V ein Vektorraum und φ eine nichtdegenerierte Bilinearform. Ferner sei $\mathcal{V} = (v_1, \ldots, v_n)$ eine Basis von V und $f : V \to V$ ein Isomorphismus. Dann ist f genau dann eine Isometrie, wenn $\varphi(f(v_i), f(v_j)) = \varphi(v_i, v_j)$ für alle i, j gilt.*

Beweis. Die Aussage folgt unmittelbar aus der Linearität von f und der Bilinearität von φ. ■

Einige der Isometriegruppen gehören zu den wichtigsten Objekten der Physik. Dazu gehören die Isometriegruppen von Euklidschen und von unitären Vektorräumen. Ebenfalls von herausragender Bedeutung ist die Isometriegruppe des 4-dimensionalen Minkowski-Raumes, die sogenannte Lorentz-Gruppe. Es ist meist üblich, die Isometriegruppen als Matrizengruppen zu beschreiben. Tatsächlich können wir die Isometriegruppen als sogenannte Untergruppen der allgemeinen linearen Gruppe $GL(n, K)$, also der Gruppe der regulären $n \times n$-Matrizen betrachten.

Wir betrachten zunächst den Fall, wo V ein reeller Vektorraum ist und φ eine nichtdegenerierte symmetrische Bilinearform ist. Da $\ker \varphi = \{0\}$ ist, ist in der Signatur $n_0 = 0$. Wir bezeichnen mit I_{n_+,n_-} die $n \times n$-Diagonalmatrix $(n = n_+ + n_-)$, deren erste n_+ Diagonalelemente $+1$ sind und die restlichen -1 sind. Nach Satz 10.4 existiert eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$, bezüglich der die Grammatrix von φ gleich I_{n_+,n_-} ist. Sei $f : V \to V$ ein Isomorphismus, deren darstellende Matrix bezüglich $\mathcal{V}$ die Matrix A sei. Wir wollen nachprüfen, welche Bedingungen A erfüllen muss, damit A eine Isometrie von (V, φ) ist: Nach Lemma 10.8 genügt es zu zeigen, dass $\varphi(f(v_i), f(v_j)) = \varphi(v_i, v_j)$. Einsetzen ergibt die Bedingung

$$A^T I_{n_+,n_-} A = I_{n_+,n_-}. \tag{10.13}$$

Wir bezeichnen die Menge der reellen $n \times n$-Matrizen A, die der obigen Bedingung genügen, mit $O(n_+, n_-)$. Die obigen Überlegungen ergeben sofort, dass $O(n_+, n_-)$ bezüglich Matrizenmultiplikation eine Gruppe ist. Die für die spezielle

Relativitätstheorie besonders wichtige Gruppe $O(3,1)$ heisst **Lorentz-Gruppe**. Im positiv definiten Spezialfall, $n_+ = n$, ist die Bedingung einfach

$$A^T A = E_n \text{ oder } A^{-1} = A^T.$$

Matrizen, die dieser Bedingung genügen, heissen **orthogonal**. Die Menge der orthogonalen Matrizen wird mit $O(n)$ bezeichnet. Dies ist ebenfalls eine Gruppe. Man nennt sie die **orthogonale Gruppe.**

Von speziellem Interesse ist auch der Hermitesche Fall. Wir betrachten also einen komplexen Vektorraum V, versehen mit einer Hermiteschen Form φ. Natürlich definieren wir wie im bilinearen Fall $\mathrm{Iso}(V,\varphi)$ als die Menge der Isomorphien $f : V \to V$ mit $\varphi(f(u), f(v)) = \varphi(u,v)$ für alle $u, v \in V$. Man zeigt dann wie oben, dass $\mathrm{Iso}(V,\varphi)$ eine Gruppe ist. Nach Einführung einer Basis $\mathcal{V} = (v_1, \ldots, v_n)$, bezüglich der die Grammatrix I_{n_+,n_-} ist, können wir das in Matrizensprache übersetzen. Ein Isomorphismus $f : V \to V$ ist genau dann in $\mathrm{Iso}(V,\varphi)$ wenn die darstellende Matrix von f bezüglich der Basis $\mathcal{V}$ die folgende Gleichung erfüllt:

$$A^T I_{n_+,n_-} \overline{A} = I_{n_+,n_-}.$$

Von besonderem Interesse ist wieder der Fall einer positiv definiten Hermiteschen Form, wenn also $I_{n_+,n_-} = E_n$ ist (d.h. wenn (V,φ) ein unitärer Raum ist). In diesem Fall lautet die obige Bedingung:

$$A^T \overline{A} = E_n \text{ oder } A^{-1} = \overline{A^T}.$$

Komplexe $n \times n$-Matrizen, die diese Bedingung erfüllen, heissen **unitär.** Die Menge aller unitären Matrizen wird üblicherweise mit $U(n)$ bezeichnet. $U(n)$ ist unter der Matrizenmultiplikation eine Gruppe. Man bezeichnet sie als die **unitäre Gruppe**. $U(n)$ ist eine Untergruppe von $GL(n,\mathbb{C})$.

Es sollte aus der obigen Diskussion klar geworden sein, dass wir die „abstrakte Gruppen“ $\mathrm{Iso}(V,\varphi)$, z.B. im reellen symmetrischen Fall, mit den entsprechenden „konkreten“ Matrizengruppen $O(n_+, n_-)$ identifizieren können. Wir wollen das formal präzis formulieren:

Definition 10.13 *Seien zwei Gruppen $(G_1, *)$ und $(G_2, \cdot)$ gegeben. Eine bijektive Abbildung $f : G_1 \to G_2$ heisst* ***Gruppenisomorphismus****, wenn*

- $f(a * b) = f(a) \cdot f(b)$ *für alle* $a, b \in G_1$
- $f(a^{-1}) = f(a)^{-1}$ *für alle* $a \in G_1$

gelten.

Man überlegt sich sofort, dass ein Gruppenisomorphismus das Neutralelement von G_1 in das Neutralelment von G_2 überführt. Gruppen zwischen denen ein

Gruppenisomorphismus existiert („isomorphe Gruppen“) sind „im wesentlichen“ dieselben.

Wir weisen nun nach, dass im wesentlichen $\mathrm{Iso}(V,\varphi)$ eine der obigen Matrizengruppen ist. Wir beschränken uns auf den reellen symmetrischen Fall.

Satz 10.12 *Sei V ein reeller Vektorraum und φ eine nichtdegenerierte symmetrische Bilinearform mit Signatur (n_+, n_-). Dann existiert eine Gruppenisomorphismus $F : \mathrm{Iso}(V,\varphi) \to O(n_+, n_-)$.*

Beweis. Wir haben den Beweis im wesentlichen schon geführt. Wir führen eine Basis $\mathcal{V} = (v_1, \ldots, v_n)$ ein bezüglich der die Grammatrix von φ durch I_{n_+,n_-} gegeben ist. Ist $f \in \mathrm{Iso}(V,\varphi)$ so definieren wir $F(f)$ als die darstellende Matrix von f bezüglich $\mathcal{V}$. Aus dem letzten Semester wissen wir schon, dass $F(f \circ g) = F(f)F(g)$ und $F(f)^{-1} = F(f)^{-1}$ für $f, g \in \mathrm{Iso}(V,\varphi)$ gelten. (Das hat nichts mit der Tatsache zu tun, dass f, g Isometrien sind). Dass F bijektiv ist, folgt sofort: F ist natürlich injektiv, was auch nichts mit Isometrien zu tun hat: Sind f und g verschiedene Endomorphismen, so sind auch die darstellenden Matrizen verschieden. Zur Surjektivität beachte man, dass zu jeder Matrix A, die (10.13) erfüllt, die zugehörige Abbildung f, die durch diese Matrix dargestellt wird, eine Isometrie ist. ■

Zum Schluss diskutieren wir noch kurz die Isometriegruppe einer nichtdegenerierten symplektischen Bilinearform. Sei K beliebig (wie immer $\mathrm{char}\, K \neq 2$) und V ein $2n$-dimensionaler Vektorraum, versehen mit einer nichtdegenerierten symplektischen Form φ. Wie wir schon wissen, existiert dann eine Basis, bezüglich der die Grammatrix durch die $2n \times 2n$-Matrix

$$J_{2n} := \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & 0 & \cdots \\ 0 & \ddots & 0 \\ \vdots & 0 & \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} \end{pmatrix}$$

gegeben ist. Ist A die darstellende Matrix eines Endomorphismus $f : V \to V$, so ist $f \in \mathrm{Iso}(V,\varphi)$ genau dann, wenn

$$A^T J_{2n} A = J_{2n}$$

ist. Die Menge $\mathrm{Sp}(2n, K)$dieser Matrizen bilden bezüglich der Multiplikation eine Gruppe; man nennt sie die **Spinorgruppe.** Mit der gleichen Überlegung wie oben folgt, dass $\mathrm{Iso}(V,\varphi)$ gruppenisomorph zur entsprechenden Spinorgruppe ist.

Die orthogonalen und die unitären Gruppen sind besonders wichtig. Wir werden sie im nächsten Kapitel ausführlicher diskutieren.

11 Euklidsche und unitäre Vektorräume

In diesem Kapitel sei V ein n-dimensionaler reeller oder komplexer Vektorraum.

Definition 11.1 *Eine positive definite Bilinearform φ auf einem reellen Vektorraum oder eine positiv definite Hermitesche Form auf einem komplexen Vektorraum nennt man ein* ***Skalarprodukt.*** *Wir schreiben für Skalarprodukte meist $\langle u, v\rangle$ anstelle von $\varphi(u, v)$.*

Zur Erinnerung: Einen reellen Vektorraum versehen mit einem Skalarprodukt nennt man einen **Euklidschen Vektorraum.** Einen komplexen Vektorraum versehen mit einem Skalarprodukt nennt man **unitären Vektorraum**.

Beispiel 11.1 *Die Standardbeispiele kennen wir schon: $\mathbb{R}^n$ versehen mit dem Skalarprodukt $\langle x, y\rangle := \sum_{i=1}^n x_i y_i$, bzw. $\mathbb{C}^n$ versehen mit dem Skalarprodukt $\langle x, y\rangle := \sum_{i=1}^n x_i \overline{y_i}$.*

Bemerkung 11.1 *Wie wir schon aus dem letzten Kapitel wissen (Satz 10.10), ist jeder (endlich dimensionale) Euklidsche Vektorraum isometrisch zum $\mathbb{R}^n$ versehen mit dem Standardskalarprodukt. Ebenso ist jeder (endlich dimensionale) unitäre Vektorraum isometrisch zum $\mathbb{C}^n$ versehen mit dem Standardskalarprodukt.*

Eine wichtige Bemerkung ist, dass in einem Euklidschen oder unitären Vektorraum V, V basisunabhängig mit dem Dualraum identifiziert werden kann. Dies wird oft fast automatisch verwendet (siehe Diff.-Int. II, Gradienten). Wir betrachten den Euklidschen Fall, der unitäre geht analog.

Wir können jedem Element $v \in V$ ein Element aus $\phi(v) \in V^*$ zuordnen:

$$\phi(v)(w) := \langle v, w\rangle .$$

Offensichtlich ist die Abbildung $\phi : V \to V^*$ linear und der Kern der Abbildung ist $\{0\}$, denn aus $\phi(v) = 0$ folgt $\langle v, w\rangle = 0$ für alle w, also $v = 0$. Da V und V^* dieselbe Dimension haben, ist diese Abbildung ein Isomorphismus. (Wir haben die Positivdefinitheit nicht verwendet: Die Bemerkung ist richtig für jede nichtdegenerierte Bilinearform). In einem Euklidschen Vektorraum braucht man also nicht zwischen V und seinem Dualraum zu unterscheiden. *Man muss sich jedoch klar darüber sein, dass diese Identifikation eines Vektorraumes mit seinem Dualraum vom Skalarprodukt abhängt.* In $\mathbb{R}^n$ ist die Identifikation natürlich ganz trivial: Einem Element $x \in \mathbb{R}^n$ ordnet man das Element $\phi(x) : \mathbb{R}^n \to \mathbb{R}$, definiert durch $\phi(x)(y) := \sum_{i=1}^n x_i y_i$ zu.

Wählen wir jedoch ein geringfügig anderes Skalarprodukt in $\mathbb{R}^n$, z.B. $\langle x, y\rangle := \sum_{i=1}^n i x_i y_i$, so ist auch die Identifikation eine andere.

11.1 Längen und Winkel

Sei V ein Euklidscher oder unitärer Vektorraum. Dann ist in jedem Fall $\langle v, v\rangle \in \mathbb{R}^+ := \{x \in \mathbb{R} : x \geq 0\}$. Ist $v \neq 0$, so gilt $\langle v, v\rangle > 0$.

Wir definieren die **Länge oder (Euklidsche) Norm eines Vektors** durch

$$\|v\| = \sqrt{\langle v, v\rangle}.$$

Lemma 11.1 *Es gelten die folgenden Eigenschaften:*
a) Es ist $\|v\| \geq 0$, und $\|v\| = 0$ gilt genau dann, wenn $v = 0$ gilt.
b) Für $\lambda \in K$ und $v \in V$ gilt $\|\lambda v\| = |\lambda| \|v\|$.

Beweis. Die beiden Eigenschaften sind offensichtlich. ■

Satz 11.1 (Schwarzsche Ungleichung) *Sei V ein Euklidscher oder unitärer Vektorraum. Dann gilt für $v, w \in V$*

$$|\langle v, w\rangle| \leq \|v\| \|w\|.$$

Gleichheit gilt genau dann, wenn v und w linear abhängig sind.

Beweis. Wir führen den Beweis im Euklidschen Fall. Der unitäre geht völlig analog.

Seien v und w linear abhängig. Dann existiert $\alpha \in K$ mit $w = \alpha v$ (oder $v = \alpha w$). Somit folgt unter Verwendung des obigen Lemmas

$$|\langle v, w\rangle| = |\langle v, \alpha v\rangle| = |\alpha| \langle v, v\rangle = \|v\| (|\alpha| \|v\|) = \|v\| \|w\|.$$

Seien nun v, w linear unabhängig. Für $(\alpha, \beta) \in \mathbb{R}^2 \setminus \{(0,0)\}$ gilt $\alpha v + \beta w \neq 0$ und somit ist

$$\langle \alpha v + \beta w, \alpha v + \beta w\rangle = \alpha^2 \|v\|^2 + 2\alpha\beta \langle v, w\rangle + \beta^2 \|w\|^2 > 0.$$

Daraus ergibt sich, dass die Matrix

$$\begin{pmatrix} \|v\|^2 & \langle v, w\rangle \\ \langle v, w\rangle & \|w\|^2 \end{pmatrix}$$

positiv definit ist. Damit muss aber auch ihre Determinante strikt positiv sein, d.h. es gilt

$$\|v\|^2 \|w\|^2 - \langle v, w\rangle^2 > 0.$$

Damit ist der Satz bewiesen. ■

Lemma 11.2 (Minkowski-Ungleichung oder Dreiecksungleichung) *Für $v, w \in V$ gilt*

$$\|v + w\| \leq \|v\| + \|w\|.$$

Beweis. Ausmultiplizieren ergibt

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

Unter Verwendung der Schwarzschen Ungleichung folgt

$$\|v+w\|^2 \leq \|v\|^2 + \|w\|^2 + 2\|v\|\,\|w\| = (\|v\| + \|w\|)^2 ,$$

und damit die Minkowski-Ungleichung. ■

Die Eigenschaften von Lemma 11.1 und Lemma 11.2 machen den Vektorraum zu einem **normierten Vektorraum**. Eine Abbildung $\|\,.\,\| : V \to \mathbb{R}^+$, die diese beiden Eigenschaften hat, nennt man eine **Norm.**

Sind $v, w \in V$ mit $\langle v, w\rangle = 0$, so sagt man auch, dass v und w **senkrecht aufeinander stehen**, oder dass sie **orthogonal** sind. Der nachfolgende Satz ist nach der obigen Diskussion evident.

Satz 11.2 (Satz von Pythagoras) *Stehen v und w senkrecht aufeinander, so gilt*

$$\|v+w\|^2 = \|v\|^2 + \|w\|^2 .$$

Die obigen Eigenschaften gelten in Euklidschen und unitären Vektorräumen. Für Euklidsche Vektorräume lässt sich ein Winkel zwischen zwei von Null verschiedenen Vektoren definieren. Sind $v, w \neq 0$, so ist nach der Schwarzschen Ungleichung

$$\frac{\langle v, w\rangle}{\|v\|\,\|w\|} \in [-1, 1] .$$

Es existiert daher ein eindeutig bestimmter Winkel $\alpha \in [0, \pi]$ mit

$$\cos\alpha = \frac{\langle v, w\rangle}{\|v\|\,\|w\|}.$$

Wir bezeichnen α als den **Winkel** zwischen v und w. (Man beachte, dass im unitären Fall $\langle v, w\rangle$ im allgemeinen komplex ist, sodass ein solcher Zwischenwinkel nicht definiert werden kann).

11.2 Orthogonale Projektion

$(V, \langle\,,\,\rangle)$ sei ein Euklidscher oder unitärer Vektorraum. Wir sagen, dass zwei Unterräume U_1 und U_2 **senkrecht aufeinander stehen**, wenn $\langle u_1, u_2\rangle = 0$ ist für alle $u_1 \in U_1$ und $u_2 \in U_2$. Zur Erinnerung aus dem letzten Kapitel: Ist U ein Unterraum von V, so ist $U^\perp$ die Menge der Vektoren, die auf allen Vektoren in U senkrecht stehen. Da U nichtdegeneriert ist (ein Skalarprodukt ist positiv definit), gilt $V = U \oplus U^\perp$ (Lemma 10.3).

Satz 11.3 *Sei U ein Unterraum von V. Es existiert ein eindeutiger Endomorphismus π_U von V mit den folgenden Eigenschaften:*

a) π_U ist eine Projektion von V auf U, d.h. es gilt $\pi_U \circ \pi_U = \pi_U$ und $\operatorname{im} \pi_U = U$

b) $\ker \pi_U$ steht senkrecht auf U.

Bemerkung 11.2 *Für einen Endomorphismus f besagt $f \circ f = f$ einfach, dass $\operatorname{im} f$ unter f ein invarianter Unterraum ist. a) besagt daher, dass jeder Vektor unter π_U auf U abgebildet wird und die Vektoren in U unter π_U invariant sind.*

Beweis. *Existenz:* Es gilt, wie oben bemerkt

$$V = U \oplus U^{\perp} \tag{11.1}$$

Jeder Vektor $v \in V$ hat also eine eindeutige Darstellung $v = u + u'$ mit $u \in U$, $u' \in U^{\perp}$. Wir definieren $\pi_U(v) := u$. Dann ist $\operatorname{im} \pi_U = U$ und $\ker \pi_U = U^{\perp}$, und die Eigenschaften a) und b) folgen unmittelbar.

Eindeutigkeit: Ist f eine beliebige Projektion (d.h. ein Endomorphismus mit $f \circ f = f$) so gilt stets $V = \operatorname{im} f \oplus \ker f$. Dies sieht man wie folgt ein: Ist $v \in V$, so ist $f(v - f(v)) = f(v) - f(v) = 0$, d.h. $v - f(v) \in \ker f$. Somit folgt $V = \operatorname{im} f + \ker f$. Ist $v \in (\operatorname{im} f) \cap \ker f$, so gilt $v = f(v) = 0$. Damit ist $V = \operatorname{im} f \oplus \ker f$ allgemein für Projektionen gezeigt.

Ist nun π_U ein Endomorphismus, der a) und b) erfüllt, so gilt also

$$V = \operatorname{im} \pi_U \oplus \ker \pi_U = U \oplus \ker \pi_U \tag{11.2}$$

wegen a). Andererseits folgt wegen b): $\ker \pi_U \subset U^{\perp}$. Da die beiden Zerlegungen (11.1) und (11.2) gelten, folgt $\dim(\ker \pi_U) = \dim\left(U^{\perp}\right)$. Somit folgt $\ker \pi_U = U^{\perp}$. Ist nun $v \in V$ mit der Zerlegung $v = u + u'$, $u \in U$, $u' \in U^{\perp}$, so ergibt sich $\pi_U(v) = \pi_U(u) + \pi_U(u') = u$. Damit ist π_U genau die Abbildung, wie wir sie oben konstruiert haben, und wir haben also gezeigt, dass jede Abbildung, die die Eigenschaften a) und b) hat so gegeben sein muss. ∎

Die orthogonale Projektion hat eine sehr einfache geometrische Deutung:

Satz 11.4 *Sei U ein Unterraum eines Euklidschen oder unitären Vektorraums. Für $v \in V$ ist $\pi_U(v)$ der eindeutige Vektor in U mit dem kleinsten Abstand zu v, d.h. mit der Eigenschaft*

$$\|v - \pi_U(v)\| = \min_{u \in U} \|v - u\| .$$

Beweis. Ist u ein beliebiger Vektor in U, so ist

$$\begin{aligned} \|v - u\|^2 &= \|v - \pi_U(v) + \pi_U(v) - u\|^2 \\ &= \|v - \pi_U(v)\|^2 + \|\pi_U(v) - u\|^2 , \end{aligned}$$

die letzte Gleichung wegen Pythagoras, denn $v-\pi_U(v) \in U^\perp$ und $\pi_U(v)-u \in U$. Wir sehen also, dass für alle $u \in U$ die Ungleichung

$$\|v-\pi_U(v)\|^2 \leq \|v-u\|^2$$

gilt, mit Gleichheit genau dann, wenn $u = \pi_U(v)$ ist. Für die Ungleichungen spielt es jedoch keine Rolle, ob die Ausdrücke auf der linken und rechten Seite quadriert sind. Damit ist der Satz bewiesen. ■

Rechnerische Bestimmung der orthogonalen Projektion:

Wir diskutieren den Euklidschen Fall und geben die Modifikationen für den unitären Fall danach. Sei U aufgespannt durch die Vektoren $u_1, \ldots, u_m$. Ist $v \in V$, so ist $\pi_U(v)$ eindeutig festgelegt durch die Bedingungen

- Es existieren $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ mit

$$\pi_U(v) = \sum_{i=1}^{m} \alpha_i u_i. \tag{11.3}$$

- $v - \pi_U(v)$ steht senkrecht auf U. Das ist gleichbedeutend damit, dass $v - \pi_U(v)$ senkrecht auf allen u_i steht, d.h.

$$\langle v-\pi_U(v), u_j\rangle = 0,\ j = 1, \ldots, m.$$

Aus diesen beiden Eigenschaften können wir $\pi_U(v)$ sehr einfach ausrechnen: Wir erhalten nämlich das folgende Gleichungssystem für die α's:

$$\langle v, u_j\rangle - \sum_{i=1}^{m} \alpha_i \langle u_i, u_j\rangle = 0,\ j = 1, \ldots, m. \tag{11.4}$$

Wir führen die (symmetrische, positiv definite) Grammatrix Γ des Skalarproduktes auf U bezüglich der Basis $(u_1, \ldots, u_m)$ ein, $\Gamma := (\langle u_i, u_j\rangle)_{1\leq i,j\leq m}$, die (wegen der Positivdefinitheit) natürlich regulär ist. Dann erhalten wir die α's einfach durch

$$\alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = \left(\Gamma^T\right)^{-1} \begin{pmatrix} \langle v, u_1\rangle \\ \vdots \\ \langle v, u_m\rangle \end{pmatrix} = \Gamma^{-1} \begin{pmatrix} \langle v, u_1\rangle \\ \vdots \\ \langle v, u_m\rangle \end{pmatrix}, \tag{11.5}$$

wegen der Symmetrie der Γ-Matrix. Ein besonders bequemer Spezialfall liegt vor, wenn die u_i orthonormiert sind, d.h. wenn $\langle u_i, u_j\rangle = \delta_{ij}$ gilt. Dann ist Γ die Einheitsmatrix und wir erhalten

$$\pi_U(v) = \sum_{i=1}^{m} \langle v, u_i\rangle u_i. \tag{11.6}$$

Für $U = V$ ist natürlich $\pi_U = \mathrm{id}_V$. Die obige Gleichung ergibt dann das folgende Resultat:

Satz 11.5 *Ist $\mathcal{U} = (u_1, \ldots, u_n)$ eine orthonormierte Basis in V, so gilt für jeden Vektor $v \in V$*

$$v = \sum_{i=1}^{n} \langle v, u_i \rangle u_i.$$

Die Zahlen $\langle v, u_i \rangle$ sind also genau die Koordinaten von v bezüglich der Basis $\mathcal{U}$.

Wir diskutieren nun noch die Modifikationen im unitären Fall.

Sei wieder $u_1, \ldots, u_m$ eine Basis des Unterraumes U. Für $v \in V$ existieren $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$, die Gleichung (11.3) erfüllen. Nun schreiben wir Gleichung (11.4) (um zu vermeiden, dass wir Γ konjugieren müssen) besser mit Zeilenvektoren:

$$\begin{aligned}(\langle v, u_1 \rangle, \ldots, \langle v, u_m \rangle) &= (\alpha_1, \ldots, \alpha_m)\,\Gamma,\\ (\alpha_1, \ldots, \alpha_m) &= (\langle v, u_1 \rangle, \ldots, \langle v, u_m \rangle)\,\Gamma^{-1}.\end{aligned}$$

Für den Fall, dass die u_i orthonormiert sind, ist Γ wieder die Einheitsmatrix, und wir bekommen die Gleichung (11.6) auch im unitären Fall.

Beispiel 11.2 *Wir betrachten $\mathbb{C}^3$ mit dem Skalarprodukt*

$$\langle x, y \rangle := \sum_{i,j=1}^{3} g_{ij} x_i \overline{y_j},$$

$$G = (g_{ij}) = \begin{pmatrix} 1 & i & 1 \\ -i & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix}.$$

Sei $U = L[u_1, u_2]$, wobei u_1, u_2 die ersten zwei Vektoren der Standardbasis seien. Dann ist die Matrix Γ einfach die entsprechende Einschränkung von G:

$$\Gamma = \begin{pmatrix} 1 & i \\ -i & 2 \end{pmatrix},\ \Gamma^{-1} = \begin{pmatrix} 2 & -i \\ i & 1 \end{pmatrix}.$$

Wir wollen $\pi_U(u_3)$ berechnen, wobei $u_3 = (0, 0, 1)$ ist. Dazu brauchen wir die Skalarprodukte von u_3 mit u_1 und u_2:

$$(\langle u_3, u_1 \rangle, \langle u_3, u_2 \rangle) = (1, 0),$$

und somit

$$(\alpha_1, \alpha_2) = (1, 0) \begin{pmatrix} 2 & -i \\ i & 1 \end{pmatrix} = (2, -i).$$

Somit ist

$$\pi_U(u_3) = \begin{pmatrix} 2 \\ -i \\ 0 \end{pmatrix}.$$

Wir können das Gram-Schmidtsche Orthogonalisierungsverfahren unter diesen Gesichtspunkten noch etwas anders interpretieren: Wir setzen dazu voraus, dass $(V, \langle\ ,\ \rangle)$ ein Euklidscher oder unitärer Vektorraum ist. $\mathcal{V} = (v_1, \ldots, v_n)$ sei eine beliebige Basis, $U_i := L[v_1, \ldots, v_i]$. Um die Basis nach dem Gram-Schmidt-Verfahren zu orthogonalisieren, müssen wir $u_i \in U_i \backslash U_{i-1}$ so bestimmen, dass $\langle u_i, u\rangle = 0$ für alle $u \in U_{i-1}$ gilt. Nun ist $v_i - \pi_{U_{i-1}}(v_i)$ ein derartiger Vektor. Bis auf Streckung ist er daher genau der Vektor, den wir im Gram-Schmidt-Verfahren gefunden haben. Wenn wir noch die Bedingung stellen, dass die neue Basis $\mathcal{U} = (u_1, \ldots, u_n)$ orthonormiert ist, können wir

$$u_i = \frac{v_i - \pi_{U_{i-1}}(v_i)}{\left\| v_i - \pi_{U_{i-1}}(v_i) \right\|}$$

setzen ($u_1 := v_1 / \|v_1\|$). Die so gewonnene $\mathcal{U}$-Basis ist nicht ganz eindeutig durch die Gram-Schmidt-Bedingung $L[v_1, \ldots, v_i] = L[u_1, \ldots, u_i]$ und die Bedingung der Orthonormiertheit festgelegt: Wir können die u_i noch mit Körperelementen vom Betrag 1 multiplizieren, in $\mathbb{R}$ also mit ± 1 und in $\mathbb{C}$ mit Zahlen der Form $\mathrm{e}^{i\varphi}$.

Wenn wir die u_i rekursiv bestimmen, so berechnet sich die Projektion einfach durch

$$\pi_{U_{i-1}}(v_i) = \sum_{j=1}^{i-1} \langle v_i, u_j\rangle\, u_j.$$

Beispiel 11.3 *Wir nehmen das Skalarprodukt in $\mathbb{C}^3$ von Beispiel 11.2 oben und orthonormieren die Standardbasis. Wegen $\|v_1\| = 1$ ist $u_1 = v_1$. Es ist nun*

$$v_2 - \langle v_2, u_1\rangle\, u_1 = \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix}.$$

Dieser Vektor hat (bezüglich dem durch G gegebenen Skalarprodukt) Länge 1, somit brauchen wir nicht mehr zu normieren und setzen

$$u_2 = \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix}.$$

Nun berechnen wir u_3 mit

$$u_3 = \frac{v_3 - \langle v_3, u_1\rangle\, u_1 - \langle v_3, u_2\rangle\, u_2}{\|v_3 - \langle v_3, u_1\rangle\, u_1 - \langle v_3, u_2\rangle\, u_2\|}.$$

Es ist $\langle v_3, u_1\rangle = 1$ und $\langle v_3, u_2\rangle = -i$. Damit ist

$$v_3 - \langle v_3, u_1\rangle\, u_1 - \langle v_3, u_2\rangle\, u_3 = \begin{pmatrix} -2 \\ i \\ 1 \end{pmatrix},$$

wiederum mit Länge 1*. Somit ist der dritte orthonormierte Basisvektor*

$$u_3 = \begin{pmatrix} -2 \\ i \\ 1 \end{pmatrix}.$$

Satz 11.6 (Plancherel-Identität) *Sei V ein Euklidscher oder unitärer Vektorraum mit orthonormierter Basis $\mathcal{U} = (u_1, \ldots, u_n)$. Dann gilt*

$$\|v\|^2 = \sum_{i=1}^{n} |\langle v, u_i \rangle|^2 .$$

Beweis. Wir beweisen zur Abwechslung den unitären Fall. Wegen

$$v = \sum_{i=1}^{n} \langle v, u_i \rangle \, u_i$$

folgt

$$\begin{aligned} \|v\|^2 = \langle v, v \rangle &= \left\langle \sum_{i=1}^{n} \langle v, u_i \rangle \, u_i, \sum_{j=1}^{n} \langle v, u_j \rangle \, u_j \right\rangle \\ &= \sum_{i,j=1}^{n} \langle v, u_i \rangle \, \overline{\langle v, u_j \rangle} \, \langle u_i, u_j \rangle = \sum_{i,j=1}^{n} \langle v, u_i \rangle \, \overline{\langle v, u_j \rangle} \delta_{ij} = \sum_{i=1}^{n} |\langle v, u_i \rangle|^2 . \end{aligned}$$

■

Die Plancherel-Identität ist natürlich nichts anderes als ein etwas aufgemöbelter Pythagoras.

11.3 Methode der kleinsten Quadrate

Wir betrachten eine Anwendung, die in der Statistik (und vor allem auch in der Physik) eine grosse Rolle spielt. Zunächst ein Spezialfall. Wir stellen uns vor, dass wir im zeitlichen Verlauf eine Grösse y messen, von der wir wissen, dass die zeitliche Abhängigkeit durch $y(t) = a + bt$ gegeben ist, wobei wir $a, b \in \mathbb{R}$ nicht kennen. t sei die Zeitvariable. Man bezeichnet das auch als die Regressionsgerade. Um a und b zu bestimmen, müssen wir offensichtlich die Grösse y nur an zwei Zeitpunkten messen.

Nun sind jedoch Messungen stets mit Fehlern behaftet (Messfehler, Rundungsfehler etc.), und es empfielt sich daher (falls die Messung nicht zu teuer ist), „zur Sicherheit“ ein paar mehr Messungen vorzunehmen. Nehmen wir an, wir messen y an n Zeitpunkten $t_1 < t_2 < \ldots < t_n$. Die Messergebnisse seien $y_1, \ldots, y_n$. Nun suchen wir a, b mit $y_i = a + bt_i$, $1 \leq i \leq n$. Es ist offensichtlich, dass im Allgemeinen derartige Zahlen a, b nicht existieren. Eine beliebte

Methode, die von Gauss eingeführt wurde, besteht darin, dass man a und b so bestimmt, dass die Summe der „Residuenquadrate“ minimal ist: Die Residuen sind definiert durch $r_i = y_i - a - bt_i$, und wir bestimmen a und b so, dass

$$\sum_{i=1}^{n} r_i^2$$

minimal ist. (Man kann sich natürlich fragen, wieso man nicht die Summe der Absolutbeträge minimiert. Dafür gibt es eine etwas wacklige theoretische Erklärung, auf die wir hier nicht eingehen können, und eine praktische, dass nämlich die Summe der Quadrate sehr viel einfacher zu minimieren ist als die Summe der Absolutbeträge. Also: Gauss wird sich schon etwas dabei gedacht haben, und wir minimieren der Bequemlichkeit halber die Summe der Quadrate). Nun sehen wir, dass wir das sehr einfach als Projektionsproblem auffassen können. Im Vektorraum $\mathbb{R}^n$ betrachten wir den zweidimensionalen Unterraum, der aufgespannt wird von den beiden Vektoren

$$\mathbf{1} := \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}, \; v := \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}.$$

Man beachte, dass $\mathbf{1}$ und v linear unabhängig sind. Nach der Diskussion des letzten Abschnitts müssen wir also nur den Messvektor

$$y := \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

auf den Unterraum $U = L[\mathbf{1},v]$ orthogonal projizieren und dann die Projektion $\pi_U(y)$ eindeutig als $a\mathbf{1}+bv$ darstellen. Im letzten Abschnitt haben wir das schon berechnet:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \Gamma^{-1} \begin{pmatrix} \langle y, \mathbf{1} \rangle \\ \langle y, v \rangle \end{pmatrix},$$

wobei Γ die Grammatrix des Standardskalarprodukts auf U bezüglich der Basis $(\mathbf{1},v)$ ist:

$$\Gamma = \begin{pmatrix} n & \sum_{i=1}^n t_i \\ \sum_{i=1}^n t_i & \sum_{i=1}^n t_i^2 \end{pmatrix}.$$

Das Beispiel lässt sich natürlich noch viel komplizierter machen: Statt anzunehmen, dass sich die y-Werte aus den t-Werten (bis auf die Messfehler) durch die Beziehung $t \to y = a + bt$, ergibt, können wir einen allgemeineren Regressionsansatz machen, z.B. ein Polynom von Grad k in t :

$$t \to a_0 + a_1 t + \ldots + a_k t^k. \tag{11.7}$$

Wir messen die y-Werte wieder zu Zeitpunkten $t_1 < \ldots < t_n$. Ist $n > k+1$, so hat man wieder zuviele Messungen für die Bestimmung der a_i und wir minimimieren wieder

$$\sum_{i=1}^{n} \left(y_i - \left(a_0 + a_1 t_i + \ldots + a_k t_i^k\right)\right)^2 .$$

Hier projizieren wir den Vektor y auf den $(k+1)$-dimensionalen Unterraum, der aufgespannt wird von den Vektoren $v_0, \ldots, v_k$, mit

$$v_j := \begin{pmatrix} t_1^j \\ \vdots \\ t_n^j \end{pmatrix} .$$

Das Ergebnis dieser Projektion ist wieder

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{pmatrix} = \Gamma^{-1} \begin{pmatrix} \langle y, v_0 \rangle \\ \langle y, v_1 \rangle \\ \vdots \\ \langle y, v_k \rangle \end{pmatrix} , \tag{11.8}$$

mit $\Gamma = (\gamma_{ij})_{0 \le i,j \le k}$,

$$\gamma_{ij} = \langle v_i, v_j \rangle = \sum_{r=1}^{n} t_r^{i+j}.$$

In der statistischen Theorie bezeichnet man die rechte Seite von (11.8) als die **Schätzung** der Regressionskoeffizienten. Die Philosphie hinter dem Verfahren ist etwa die folgende: Wir gehen davon aus, dass wir ein Gesetz „kennen“, das die y-Werte in Abhängigkeit der t-Werte in der Form (11.7) angibt, wobei wir jedoch die Koeffizienten a_i nicht kennen und über Messungen bestimmen müssen. Natürlich wird vernünftigerweise niemand davon ausgehen, dass die Beziehung wegen der unvermeidlichen Messfehler ganz genau stimmt. Wir schätzen daher die a_i aus den Messungen mit dem obigen Verfahren. Bei dem ganzen Verfahren zweifeln wir jedoch das „Naturgesetz“ (11.7) nicht an und interpretieren alle Unstimmigkeiten als Messfehler.

Nun ist offensichtlich, dass die Messungen uns zum Schluss führen können, dass unser Naturgesetz gar nicht stimmt, dies insbesondere dann, wenn die Summe der Residuenquadrate auch nach Minimierung noch „sehr gross“ bleibt. Die Diskussion dieses Aspektes gehört in die statistische Testtheorie und kann hier nicht diskutiert werden.[1]

[1] Evidenterweise ist hier sehr viel „Philosophie“ mit im Spiel, denn wenn wir fest von einem Naturgesetz überzeugt sind, werden uns ein paar lumpige Messungen nicht aus der Ruhe bringen. Solche Aspekte spielen natürlich für alle unsere Erkenntnisse eine Rolle, ausser für die mathematisch und theologisch erworbenen.

11.4 Fourierkoeffizienten

Wir betrachten reellwertige Funktionen auf dem abgeschlossenen Intervall $[0, 2\pi)$. Dass das Intervall die Länge 2π hat, spielt keine grosse Rolle, ist jedoch für die Notation in der nachfolgenden Diskussion bequem. Es geht hier einfach um die Diskussion von periodischen Funktionen. Eine Funktion $f : \mathbb{R} \to \mathbb{R}$ heisst T-periodisch ($T > 0$), wenn $f(x + T) = f(x)$ für alle $x \in \mathbb{R}$ gilt. Es ist offensichtlich (der Leser möge das selbst beweisen), dass eine T-periodische Funktion durch ihre Werte auf einem Intervall $[0, T)$ eindeutig festgelegt ist. Jede T-periodische Funktion f kann in sehr einfacher Weise in eine 2π-periodische umgewandelt werden: $\widetilde{f}(x) := f(Tx/2\pi)$. Es reicht daher aus (modulo einer trivialen Transformation), 2π-periodische Funktionen zu betrachten. Schränken wir uns weiter auf stetige Funktionen ein, so müssen wir nur stetige Funktionen $[0, 2\pi) \to \mathbb{R}$ betrachten. Jede stetige Funktion $f : [0, 2\pi) \to \mathbb{R}$, die $f(0) = \lim_{x \to 2\pi} f(x)$ erfüllt, kann sehr einfach zu einer 2π-periodischen Funktion auf der ganzen rellen Achse erweitert werden.

Periodische Funktionen sind für viele Vorgänge von grosser Bedeutung, z.B. für alle Schwingungsvorgänge.

Die obige Diskussion spielt für das folgende keine Rolle. Wir betrachten einfach den Vektorraum $C([0, 2\pi], \mathbb{R})$ der reellwertigen stetigen Funktionen auf diesem Intervall und definieren darauf das Skalarprodukt

$$\langle f, g \rangle := \int_0^{2\pi} f(x)\, g(x)\, dx. \tag{11.9}$$

Die folgenden Funktionen spielen eine besondere Rolle in vielen Bereichen der Mathematik:

$$f_0(x) = \frac{1}{\sqrt{2\pi}},\ f_k(x) = \frac{1}{\sqrt{\pi}} \cos(kx),\ k \in \mathbb{N},$$
$$g_k(x) = \frac{1}{\sqrt{\pi}} \sin(kx),\ k \in \mathbb{N}.$$

Proposition 11.1 *Die obigen Funktionen sind orthonormiert bezüglich des Skalarproduktes (11.9).*

Beweis.

$$\langle f_0, f_k \rangle = \frac{1}{\sqrt{2}\pi} \int_0^{2\pi} \cos(kx)\, dx = 0,\ k \geq 1,$$

und $\langle f_0, g_k \rangle = 0$ ergibt sich gleich. Unter Verwendung der üblichen Additionstheoreme für trigonometrische Funktionen erhalten wir:

$$\begin{aligned} \langle f_k, g_l \rangle &:= \frac{1}{\pi} \int_0^{2\pi} \cos(kx) \sin(lx)\, dx \\ &= \frac{1}{\pi} \int_0^{2\pi} \left[\frac{1}{2} \sin((k + l)x) + \frac{1}{2} \sin((l - k)x) \right] = 0. \end{aligned}$$

$$\langle g_k, g_l\rangle := \frac{1}{\pi}\int_0^{2\pi} \sin(kx)\sin(lx)\,dx$$
$$= \frac{1}{\pi}\int_0^{2\pi}\left[\frac{1}{2}\cos((k-l)x) + \frac{1}{2}\cos((k+l)x)\right] = \delta_{kl},\ k,l \geq 1.$$

$\langle f_k, f_l\rangle = \delta_{kl}$, $k,l \geq 0$, folgt analog. ■

Wir betrachten den $(2N+1)$-dimensionalen Unterraum U_N von $C([0,2\pi],\mathbb{R})$, der aufgespannt wird von den Funktionen f_k, $0 \leq k \leq N$, g_k, $1 \leq k \leq N$. Die orthogonale Projektion einer Funktion $\varphi \in C([0,2\pi],\mathbb{R})$ ist dann gegeben durch

$$\pi_{U_N}(\varphi) = \langle\varphi, f_0\rangle f_0 + \sum_{k=1}^{N}\left[\langle\varphi, f_k\rangle f_k + \langle\varphi, g_k\rangle g_k\right].$$

Definition 11.2 *Die Zahlen*

$$a_0^\varphi := \langle\varphi, f_0\rangle = \frac{1}{\sqrt{2\pi}}\int_0^{2\pi}\varphi(x)\,dx,$$
$$a_k^\varphi := \langle\varphi, f_k\rangle = \frac{1}{\sqrt{\pi}}\int_0^{2\pi}\varphi(x)\cos(kx)\,dx,\ k \geq 1,$$
$$b_k^\varphi := \langle\varphi, g_k\rangle = \frac{1}{\sqrt{\pi}}\int_0^{2\pi}\varphi(x)\sin(kx)\,dx,\ k \geq 1,$$

heissen die ***Fourierkoeffizienten*** *der Funktion φ.*

Da $\varphi - \pi_{U_N}(\varphi)$ orthogonal auf allen Vektoren in U_N steht, folgt sofort

$$\|\varphi\|^2 = \int_0^{2\pi}\varphi(x)^2\,dx = \|\pi_{U_N}(\varphi)\|^2 + \|\varphi - \pi_{U_N}(\varphi)\|^2$$
$$= a_0^2 + \sum_{k=1}^{N}\left(a_k^2 + b_k^2\right) + \|\varphi - \pi_{U_N}(\varphi)\|^2.$$

(Wir lassen φ in den Notationen jeweils weg). Aus der obigen Gleichung folgt insbesondere, dass die Fourierkoeffizienten quadratisch summierbar sind:

Lemma 11.3

$$a_0^2 + \sum_{k=1}^{\infty}\left(a_k^2 + b_k^2\right) < \infty.$$

Eine naheliegende und richtige Vermutung ist, dass $\pi_{U_N}(\varphi)$ die Funktion φ approximiert, wenn $N \to \infty$ geht. Wir können das hier nicht beweisen, formulieren aber die entsprechenden Sätze. Die Art der Approximation ist in der Formulierung sehr wichtig.

Satz 11.7 (ohne Beweis)

a)

$$\lim_{N\to\infty} \|\varphi - \pi_{U_N}(\varphi)\| = 0.$$

b) (folgt sofort aus a))

$$\|\varphi\|^2 = a_0^2 + \sum_{k=1}^{\infty} \left(a_k^2 + b_k^2\right).$$

c) Ist φ einmal stetig differenzierbar, und gilt $\varphi(0) = \lim_{x\to 2\pi} \varphi(x)$, so gilt für jedes $x \in [0, 2\pi]$:

$$\varphi(x) = \lim_{N\to\infty} \pi_{U_N}(\varphi)(x),$$

d.h. es gilt

$$\varphi(x) = \frac{a_0}{\sqrt{2\pi}} + \frac{1}{\sqrt{\pi}} \sum_{k=1}^{\infty} \left[a_k \cos(kx) + b_k \sin(kx)\right]. \tag{11.10}$$

Definition 11.3 *Die Reihe (11.10) nennt man die* ***Fourierreihe*** *der Funktion φ.*

Der Satz enthält einige Subtilitäten: a) besagt, dass für jede stetige Funktion die Fourier-Reihe im quadratischen Mittel konvergiert. Es ist nicht richtig, dass für jede stetige Funktion die Fourierreihe punktweise, d.h. für jedes $x \in [0, 2\pi]$ konvergiert. Die Voraussetzungen, wie sie im obigen Satz formuliert sind, sind jedoch stärker als sie notwendig wären.

11.5 Orthogonale und unitäre Matrizen

Zur Erinnerung: Im Abschnitt 10.5 über Isometrien hatten wir orthogonale und unitäre Matrizen eingeführt. Orthogonale Matrizen sind reelle quadratische Matrizen A, die

$$A^T A = E_n \tag{11.11}$$

erfüllen. Orthogonale Matrizen sind die darstellenden Matrizen von Isometrien eines Euklidschen Vektorraums bezüglich orthonormierten Basen. Unitäre Matrizen sind komplexe quadratische Matrizen, für die

$$A^T \overline{A} = E_n$$

gilt. Unitäre Matrizen sind die darstellenden Matrizen von Isometrien eines unitären Vektorraums bezüglich orthonormierten Basen. Die Menge der orthogonalen $n \times n$-Matrizen hatten wir mit $O(n)$ bezeichnet und die Menge der unitären Matrizen mit $U(n)$. Wie wir gesehen hatten, sind $O(n)$ und $U(n)$ Gruppen.

Hier einige Eigenschaften:

Lemma 11.4 *a) Ist* $A \in O(n)$ *so gilt* $\det A \in \{-1, 1\}$.

b) Ist $A \in U(n)$ *so gilt* $|\det A| = 1$.

c) Ist $A \in O(n)$ *[bzw.* $\in U(n)$*], so ist* $A^T \in O(n)$ *[bzw.* $\in U(n)$*].*

d) Eine reelle quadratische Matrix ist genau dann orthogonal, wenn die Spalten bezüglich des Standardskalarproduktes in $\mathbb{R}^n$ *orthonormiert sind. Dies ist genau dann der Fall, wenn die Zeilen orthonormiert sind.*

e) Eine komplexe quadratische Matrix ist genau dann unitär, wenn die Spalten bezüglich des Standardskalarproduktes in $\mathbb{C}^n$ *orthonormiert sind. Dies ist wieder genau dann der Fall, wenn die Zeilen orthonormiert sind.*

Beweis. a) Ist $A \in O(n)$ so gilt

$$\begin{aligned} 1 &= \det E_n = \det\left(A^T A\right) \\ &= \det\left(A^T\right) \det A = (\det A)^2 . \end{aligned}$$

b) Ist $A \in U(n)$ so gilt

$$\begin{aligned} 1 &= \det E_n = \det\left(A^T \overline{A}\right) \\ &= \det\left(A^T\right) \det \overline{A} = \det A \overline{\det A} = |\det A|^2 . \end{aligned}$$

c) Ist $A \in O(n)$ so gilt $A^T A = A A^T = E_n$. Daraus folgt sofort $A^T \in O(n)$. Im unitären Fall folgt die Behauptung durch Konjugieren der Gleichung $\overline{A} A^T = E_n$.

d) $A \in O(n)$ gilt genau dann, wenn

$$\sum_{j=1}^{n} a_{ji} a_{jk} = \delta_{ik},\ 1 \leq i, k \leq n$$

gilt. Das ist aber nichts anderes als dass die Spaltenvektoren

$$s_i = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{2i} \end{pmatrix}$$

bezüglich des Standardskalarproduktes orthonormiert sind. Dass dies äquivalent zur entsprechenden Aussage für die Zeilen ist, folgt einfach aus c).

e) Der unitäre Fall geht analog zum orthogonalen Fall. ■

Bemerkung 11.3 *Teil d) des obigen Lemmas besagt einfach, dass eine quadratische Matrix genau dann orthogonal ist, wenn die Spalten eine orthonormierte Basis von* $\mathbb{R}^n$ *bilden. Analog im unitären Fall.*

Die orthogonalen und unitären Matrizen mit Determinante 1 spielen eine besondere Rolle:

Definition 11.4

$$SO(n) = \{A \in O(n) : \det A = 1\},$$
$$SU(n) = \{A \in U(n) : \det A = 1\}.$$

Die Matrizen in $SO(n)$ heissen ***spezielle orthogonale Matrizen****, und die in $SU(n)$* ***spezielle unitäre Matrizen.***

Lemma 11.5 *$SO(n)$ ist eine Untergruppe von $O(n)$, d.h. die Menge der speziellen orthogonalen Matrizen ist abgeschlossen gegenüber den Gruppenoperationen in $O(n)$. Eine entsprechende Aussage gilt für $SU(n)$.*

Beweis. Wir diskutieren den orthogonalen Fall. E_n ist offensichtlich in $SO(n)$. Sind A, B in $SO(n)$, so ist $AB \in SO(n)$, denn erstens ist diese Matrix orthogonal, weil $O(n)$ bezüglich der Multiplikation eine Gruppe ist, und zweitens gilt $\det(AB) = \det A \det B = 1$. Ist $A \in SO(n)$, so ist auch $A^{-1} \in SO(n)$, was sich sofort aus $\det(A^{-1}) = (\det A)^{-1}$ ergibt. ■

Wir wollen nun den wichtigen Spezialfall von orthogonalen 2×2-Matrizen diskutieren. Zunächst jedoch der Trivialfall:

$$O(1) = \{-1, 1\},\ U(1) = \left\{e^{i\varphi} : 0 \leq \varphi < 2\pi\right\}.$$

Nun zu $O(2)$: Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine reelle Matrix. Nach Lemma 11.4 c) ist diese Matrix genau dann orthogonal, wenn die folgenden drei Gleichungen erfüllt sind:

$$a^2 + c^2 = 1, \quad b^2 + d^2 = 1, \quad ab + cd = 0.$$

Die erste Gleichung ist genau dann erfüllt, wenn $\varphi \in [0, 2\pi)$ existiert mit $\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix}$. Analog gilt für die zweite Gleichung, dass sie genau dann erfüllt ist, wenn $\psi \in [0, 2\pi)$ existiert mit $\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} \cos\psi \\ \sin\psi \end{pmatrix}$. Die dritte Gleichung bedeutet dann

$$\cos\varphi \cos\psi + \sin\varphi \sin\psi = \cos(\varphi - \psi) = 0.$$

Dies ist gleichbedeutend mit

$$\psi = \left(\varphi + \frac{\pi}{2}\right) \bmod 2\pi, \text{ oder}$$
$$\psi = \left(\varphi + \frac{3\pi}{2}\right) \bmod 2\pi.$$

Es gibt also zwei Möglichkeiten für unsere Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} =: A_\varphi^+, \text{ oder}$$
$$= \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix} =: A_\varphi^-.$$

Im ersten Fall hat die Matrix Determinante 1, ist also in $SO(2)$. Im zweiten Fall ist die Determinante -1.

Wir untersuchen als Nächstes die Eigenwerte dieser Matrizen.

Zunächst die Eigenwerte von A_φ^+ : Das charakteristische Polynom ist

$$\begin{aligned}\chi_{A_\varphi^+}(x) &= \det\left(A_\varphi^+ - xE_2\right) = (\cos\varphi - x)^2 + \sin^2\varphi \\ &= x^2 - 2x\cos\varphi + 1.\end{aligned}$$

Die zwei Eigenwerte sind also

$$\cos\varphi \pm \sqrt{\cos^2\varphi - 1} = \cos\varphi \pm \sqrt{-\sin^2\varphi}.$$

Man sieht also, dass die Eigenwerte nur für $\varphi = 0, \pi$ reell sind. Sie sind in diesem Fall 1 bzw. -1 und in beiden Fällen algebraisch und geometrisch doppelt. ($A_0^+ = E_2$ und $A_\pi^+ = -E_2$). Ansonsten sind die Eigenwerte $\mathrm{e}^{\pm i\varphi}$.

Nun zu den Eigenwerten von A_φ^-.

$$\begin{aligned}\chi_{A_\varphi^-}(x) &= \det\left(A_\varphi^- - xE_2\right) = -(\cos\varphi - x)(\cos\varphi + x) - \sin^2\varphi \\ &= x^2 - 1.\end{aligned}$$

Wir erhalten also einfach die beiden Eigenwerte ± 1. A_φ^- ist also ähnlich zur Matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Die beiden Eigenvektoren sind einfach zu bestimmen:

$$\begin{aligned}\text{zu } 1: &\begin{pmatrix} \cos(\varphi/2) \\ \sin(\varphi/2) \end{pmatrix} \\ \text{zu } -1: &\begin{pmatrix} -\sin(\varphi/2) \\ \cos(\varphi/2) \end{pmatrix}.\end{aligned}$$

Wir erhalten also

$$\begin{pmatrix} \cos(\varphi/2) & -\sin(\varphi/2) \\ \sin(\varphi/2) & \cos(\varphi/2) \end{pmatrix}^{-1} A_\varphi^- \begin{pmatrix} \cos(\varphi/2) & -\sin(\varphi/2) \\ \sin(\varphi/2) & \cos(\varphi/2) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Die Basistransformationsmatrix ist natürlich $A_{\varphi/2}^+$, also selbst orthogonal (sogar in $SO(2)$).

Diese Situation ist wichtig genug für eine Definition. Wir geben sie parallel für den Euklidschen und den unitären Fall an.

Definition 11.5 *Seien A, B quadratische reelle Matrizen [bzw. quadratische komplexe Matrizen]. Dann heissen A und B* ***orthogonal ähnlich*** *[bzw.* ***unitär ähnlich****], wenn $S \in O(n)$ existiert mit*

$$B = S^{-1}AS = S^TAS$$

[bzw. wenn eine unitäre Matrix U existiert mit

$$B = U^{-1}AU = \overline{U}^T AU].$$

Die Matrizen $\in O(2) \setminus SO(2)$ sind also orthogonal ähnlich zu der Matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Lemma 11.6 *Sei $(V, \langle\ ,\ \rangle)$ ein Euklidscher [bzw. unitärer] Vektorraum. $\mathcal{V} = (v_1, \ldots, v_n)$ sei eine orthonormierte Basis. A sei eine $n \times n$-Matrix. Dann sind die folgenden Aussagen äquivalent:*

a) $A \in O(n)$ [bzw. $A \in U(n)$].

b) Die Abbildung $f : V \to V$, deren darstellende Matrix bezüglich $\mathcal{V}$ A ist, ist eine Isometrie.

c) Der Satz von Vektoren $u_1, \ldots, u_n$, definiert durch $u_j := \sum_i a_{ij} v_i$, ist eine orthonormierte Basis.

Beweis. Die Äquivalenz von a) und b) haben wir schon gezeigt: Orthogonale Matrizen sind genau die darstellenden Matrizen von Isometrien bezüglich orthonormierten Basen.

Wir zeigen die Äquivalenz von a) und c):

$$\langle u_j, u_t \rangle = \sum_{i,s} a_{ij} a_{st} \langle v_i, v_s \rangle = \sum_i a_{ij} a_{it}.$$

Wir sehen also, dass die Orthogonalitätsbedingung an die Matrix äquivalent ist zu $\langle u_j, u_t \rangle = \delta_{jt},\ 1 \leq j, t \leq n$. ∎

Unsere nächste Aufgabe ist es, Normalformen für orthogonale und unitäre Matrizen zu finden. Wir brauchen zwei Vorüberlegungen, die als Lemmata formuliert sind:

Lemma 11.7 *Sei V ein beliebiger $\mathbb{R}$-Vektorraum ($\neq \{0\}$) und f ein Endomorphismus. Dann existiert mindestens ein eindimensionaler oder ein zweidimensionaler invarianter Unterraum.*

Beweis. Hat f einen reellen Eigenwert, so existiert natürlich ein eindimensionaler invarianter Unterraum. Habe also f keinen reellen Eigenwert. Wir untersuchen die Sache am einfachsten via Matrizen. Sei $\mathcal{V} = (v_1, \ldots, v_n)$ irgendeine Basis von V und A die darstellende Matrix von f. Dann hat A sicher mindestens einen komplexen Eigenwert $\lambda \notin \mathbb{R}$, d.h. es existiert $x \in \mathbb{C}^n \setminus \{0\}$ mit $Ax = \lambda x$. Da A reell ist, folgt $A\overline{x} = \overline{\lambda}\overline{x}$, d.h. $\overline{\lambda}$ ist ein Eigenwert mit Eigenvektor $\overline{x}$. Da λ nicht reell ist, folgt $\lambda \neq \overline{\lambda}$, und damit folgt, dass x und $\overline{x}$ linear unabhängig sind. Wir betrachten den reellen Vektor, der aus den Realteilen von x besteht:

$\operatorname{Re} x := \frac{1}{2}(x + \overline{x})$, und desgleichen $\operatorname{Im} x := \frac{1}{2i}(x - \overline{x})$. Wir können natürlich die beiden Vektoren $\operatorname{Re} x$ und $\operatorname{Im} x$ als Elemente von $\mathbb{C}^n$ auffassen. Da die Matrix

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

regulär ist, folgt aus der Unabhängigkeit von x und $\overline{x}$, dass $\operatorname{Re} x$ und $\operatorname{Im} x$ linear unabhängig sind. Damit sind sie aber natürlich auch linear unabhängig als Vektoren in $\mathbb{R}^n$. Nun folgt

$$\begin{aligned} A \operatorname{Re} x &= \frac{1}{2}(Ax + A\overline{x}) = \frac{1}{2}\left(\lambda x + \overline{\lambda}\overline{x}\right) \\ &= \operatorname{Re}(\lambda x) = \operatorname{Re}\lambda \operatorname{Re} x - \operatorname{Im}\lambda \operatorname{Im} x \end{aligned}$$

und analog

$$A \operatorname{Im} x = \operatorname{Re}\lambda \operatorname{Im} x + \operatorname{Im}\lambda \operatorname{Re} x.$$

Daraus folgt

$$A \operatorname{Re} x \in L[\operatorname{Re} x, \operatorname{Im} x] \text{ und } A \operatorname{Im} x \in L[\operatorname{Re} x, \operatorname{Im} x],$$

d.h. $L[\operatorname{Re} x, \operatorname{Im} x]$ ist invariant unter der Abbildung $\mathbb{R}^n \ni z \to Az \in \mathbb{R}^n$. Dies überträgt sich nun unmittelbar auf f : Der zweidimensionale Unterraum $L[\sum_{i=1}^n \operatorname{Re}(x_i) v_i, \sum_{i=1}^n \operatorname{Im}(x_i) v_i]$ ist invariant unter f. ■

Lemma 11.8 *$(V, \langle\,,\,\rangle)$ sei Euklidsch, f eine Isometrie. Ist der Unterraum $U \subset V$ invariant unter f, so ist auch das orthogonale Komplement $U^\perp$ invariant unter f.*

Beweis. Zunächst eine Vorbemerkung: Ist f ein Isomorphismus und U ein invarianter Unterraum unter f, so ist U auch invariant unter f^{-1}. Der Beweis ist einfach: Die Einschränkung von f auf U, $f|_U$, ist eine Abbildung $U \to U$ mit Kern $\{0\}$. Daher ist diese Abbildung ein Isomorphismus, was impliziert, dass $f^{-1}(u) \in U$ für $u \in U$ ist.

Nun zum eigentlichen Beweis des Lemmas: Sei $v \in U^\perp$. Dann gilt für jedes Element $u \in U$

$$\begin{aligned} \langle u, f(v)\rangle &= \left\langle f\left(f^{-1}(u)\right), f(v)\right\rangle = \left\langle f^{-1}(u), v\right\rangle \text{ wegen der Isometrieeigenschaft} \\ &= 0 \text{ nach der Vorbemerkung und } v \in U^\perp. \end{aligned}$$

Daraus folgt $f(v) \in U^\perp$. ■

Satz 11.8 *a) Sei $(V, \langle\,,\,\rangle)$ ein Euklidscher Vektorraum und f eine Isometrie. Dann existiert eine orthonormierte Basis, bezüglich der die darstellende Matrix*

von f die folgende „Kästchengestalt“ hat:

$$\begin{pmatrix} A^+_{\varphi_1} & & & & & & & & \\ & A^+_{\varphi_2} & & & & & & 0 & \\ & & \ddots & & & & & & \\ & & & A^+_{\varphi_k} & & & & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & 0 & & & & & -1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & -1 \end{pmatrix}.$$

Die A^+_φ sind dabei die früher eingeführten 2×2-Kästchen. (Natürlich können die $+1$, -1 oder die Kästchen auch fehlen).

b) Jede orthogonale Matrix ist orthogonal ähnlich zu einer Matrix der obigen Form.

Beweis. a) Wir führen eine Induktion nach $n := \dim V$. $n = 1, 2$ hatten wir schon ausführlich diskutiert.

1. Fall f habe einen (reellen) Eigenwert λ. v sei ein zugehöriger Eigenvektor. Dann gilt

$$\lambda^2 \|v\|^2 = \|\lambda v\|^2 = \|f(v)\|^2 = \langle f(v), f(v)\rangle = \langle v, v\rangle = \|v\|^2.$$

Somit ist $\lambda \in \{-1, 1\}$.

Sei $U := L[v]$. U ist natürlich ein eindimensionaler invarianter Unterraum. Nach Lemma 10.3 gilt

$$V = U \oplus U^\perp \tag{11.12}$$

und demzufolge hat $U^\perp$ die Dimension $n-1$. Nach Lemma 11.8 ist $U^\perp$ ebenfalls invariant unter f. Wir können daher f auf $U^\perp$ einschränken. Die Einschränkung bezeichnen wir mit f'. f' ist dann $\in \mathrm{Iso}\left(U^\perp\right)$ (bezüglich der Einschränkung des Skalarproduktes auf diesen Unterraum). Nach Induktionsvoraussetzung existiert daher eine daher eine Basis $v_2, \ldots, v_n$ bezüglich der die darstellende Matrix B von f' die obige Kästchenform hat. Wegen (11.12) ist $v_2, \ldots, v_n, v$ eine Basis von V, und da U und $U^\perp$ invariant unter f sind, folgt, dass die darstellende Matrix von f bezüglich dieser Basis durch

$$\begin{pmatrix} B & 0 \\ 0 & \lambda \end{pmatrix}$$

gegeben ist, wobei $\lambda = \pm 1$ ist. Durch eine eventuelle Umstellung der Basis erhält man die gesuchte Kästchenform.

2. Fall: f habe keinen (reellen) Eigenwert. In diesem Fall gibt es keine invarianten eindimensionalen Unterräume. Nach Lemma 11.7 existiert dann jedoch mindestens ein zweidimensionaler invarianter Unterraum, nennen wir ihn wieder U. (11.12) gilt nach wie vor, und U und $U^\perp$ sind beide invariant. Sei f_1 die Einschränkung von f auf U und f_2 die Einschränkung von f auf $U^\perp$. Wählen wir eine beliebige orthonormierte Basis v_1, v_2 von U, so ist die darstellende Matrix von f_1 bezüglich dieser Basis eine orthogonale Matrix, und demzufolge ist sie eine der Matrizen A_φ^+ oder A_φ^-. Nun hat aber letztere stets Eigenwerte (± 1), was wir jedoch in diesem Fall ausgeschlossen hatten. Auf f_2 können wir wieder die Induktionsvoraussetzung anwenden und erhalten eine Basis $v_3, \ldots, v_n$ von $U^\perp$, bezüglich der die darstellende Matrix B eine $(n-2) \times (n-2)$-Kästchenmatrix ist. Dann ist die darstellende Matrix von f

$$\begin{pmatrix} A_\varphi^+ & 0 \\ 0 & B \end{pmatrix}.$$

Damit ist Teil a) bewiesen.

b) folgt sofort aus a), denn b) ist nur eine matrizentheoretische Umformulierung von a): Eine orthogonale Matrix definiert bezüglich einer (beliebigen) orthonormierten Basis eine Isometrie. Wenden wir a) auf diese Isometrie an, so erhalten wir eine neue orthonormierte Basis, bezüglich der die darstellende Matrix die Kästchenform hat. Die Matrix der Basistransformation ist selbst eine orthogonale Matrix, denn sie transformiert eine orthonormierte Basis in eine orthonormierte. Somit ist jede orthogonale Matrix orthogonal ähnlich zu einer Matrix der Kästchenform. ■

Bemerkung 11.4 *Die Anzahl der* -1 *in der Kästchenmatrix kann man noch reduzieren: Die Matrix* $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ *ist einfach* A_π^+, *sodass man die Kästchenmatrix darauf reduzieren kann, dass nur noch eine* -1 *oder gar keine vorhanden ist. Die Matrix* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *ist natürlich* A_0^+; *die Einsen lassen wir jedoch besser stehen. Wir können also zu einer Kästchenmatrix gelangen mit den Winkeln* $\varphi_i \in (0, 2\pi)$, *einer Anzahl* $+1$ *und einer oder keiner* -1. *Die Matrix hat dann Determinante* $+1$, *wenn keine* -1 *vorkommt, und sonst hat sie Determinante* -1.

Der unitäre Fall ist noch etwas einfacher als der Euklidsche, da wir hier stets Eigenwerte haben:

Satz 11.9 *a) Sei* $(V, \langle\,,\,\rangle)$ *ein unitärer Vektorraum und* f *eine Isometrie. Dann existiert eine orthonormierte Basis von* V, *bezüglich der die darstellende Matrix eine Diagonalmatrix ist, deren Einträge in der Diagonalen alle Betrag* 1 *haben, die also von der Form* $\mathrm{e}^{i\varphi_k}$ *sind für* $1 \le k \le n = \dim V$.

b) Jede unitäre Matrix ist unitär ähnlich zu einer Diagonalmatrix dieser Form.

Beweis. Da V ein komplexer Vektorraum ist, existieren stets Eigenwerte von f. Sei $\lambda \in \operatorname{spec}(f)$ und v ein Eigenvektor. Dann gilt

$$|\lambda|^2 \|v\|^2 = \langle \lambda v, \lambda v \rangle = \langle f(v), f(v) \rangle = \langle v, v \rangle = \|v\|^2 .$$

Wegen $v \neq 0$, d.h. $\|v\|^2 \neq 0$ folgt $|\lambda| = 1$, d.h. es existiert $\varphi \in [0, 2\pi)$ mit $\lambda = \mathrm{e}^{i\varphi}$. Der Rest des Arguments geht genau gleich wie im Euklidschen Fall (Fall 1). ■

11.6 Selbstadjungierte Abbildungen

$(V, \langle\ ,\ \rangle)$ sei ein Euklidscher oder unitärer Vektorraum.

Definition 11.6 *Ein Endomorphismus $f : V \to V$ heisst **selbstadjungiert** oder **symmetrisch** (letztere meist im Euklidschen Fall), falls*

$$\langle f(v), w \rangle = \langle v, f(w) \rangle , \ \forall v, w \in V$$

gilt.

Lemma 11.9 *$\mathcal{V} = (v_1, \ldots, v_n)$ sei eine orthonormierte Basis von V.*

a) Euklidscher Fall: f ist genau dann symmetrisch, wenn die darstellende Matrix bezüglich $\mathcal{V}$ symmetrisch ist.

b) Unitärer Fall: f ist genau dann selbstadjungiert, wenn die darstellende Matrix bezüglich $\mathcal{V}$ Hermitesch ist.

Beweis. Wir beweisen b): Aus der Linearität von f und der Sesquilinearität des Skalarproduktes folgt sofort, dass f genau dann selbstadjungiert ist, wenn

$$\langle f(v_i), v_j \rangle = \langle v_i, f(v_j) \rangle , \ \forall i, j$$

gilt. Sei $A = (a_{ij})$ die darstellende Matrix von f bezüglich $\mathcal{V}$. Dann ist die linke Seite der obigen Gleichung

$$\left\langle \sum_{k=1}^{n} a_{ki} v_k, v_j \right\rangle = \sum_{k=1}^{n} a_{ki} \langle v_k, v_j \rangle = a_{ji},$$

und die rechte Seite

$$\left\langle v_i, \sum_{k=1}^{n} a_{kj} v_k \right\rangle = \sum_{k=1}^{n} \overline{a_{kj}} \langle v_i, v_k \rangle = \overline{a_{ij}}.$$

Somit ist f genau dann selbstadjungiert, wenn $a_{ji} = \overline{a_{ij}}$ für alle i, j gilt, d.h. wenn A Hermitesch ist. ■

Bemerkung 11.5 *Die Eigenschaft, dass die darstellende Matrix von f symmetrisch ist, hat für Vektorräume ohne Skalarprodukt keine basisunabängige Bedeutung: Ist A symmetrisch und S eine reguläre Matrix, so ist im Allgemeinen $S^{-1}AS$ nicht symmetrisch.*

In einem Euklidschen Vektorraum hat jedoch die Symmetrie der darstellenden Matrix bezüglich einer orthonormierten Basis eine basisunabhängige Bedeutung. Ist die darstellende Matrix symmetrisch, so ist sie es auch bezüglich einer beliebigen anderen orthonormierten Basis. Dies sieht man auch auf der Ebene von Matrizen sofort. Die Matrix einer Basistransformation von einer orthonormierten Basis zu einer anderen orthonormierten ist orthogonal. Ist A symmetrisch und S orthogonal, so gilt $S^{-1}AS = S^TAS$, was offensichtlich wieder symmetrisch ist. Analog: Ist A Hermitesch und S unitär, so ist $S^{-1}AS$ wieder Hermitesch.

Bemerkung 11.6 *Die Menge der symmetrischen (bzw. selbstadjungierten) Endomorphismen ist nicht abgeschlossen gegenüber Komposition: Sind f, g symmetrisch, so ist $f \circ g$ i.a. nicht symmetrisch:*

$$\langle f(g(v)), w\rangle = \langle g(v), f(w)\rangle = \langle v, g(f(w))\rangle .$$

$f \circ g$ ist also genau dann symmetrisch, wenn $f \circ g = g \circ f$ gilt. Letzteres ist aber in der Regel nicht der Fall.

Die Menge der symmetrischen Endomorphismen bilden jedoch einen $\mathbb{R}$-Vektorraum: Sind f, g symmetrisch, und sind $\alpha, \beta \in \mathbb{R}$, so folgt sofort dass $\alpha f + \beta g$ symmetrisch ist.

Eine ähnliche Aussage gilt für selbstadjungierte Endomorphismen in einem unitären Vektorraum, wobei man sich jedoch beschränken muss: Ist f selbstadjungiert und ist $\alpha \in \mathbb{C}$, so ist αf i.a. nicht selbstadjungiert:

$$\begin{aligned}\langle \alpha f(v), w\rangle &= \alpha \langle f(v), w\rangle = \alpha \langle v, f(w)\rangle \\ &= \langle v, \overline{\alpha} f(w)\rangle .\end{aligned}$$

Man sieht somit, dass αf nur dann selbstadjungiert ist, wenn $\alpha \in \mathbb{R}$ ist. Die Menge der selbstadjungierten Endomorphismen eines unitären Vektorraums bilden somit einen $\mathbb{R}$-Vektorraum und keinen $\mathbb{C}$-Vektorraum.

Lemma 11.10 *Sei $V \neq \{0\}$. Jeder symmetrische Endomorphismus eines Euklidschen, bzw. selbstadjungierte Endomorphismus eines unitären Vektorraums, hat mindestens einen reellen Eigenwert. Alle Eigenwerte des Endomorphismus sind reell.*

Beweis. Wir betrachten den unitären Fall:

Sei f selbstadjungiert und $\lambda \in \operatorname{spec} f$. Dann existiert eine Eigenvektor $v \neq 0$ und es gilt:

$$\begin{aligned}\lambda \|v\|^2 &= \lambda \langle v, v\rangle = \langle \lambda v, v\rangle = \langle f(v), v\rangle \\ &= \langle v, f(v)\rangle = \langle v, \lambda v\rangle = \overline{\lambda} \|v\|^2 .\end{aligned}$$

Wegen $\|v\| \neq 0$ folgt $\lambda = \overline{\lambda}$. Somit sind alle Eigenwerte reell.

Ist f ein symmetrischer Endomorphismus eines Euklidschen Vektorraums, so betrachten wir die darstellende Matrix bezüglich einer beliebigen orthonormierten Basis. Diese Matrix ist nach Lemma 11.9 symmetrisch. Aufgefasst als komplexe Matrix ist sie also Hermitesch. Nach der Überlegung im unitären Fall folgt also, dass diese Matrix ausschliesslich reelle Eigenwerte hat, welche somit auch die Eigenwerte von f sind. ■

Satz 11.10 (Spektralsatz, Hauptachsentransformation) *Sei $f : V \to V$ ein Endomorphismus. f ist genau dann symmetrisch (bzw. selbstadjungiert), wenn eine orthonormale Basis existiert, die f reell diagonalisiert.*

Beweis. I) Ist f mit einer orthonormierten Basis reell diagonalisierbar, so ist f nach Lemma 11.9 offensichtlich symmetrisch (bzw. selbstadjungiert), da jede reelle Diagonalmatrix symmetrisch ist, bzw. Hermitesch.

II) Sei umgekehrt f symmetrisch, bzw. selbstadjungiert. Wir diskutieren den selbstadjungierten Fall (in einem unitären Vektorraum) und zeigen mit Induktion nach $n := \dim V$, dass f mit einer orthonormierten Matrix reell diagonalisierbar ist. Wie wir schon wissen, hat f nur reelle Eigenwerte.

Die Induktionsverankerung $n = 1$ ist trivial.

Sei also $n \geq 2$. Sei $\lambda \in \operatorname{spec}(f)$. Nach Lemma 11.10 ist $\lambda \in \mathbb{R}$. Sei v ein Eigenvektor. Wir können (mit einer Streckung) annehmen, dass $\|v\| = 1$ gilt. Sei U das orthogonale Komplement von $L[v]$.

Der springende Punkt ist, dass U f-invariant ist. Dies sieht man wie folgt: Sei $u \in U$. Dann gilt

$$\langle f(u), v\rangle = \langle u, f(v)\rangle = \langle u, \lambda v\rangle = \overline{\lambda}\langle u, v\rangle = 0.$$

Somit ist $f(u) \in U$.

Wir betrachten nun die Einschränkung f' von f auf U. Diese ist natürlich auch selbstadjungiert. Nach Induktionsvoraussetzung existiert eine orthonormierte Basis $v_2, \ldots, v_n$ von U, die f' reell diagonalisiert. Dann ist $v, v_2, \ldots, v_n$ eine orthonormierte Basis von V, die f reell diagonalisiert. ■

Korollar 11.1 *a) Jede symmetrische Matrix ist orthogonal ähnlich zu einer reellen Diagonalmatrix.*

b) Jede Hermitesche Matrix ist unitär ähnlich zu einer reellen Diagonalmatrix.

Wir wollen noch kurz auf einen Zusammenhang von Endomorphismen und Bilinearformen, und speziell von symmetrischen Endomorphismen und symmetrischen Bilinearformen eingehen. Es ist dem Leser hoffentlich schon aufgefallen, dass eine Ähnlichkeitstransformation mit orthogonalen Matrizen genau der Transformation von Grammatrizen entspricht: Ist A orthogonal ähnlich zu B, d.h. existiert eine orthogonale Matrix S mit $B = S^{-1}AS$, so ist das auch S^TAS.

Das ist genau das Transformationsverhalten von Grammatrizen bei einem Basiswechsel. Wir wollen das nun etwas abstrakter formulieren. Wir diskutieren nur den Euklidschen Fall.

Sei $(V, \langle\ ,\ \rangle)$ ein Euklidscher Vektorraum. Ist $f : V \to V$ ein Endomorphismus (beliebig zunächst), so definieren wir die Abbildung $\varphi_f : V \times V \to \mathbb{R}$ durch

$$\varphi_f(v, w) := \langle f(v), w\rangle .$$

Man sieht sofort, dass φ_f eine Bilinearform ist. Nun kann man sich sehr einfach überlegen, dass sich jede Bilinearform in dieser Weise darstellen lässt. Dazu erinnern wir uns des Isomorphismus ϕ zwischen V und V^*, den wir zum Beginn des Kapitels vorgestellt hatten: Für $v \in V$ ist $\phi(v)$ das Element in V^* mit $\phi(v)(w) = \langle v, w\rangle$. Wir bezeichnen diesen Isomorphismus hier mit ψ. Sei nun φ eine beliebige Bilinearform auf V. Für jedes $v \in V$ ist die Abbildung $w \to \varphi(v, w)$ ein Element in V^*. Wir können deshalb dessen Inverses unter ψ betrachten. Das ist ein Element $\widetilde{v} \in V$ mit $\psi(\widetilde{v})(w) = \langle\widetilde{v}, w\rangle = \varphi(v, w)$ für alle $w \in V$. Nun muss man sich überlegen, dass die Abbildung $V \ni v \to \widetilde{v} \in V$ linear ist, was dem Leser überlassen sei. Wir bezeichnen diese Abbildung mit f. f ist also ein Endomorphismus. Damit erhalten wir $\varphi(v, w) = \langle f(v), w\rangle$ für alle $v, w \in V$.

Wir haben damit bewiesen, dass $f \to \varphi_f$ surjektiv ist. Es ist nicht schwer zu zeigen, dass diese Abbildung ein Vektorraumisomorphismus zwischen dem Vektorraum der Endomorphismen und dem Vektorraum der Bilinearformen ist.

Die Bilinearform φ_f ist genau dann symmetrisch, wenn

$$\langle f(v), w\rangle = \langle f(w), v\rangle = \langle v, f(w)\rangle ,\ \forall v, w \in V$$

gilt, d.h. wenn f gemäss unserer Definition 11.6 symmetrisch ist.

Wir können nun unseren Spektralsatz 11.10 noch etwas anders interpretieren. Er besagt, dass für einen symmetrischen Endomorphismus eine orthonormale Basis $\mathcal{V} = (v_1, \ldots, v_n)$ existiert mit $f(v_i) = \lambda_i v_i$. Für die symmetrische Bilinearform φ_f bedeutet das

$$\varphi_f(v_i, v_j) = \langle f(v_i), v_j\rangle = \langle\lambda_i v_i, v_j\rangle = \lambda_i\delta_{ij}.$$

Die $\mathcal{V}$-Basis diagonalisiert also diese symmetrische Bilinearform im Sinne von Kapitel 10. Allerdings wissen wir aus dem Satz von Sylvester, dass wir die Grammatrix weiter zu einer Matrix mit nur noch ± 1 und Nullen in der Diagonalen vereinfachen können; dies geht jedoch dann nicht mehr mit einer *orthonormierten* Basis (aber noch mit einer orthogonalen, denn wir brauchen ja die v_i nur noch zu strecken).

Wir kommen noch zu einer variationellen Beschreibung der Eigenwerte eines symmetrischen oder selbstadjungierten Endomorphismus, deren unendlichdimensionalen Versionen in der Analysis und der Mathematischen Physik eine grosse Rolle spielen.

Wir betrachten einen symmetrischen Endomorphismus f eines Euklidschen Vektorraumes, oder einen selbstadjungierten eines unitären. Der selbstadjungierte Fall geht genau gleich wie der Euklidsche; wir begnügen uns mit letzterem. Wir wissen schon, dass die Eigenwerte alle reell sind und der Endomorphismus diagonalisierbar ist. Seien $\lambda_m < \lambda_{m-1} < \ldots < \lambda_1$ die der Grösse nach geordneten Eigenwerte und E_i, $1 \leq i \leq m$, die Eigenräume. Da f diagonalisierbar ist gilt

$$V = \bigoplus_{i=1}^{m} E_i.$$

Ferner stehen nach dem Spektralsatz die Eigenräume alle senkrecht aufeinander.

Satz 11.11 *Es gilt*

$$\lambda_1 = \sup_{v \in V,\, v \neq 0} \frac{\langle f(v), v \rangle}{\|v\|^2} \tag{11.13}$$

und für $k \geq 2$

$$\lambda_k = \sup \left\{ \frac{\langle f(v), v \rangle}{\|v\|^2} : v \perp \bigoplus_{i=1}^{k-1} E_i \right\}. \tag{11.14}$$

($v \perp U$ bedeutet, dass v orthogonal zu allen Vektoren in U ist).

Beweis. Jedes Element $v \in V$ hat eine eindeutige Darstellung

$$v = \sum_{i=1}^{m} v_i,\ v_i \in E_i. \tag{11.15}$$

Dann gilt

$$\begin{aligned} \|v\|^2 &= \sum_{i=1}^{m} \|v_i\|^2, \\ f(v) &= \sum_{i=1}^{m} f(v_i) = \sum_{i=1}^{m} \lambda_i v_i, \\ \langle f(v), v \rangle &= \sum_{i=1}^{m} \lambda_i \|v_i\|^2. \end{aligned}$$

Somit folgt für alle $v \in V$:

$$\langle f(v), v \rangle \leq \lambda_1 \sum_{i=1}^{m} \|v_i\|^2 = \lambda_1 \|v\|^2.$$

Andererseits gilt natürlich für $v \in E_1$: $\langle f(v), v \rangle = \lambda_1 \|v\|^2$. Damit ist (11.13) bewiesen. (11.14) folgt ganz analog: Man muss nur beachten, dass die Vektoren v,

die senkrecht auf $\bigoplus_{i=1}^{k-1} E_i$ stehen, genau die Elemente sind, die in der Darstellung (11.15) $v_1 = \ldots = v_{k-1} = 0$ haben. Der Rest des Argumentes geht genau gleich. ■

Zum Schluss dieses Abschnittes geben wir noch eine

Anwendung auf stochastische Matrizen.

Zur Erinnerung: Eine stochastische Matrix $P = (p_{ij})_{i,j\in I}$ war eine reelle quadratische Matrix mit nicht-negativen Komponenten und $\sum_j p_{ij} = 1$ für alle $i \in I$. (I ist eine endliche Menge, die wir natürlich mit $1, \ldots, n$ durchnumerieren können). $P^n = \left(p_{ij}^{(n)}\right)$ ist die n-te Potenz. Wir setzen nun stets voraus, dass P irreduzibel und aperiodisch ist (siehe Kapitel 8). Wie wir in diesem Kapitel gesehen hatten, existiert dann eindeutig ein stationärer Wahrscheinlichkeitsvektor $(\pi_i)_{i\in I}$ mit

$$\pi_i > 0,\ \forall i,\ \sum_i \pi_i = 1,\ \sum_i \pi_i p_{ij} = \pi_j,\ \forall j.$$

Eine sehr spezielle aber in Anwendungen wichtige Situation liegt vor, wenn die sogenannte „detailed balance“ Bedingung erfüllt ist:

$$\pi_i p_{ij} = \pi_j p_{ji},\ \forall i, j. \tag{11.16}$$

Definition 11.7 *Ein stochastische Matrix, die (11.16) erfüllt heisst* ***reversibel.***

Zu der stochastischen Matrix P definieren wir nun den zugehörigen Endomorphismus $f_P : \mathbb{R}^I \to \mathbb{R}^I$, $f_P(x) := Px$. Zudem führen wir das folgende Skalarprodukt auf $\mathbb{R}^I$ ein:

$$\langle x, y\rangle_\pi := \sum_{i\in I} \pi_i x_i y_i.$$

Lemma 11.11 *Ist P reversibel, so ist f_P symmetrisch bezüglich dieses Skalarproduktes.*

Beweis. Für $x, y \in \mathbb{R}^I$ gilt

$$\langle f_P(x), y\rangle_\pi = \sum_{i,j} \pi_i p_{ij} x_j y_i = \sum_{i,j} \pi_j p_{ji} x_j y_i = \langle x, f_P(y)\rangle_\pi .$$

■

Bemerkung 11.7 *P selbst braucht natürlich keine symmetrische Matrix zu sein. Die darstellende Matrix von f_P bezüglich einer orthonormierten Basis ist jedoch symmetrisch. Die Standardbasis von $\mathbb{R}^I$ ist jedoch i.a. nicht orthonormiert. Allerdings gewinnt man natürlich eine orthonormierte Basis aus der Standardbasis sehr einfach durch Streckung der Basisvektoren. Der Leser möge sich als Übungsaufgabe überleben, wie die darstellende Matrix von f_P bezüglich dieser orthonormierten Basis dann aussieht.*

Für reversible stochastische Matrizen gilt daher spec $(f_P) \subset \mathbb{R}$. Genauer: Wir wissen aus Kapitel 8, dass die Eigenwerte vom Betrag ≤ 1 sind. In unserem Fall gilt also spec $(f_P) \subset [-1,1]$. 1 ist immer ein Eigenwert einer stochastischen Matrix. Wenn P irreduzibel und aperiodisch ist, so ist 1 ein algebraisch einfacher Eigenwert, und -1 ist kein Eigenwert. (Alle von 1 verschiedenen Eigenwerte haben Betrag < 1). Wir ordnen die Eigenwerte der Grösse nach:

$$-1 < \lambda_m \leq \lambda_{m-1} \leq \ldots \leq \lambda_2 < \lambda_1 = 1,$$

wobei wir Eigenwerte, die algebraisch mehrfach sind, auch entsprechend oft aufschreiben. Mit dieser Festsetzung ist m die Anzahl der Elemente in I. Von besonderer Bedeutung ist die sogenannte **Spektrallücke**

$$\Delta := \min\left(1 - \lambda_2, \lambda_m + 1\right).$$

Sie gibt also einfach an, wie weit die von 1 verschiedenen Eigenwerte vom Rand von $[-1,1]$ entfernt sind. (Wir nehmen an, dass $m = |I| \geq 2$ ist.)

Wie wir aus Kapitel 8 schon wissen, gilt für jede irreduzible und aperiodische Matrix P :

$$\lim_{n\to\infty} p_{ij}^{(n)} = \pi_j, \ \forall i,j.$$

Dies können wir für reversible Matrizen nun noch wesentlich präziser beschreiben:

Satz 11.12 *Sei P reversibel, irreduzibel und aperiodisch. Dann gilt für $i \in I$ und $n \in \mathbb{N}$:*

$$\sum_j \left|p_{ij}^{(n)} - \pi_j\right| \leq \frac{1}{\sqrt{\pi_i}} \left(1 - \Delta\right)^n.$$

Beweis.

$$\begin{aligned}
\left(\sum\nolimits_j \left|p_{ij}^{(n)} - \pi_j\right|\right)^2 &= \left(\sum\nolimits_j \sqrt{\frac{\pi_j}{\pi_j}} \left|p_{ij}^{(n)} - \pi_j\right|\right)^2 \\
&\leq \left(\sum\nolimits_j \left(\sqrt{\pi_j}\right)^2\right) \left(\sum\nolimits_j \frac{1}{\pi_j} \left|p_{ij}^{(n)} - \pi_j\right|^2\right) \text{ (Schwarzsche Ungl.)} \\
&= \sum\nolimits_j \frac{1}{\pi_j} \left|p_{ij}^{(n)} - \pi_j\right|^2 \\
&= \sum\nolimits_j \frac{1}{\pi_j} \left(\left(p_{ij}^{(n)}\right)^2 - 2\pi_j p_{ij}^{(n)} + \pi_j^2\right) = \sum\nolimits_j \frac{1}{\pi_j} \left(p_{ij}^{(n)}\right)^2 - 1.
\end{aligned}$$

$$\sum\nolimits_j \frac{1}{\pi_j} \left(p_{ij}^{(n)}\right)^2 = \frac{1}{\pi_i} \sum\nolimits_j \underbrace{\pi_i p_{ij}^{(n)}}_{=\pi_j p_{ji}^{(n)}} p_{ij}^{(n)} \frac{1}{\pi_j} = \frac{1}{\pi_i} p_{ii}^{(2n)}.$$

Somit erhalten wir

$$\left(\sum\nolimits_j \left|p_{ij}^{(n)} - \pi_j\right|\right)^2 \leq \frac{1}{\pi_i} p_{ii}^{(2n)} - 1. \tag{11.17}$$

Da P reversibel ist, existiert eine orthonormierte Basis $\mathcal{V} = (v_1, \ldots, v_m)$ von Eigenvektoren, wobei v_1 der Eigenvektor zu $\lambda_1 = 1$ sei, d.h.

$$v_1 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}. \tag{11.18}$$

(Dieser Vektor ist normiert in unserem Skalarprodukt). Wie die anderen Eigenvektoren aussehen, können wir natürlich nicht sagen. Wir bezeichnen ferner mit $\mathcal{E} = (e_1, \ldots, e_m)$ die Standardbasis. Dann ist

$$\begin{aligned} p_{ii}^{(2n)} &= \frac{1}{\pi_i} \left\langle e_i, f_{P^{2n}}(e_i) \right\rangle_\pi \\ &= \frac{1}{\pi_i} \left\langle \sum\nolimits_j \left\langle e_i, v_j \right\rangle_\pi v_j,\ f_{P^{2n}} \left(\sum\nolimits_j \left\langle e_i, v_j \right\rangle_\pi v_j \right) \right\rangle_\pi \\ &= \frac{1}{\pi_i} \sum_j \lambda_j^{2n} \left\langle e_i, v_j \right\rangle_\pi^2 \\ &= \frac{1}{\pi_i} \left\langle e_i, v_1 \right\rangle_\pi^2 + \frac{1}{\pi_i} \sum_{j \neq 1} \lambda_j^{2n} \left\langle e_i, v_j \right\rangle_\pi^2. \end{aligned} \tag{11.19}$$

Nun ist $\left\langle e_i, v_1 \right\rangle_\pi$ wegen (11.18) einfach π_i, sodass der erste Summand oben einfach π_i ist. Für den zweiten Teil benützen wir, dass $|\lambda_j| \leq 1 - \Delta$, für $j \neq 1$ gilt, und somit

$$\begin{aligned} \sum_{j \neq 1} \lambda_j^{2n} \left\langle e_i, v_j \right\rangle_\pi^2 &\leq (1 - \Delta)^{2n} \sum_{j \neq 1} \left\langle e_i, v_j \right\rangle_\pi^2 \\ &\leq (1 - \Delta)^{2n} \sum_j \left\langle e_i, v_j \right\rangle_\pi^2 = (1 - \Delta)^{2n} \left\| e_i \right\|_\pi^2 = (1 - \Delta)^{2n} \pi_i. \end{aligned}$$

Kombinieren wir das mit (11.17) und (11.19), so ergibt sich

$$\left(\sum\nolimits_j \left| p_{ij}^{(n)} - \pi_j \right| \right)^2 \leq \frac{1}{\pi_i^2} \sum_{j \neq 1} \lambda_j^{2n} \left\langle e_i, v_j \right\rangle_\pi^2 \leq \frac{1}{\pi_i} (1 - \Delta)^{2n}.$$

Damit ist der Satz bewiesen. ■

Das nächste Problem ist natürlich die Bestimmung oder Abschätzung der Spektrallücke. Das ist in der Regel ein schwieriges Problem. Eine explizite Bestimmung ist ohnehin nur in Ausnahmefällen möglich.

11.7 Eine Darstellung des dreidimensionalen Euklidschen Raumes

Wir benötigen einige Vorüberlegungen über die Spur von Matrizen. Wie schon früher eingeführt, sei $M(n, K)$ der Vektorraum der $n \times n$-Matrizen mit Koeffizienten im Körper K. Ist $A \in M(n, K)$, so ist die Spur $\operatorname{trace}(A) \in K$. Wir

betrachten die Abbildung

$$M(n,K) \times M(n,K) \ni (A,B) \to \operatorname{trace}(AB). \tag{11.20}$$

Die folgenden Eigenschaften sind sehr leicht nachzuprüfen:

- Für Matrizen A, B gilt

$$\operatorname{trace}(AB) = \operatorname{trace}(BA)$$

- Für $\alpha, \alpha' \in K$ und Matrizen A, A', B gilt

$$\operatorname{trace}((\alpha A + \alpha' A')\, B) = \alpha \operatorname{trace}(AB) + \alpha' \operatorname{trace}(A'B).$$

Damit ist (11.20) eine symmetrische Bilinearform auf $M(n,K)$.

Wir betrachten nur einen Spezialfall. Sei H die Menge der Hermiteschen 2×2-Matrizen mit Spur 0 :

$$H := \left\{ \begin{pmatrix} a & \overline{b} \\ b & -a \end{pmatrix} : a \in \mathbb{R},\ b \in \mathbb{C} \right\}.$$

Die Menge der Hermiteschen Matrizen ist ein $\mathbb{R}$-Vektorraum, und H ist ein Unterraum, also selbst ein $\mathbb{R}$-Vektorraum. Eine Hermitesche Matrix der obigen Form können wir wie folgt schreiben

$$\begin{pmatrix} a & b \\ \overline{b} & -a \end{pmatrix} = \operatorname{Re}(b) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \operatorname{Im}(b) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + a \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 11.8 *Die drei Matrizen*

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

nennt man die ***Pauli-Matrizen****.*

Die drei Pauli-Matrizen spannen offenbar H als $\mathbb{R}$-Vektorraum auf und sie sind linear unabhängig. Demzufolge bilden sie eine Basis von H. Wir führen nun die oben schon diskutierte Bilinearform auf H ein (mit einem unwichtigen Faktor $1/2$) : Für $A, B \in H$ sei

$$\langle A, B \rangle_H := \frac{1}{2} \operatorname{trace}(AB).$$

Lemma 11.12 *a)* $\langle A, B \rangle_H \in \mathbb{R}$ *und* $\langle \cdot, \cdot \rangle_H$ *ist ein Skalarprodukt auf* H*.*

b) $\langle A, B \rangle_H = 0$ *gilt genau dann, wenn* $AB + BA = 0$ *ist.*

c) $\sigma_1, \sigma_2, \sigma_3$ *ist eine orthonormierte Basis.*

Beweis. a) Da $\overline{\operatorname{trace}(AB)} = \operatorname{trace}\left(\overline{AB}\right) = \operatorname{trace}\left(A^T B^T\right) = \operatorname{trace}(AB)$ gilt, ist $\langle A, B\rangle_H$ reell. Wir hatten schon gesehen, dass $\langle\cdot,\cdot\rangle_H$ symmetrisch und bilinear ist. Sei $A \in H$. A ist reell diagonalsierbar mit Eigenwerten λ_1, λ_2. Wegen $\operatorname{trace}(A) = 0$ folgt $\lambda_1 + \lambda_2 = 0$, d.h. es gibt die zwei Eigenwerte λ und $-\lambda$. Somit hat A^2 den Eigenwert λ^2 mit Vielfachheit 2, d.h. es gilt einfach $A^2 = \lambda^2 E_2$. Damit gilt

$$\langle A, A\rangle_H := \frac{1}{2}\operatorname{trace}\left(A^2\right) = \lambda^2 \geq 0$$

und $= 0$ genau dann, wenn $\lambda = 0$ ist, d.h. $A = 0$. Damit ist bewiesen, dass $\langle\cdot,\cdot\rangle_H$ positiv definit ist.

b)

$$2\operatorname{trace}(AB) = \operatorname{trace}\left((A+B)^2\right) - \operatorname{trace}\left(A^2\right) - \operatorname{trace}\left(B^2\right).$$

Nun sind, wie oben gesehen, A^2 und B^2 Vielfache der Einheitsmatrix. Das gleiche gilt für $(A+B)^2$, denn es gilt $A+B \in H$. Somit gilt $\operatorname{trace}(AB) = 0$ genau dann, wenn $(A+B)^2 - A^2 - B^2 = 0$ gilt, d.h. wenn $AB + BA = 0$ ist.

c) Die folgenden Multiplikationsregeln der Pauli-Matrizen sind sehr leicht zu überprüfen:

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\begin{aligned} \sigma_1\sigma_2 &= -\sigma_2\sigma_1 = i\sigma_3 \\ \sigma_2\sigma_3 &= -\sigma_3\sigma_2 = i\sigma_1 \\ \sigma_3\sigma_1 &= -\sigma_1\sigma_3 = i\sigma_2. \end{aligned}$$

Nach b) folgt also

$$\langle\sigma_i, \sigma_j\rangle_H = \delta_{ij},\ 1 \leq i, j \leq 3.$$

■

Korollar 11.2 $(H, \langle\,.\,,\,.\,\rangle_H)$ *ist isometrisch zum* 3*-dimensionalen Euklidschen Raum.*

Wir betrachten nun eine wichtige Abbildung $U(2) \to \operatorname{Iso}(H, \langle\cdot,\cdot\rangle_H)$. Sei $U \in U(2)$. Wir definieren $\widehat{U} : H \to H$ durch

$$\widehat{U}(A) := UAU^{-1}.$$

Lemma 11.13 *a) Für* $A \in H$, $U \in U(2)$ *ist* $\widehat{U}(A) \in H$.

b) $\widehat{U} \in \operatorname{Iso}(H, \langle\,.\,,\,.\,\rangle_H)$.

Beweis. a)

$$\left(UAU^{-1}\right)^T = \left(U^{-1}\right)^T A^T U^T = \overline{UAU^{-1}}.$$

Somit ist $\widehat{U}(A)$ Hermitesch. Weiter gilt

$$\operatorname{trace}\left(UAU^{-1}\right) = \operatorname{trace}(A) = 0.$$

b) $\widehat{U}$ ist offensichtlich linear und invertierbar mit $\widehat{U^{-1}} = \widehat{U}^{-1}$. Für $A, B \in H$ gilt

$$\begin{aligned}\left\langle \widehat{U}(A), \widehat{U}(B) \right\rangle_H &= \frac{1}{2}\operatorname{trace}\left(UAU^{-1}UBU^{-1}\right) = \frac{1}{2}\operatorname{trace}\left(UABU^{-1}\right) \\ &= \frac{1}{2}\operatorname{trace}(AB) = \langle A, B\rangle_H .\end{aligned}$$

■

Die darstellende Matrix von $\widehat{U}$ bezüglich einer beliebigen orthonormierten Basis von H ist damit orthogonal. Nehmen wir speziell die Pauli-Matrizen als Basis von H, so gilt nach Satz 11.5

$$\widehat{U}(\sigma_i) = \sum_{j=1}^{3} \left\langle \widehat{U}(\sigma_i), \sigma_j \right\rangle_H \sigma_j ,$$

und die darstellende Matrix $A = (a_{ij})$ ist somit gegeben durch

$$a_{ij} = \left\langle \widehat{U}(\sigma_j), \sigma_i \right\rangle_H = \frac{1}{2}\operatorname{trace}\left(U\sigma_j U^{-1}\sigma_i\right), \quad 1 \le i, j \le 3 .$$

Wir bezeichnen mit Φ diejenige Abbildung, welche einem $U \in U(2)$ diese darstellende Matrix zuordnet. Das heisst, $\Phi : U(2) \to O(3)$ ist definiert durch $\Phi(U) := \left(\frac{1}{2}\operatorname{trace}\left(U\sigma_j U^{-1}\sigma_i\right)\right)_{1\le i,j\le 3}$. Hier einige wichtige Eigenschaften dieser Abbildung:

Proposition 11.2 *a)* Φ *ist ein Gruppenhomomorphismus, d.h. es gilt*

- $\Phi(E_2) = E_3$
- $\Phi(UV) = \Phi(U)\Phi(V)$, $U, V \in U(2)$
- $\Phi(U^{-1}) = \Phi(U)^{-1}$, $U \in U(2)$.

b) $\Phi(-U) = U$
c) $\Phi(U) \in SO(3)$ *für alle* $U \in U(2)$.
d) $\Phi|_{SU(2)}$ *bildet* $SU(2)$ *surjektiv auf* $SO(3)$ *ab.*

Beweis. a) Die erste Aussage ist evident. Für die zweite beachte man, dass für $U, V \in U(2)$, $A \in H$

$$\widehat{(UV)}(A) = UVA(UV)^{-1} = U\left(VAV^{-1}\right)U^{-1} = \widehat{U}\left(\widehat{V}(A)\right)$$

gilt, d.h. $\widehat{(UV)} = \widehat{U} \circ \widehat{V}$. Daraus folgt die Behauptung. Die dritte Aussage folgt aus den ersten beiden.

b) ist evident.

c) Wir verwenden Satz 11.9. Zu $U \in U(2)$, existiert $S \in U(2)$ und $\varphi_1, \varphi_2 \in [0, 2\pi)$ mit

$$U = S^{-1} \begin{pmatrix} \mathrm{e}^{i\varphi_1} & 0 \\ 0 & \mathrm{e}^{i\varphi_2} \end{pmatrix} S.$$

Wir definieren

$$U_t = S^{-1} \begin{pmatrix} \mathrm{e}^{it\varphi_1} & 0 \\ 0 & \mathrm{e}^{it\varphi_2} \end{pmatrix} S \in U(2),\ 0 \leq t \leq 1.$$

Die Matrixelemente von U_t sind stetige Funktionen in t. Daraus folgt, dass die Matrixelemente von $\Phi(U_t)$, die gegeben sind durch $\frac{1}{2}\operatorname{trace}\left(U_t \sigma_i U_t^{-1} \sigma_j\right)$, stetige Funktionen in t sind. Somit ist auch $\det(\Phi(U_t))$ eine stetige Funktion in t. $\det(\Phi(U_t))$ kann aber nur die beiden Werte -1 und $+1$ annehmen (es ist die Determinante einer orthogonalen Matrix). Damit muss

$$\det(\Phi(U)) = \det(\Phi(U_1)) = \det(\Phi(U_0)) = \det(E_3) = 1$$

gelten.

d) Sei $B = (b_{ij}) \in SO(3)$. Wir suchen $U \in SU(2)$ mit $\Phi(U) = B$.

Wir definieren für $j \in \{1, 2, 3\}$ die komplexen 2×2-Matrizen

$$\xi_j := \sum_{i=1}^{3} b_{ij} \sigma_i. \tag{11.21}$$

Damit ist

$$\begin{aligned} \Phi(U) = B &\Longleftrightarrow \widehat{U}(\sigma_j) = \xi_j, \quad j = 1, 2, 3 \\ &\Longleftrightarrow \sigma_j = U^{-1} \xi_j U, \quad j = 1, 2, 3. \end{aligned}$$

Die ξ_j können wir natürlich wie üblich als lineare Abbildungen $\mathbb{C}^2 \to \mathbb{C}^2$ auffassen. Wir suchen also ein unitäre Basistransformation in $SU(2)$, sodass die darstellenden Matrizen der ξ_j in dieser neuen Basis gerade durch die σ_j gegeben sind.

Da B eine orthogonale Matrix ist, ergibt sich aus (11.21), dass (ξ_1, ξ_2, ξ_3) wie $(\sigma_1, \sigma_2, \sigma_3)$ eine orthonormierte Basis von H ist. Daraus folgt $\xi_i^2 = E_2$ (vgl. Beweis Lemma 11.12 a)), $\operatorname{trace}(\xi_i) = 0$, $i = 1, 2, 3$. Die ξ_i sind also alle Hermitesch mit Eigenwerten $+1$ und -1.

Wir beginnen mit ξ_3. Nach dem Spektralsatz ist ξ_3 unitär ähnlich zu $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Es existiert also eine Matrix $V \in U(2)$ mit

$$V^{-1} \xi_3 V = \sigma_3. \tag{11.22}$$

V ist nicht ganz eindeutig: In den Spalten müssen einfach Eigenvektoren der Länge 1 von ξ_3 stehen. Diese sind dann automatisch orthogonal; wir haben jedoch noch die Freiheit, diese Eigenvektoren mit Zahlen $\mathrm{e}^{i\varphi}$ zu multiplizieren. Dies werden wir weiter unten ausnützen, um V noch etwas zu verändern. Wir schreiben $V = (v_1, v_2)$, v_i die Spaltenvektoren von V. Wir untersuchen nun, welche Folgerungen wir aus (11.22) für ξ_1 und ξ_2 ziehen können. v_1 ist ein Eigenvektor zum Eigenwert 1 von ξ_3. Unter Ausnützung von $\langle \xi_1, \xi_3 \rangle_H = 0$ und Lemma 11.12 b) erhalten wir

$$\xi_1 v_1 = \xi_1 \xi_3 v_1 = -\xi_3 \xi_1 v_1.$$

Somit ist $\xi_1 v_1$ ein Eigenvektor zum Eigenwert -1 von ξ_3, d.h. von der Form av_2, $a \in \mathbb{C}$. Analog folgt, dass $\xi_1 v_2$ ein Eigenvektor zum Eigenwert $+1$ von ξ_3 ist. Somit folgt, dass $V^{-1}\xi_1 V$ von der Form

$$V^{-1}\xi_1 V = \begin{pmatrix} 0 & b \\ a & 0 \end{pmatrix}$$

ist. Da die Matrix auf der rechten Seite nach wie vor Hermitesch ist, folgt $a = \overline{b}$, und wegen $\xi_1^2 = E_2 : |a|^2 = |b|^2 = 1$. Somit ist $V^{-1}\xi_1 V$ von der Form

$$V^{-1}\xi_1 V = \begin{pmatrix} 0 & \mathrm{e}^{-i\lambda} \\ \mathrm{e}^{i\lambda} & 0 \end{pmatrix},\ 0 \leq \lambda < 2\pi.$$

Analog folgt

$$V^{-1}\xi_2 V = \begin{pmatrix} 0 & \mathrm{e}^{-i\mu} \\ \mathrm{e}^{i\mu} & 0 \end{pmatrix},\ 0 \leq \mu < 2\pi.$$

Wir können nun λ und μ noch etwas weiter einschränken: Aus $\xi_1\xi_2 = -\xi_2\xi_1$ folgt

$$\begin{pmatrix} 0 & \mathrm{e}^{-i\lambda} \\ \mathrm{e}^{i\lambda} & 0 \end{pmatrix} \begin{pmatrix} 0 & \mathrm{e}^{-i\mu} \\ \mathrm{e}^{i\mu} & 0 \end{pmatrix} = \begin{pmatrix} \mathrm{e}^{i(\mu-\lambda)} & 0 \\ 0 & \mathrm{e}^{i(\lambda-\mu)} \end{pmatrix} = -\begin{pmatrix} \mathrm{e}^{i(\lambda-\mu)} & 0 \\ 0 & \mathrm{e}^{i(\mu-\lambda)} \end{pmatrix}.$$

Daraus folgt $\mathrm{e}^{2i\mu} = -\mathrm{e}^{2i\lambda}$ und damit $\mathrm{e}^{i\mu} = \pm i\mathrm{e}^{i\lambda}$.

Folgerung: Für jede unitäre Matrix V, die (11.22) erfüllt, existiert λ mit

$$V^{-1}\xi_1 V = \begin{pmatrix} 0 & \mathrm{e}^{-i\lambda} \\ \mathrm{e}^{i\lambda} & 0 \end{pmatrix},\ V^{-1}\xi_2 V = \begin{pmatrix} 0 & \mp i\mathrm{e}^{-i\lambda} \\ \pm i\mathrm{e}^{i\lambda} & 0 \end{pmatrix}. \tag{11.23}$$

Wir versuchen nun, eine Matrix $U \in SU(2)$ mit Spaltenvektoren u_1, u_2 so zu konstruieren, dass $\sigma_i = U^{-1}\xi_i U$ gilt. Wir beginnen mit einer beliebigen Matrix $V \in U(2)$, die (11.22) und (11.23) erfüllt, und versuchen es mit $u_1 = \mathrm{e}^{i\varphi}v_1$, $u_2 = \mathrm{e}^{i\psi}v_2$, wobei wir φ, ψ noch bestimmen müssen. Für jede Wahl von φ, ψ bleibt (11.22) richtig und es gilt $U \in U(2)$. Es ist dann

$$\begin{aligned} U^{-1}\xi_1 U &= \begin{pmatrix} \mathrm{e}^{-i\varphi} & 0 \\ 0 & \mathrm{e}^{-i\psi} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{e}^{-i\lambda} \\ \mathrm{e}^{i\lambda} & 0 \end{pmatrix} \begin{pmatrix} \mathrm{e}^{i\varphi} & 0 \\ 0 & \mathrm{e}^{i\psi} \end{pmatrix} \\ &= \begin{pmatrix} 0 & \mathrm{e}^{i(-\lambda+\psi-\varphi)} \\ \mathrm{e}^{-i(-\lambda+\psi-\varphi)} & 0 \end{pmatrix}. \end{aligned}$$

Wählen wir φ, ψ so dass

$$-\lambda + \psi - \varphi = 0 \tag{11.24}$$

gilt, so ist

$$U^{-1}\xi_1 U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_1.$$

Ferner folgt mit derselben Rechnung

$$U^{-1}\xi_2 U = \pm\sigma_2.$$

Wir zeigen nun, dass $U^{-1}\xi_2 U = -\sigma_2$ nicht möglich ist. Wäre dies richtig, so wäre $\widehat{U}(\sigma_1) = \xi_1 = \sum_i b_{i1}\sigma_i$, $\widehat{U}(\sigma_2) = -\xi_2 = -\sum_i b_{i2}\sigma_i$, und $\widehat{U}(\sigma_3) = \xi_3 = \sum_i b_{i3}\sigma_i$. Weil die Determinante von B gleich 1 ist, wäre die Determinante der darstellenden Matrix von $\widehat{U}$ gleich -1, im Widerspruch zu Teil c) dieser Proposition.

Nun sind wir noch nicht ganz fertig, denn wir haben erst gezeigt, dass zu jeder orthogonalen Matrix B eine Matrix $U \in U(2)$ existiert mit $\Phi(U) = B$. U nach der obigen Konstruktion ist jedoch noch nicht ganz eindeutig. Es gilt offensichtlich $\Phi(\mathrm{e}^{i\rho}U) = B$ für jedes $\rho \in [0, 2\pi)$. Nun ist jedoch

$$\det\left(\mathrm{e}^{i\rho}U\right) = \mathrm{e}^{2i\rho}\det(U).$$

Da jede unitäre Matrix U eine Determinante vom Betrag 1 hat, folgt also, dass für genau zwei Werte ρ die Matrix $U' := \mathrm{e}^{i\rho}U$ in $SU(2)$ ist: $\rho = \rho_1$, $\rho = \rho_2 = \rho_1 + \pi$. Die zwei Möglichkeiten, U' zu bestimmen, unterscheiden sich nur durchs Vorzeichen.

Damit ist die Proposition vollständig bewiesen. ■

Bemerkung 11.8 *Die obige Konstruktion einer Matrix $U \in SU(2)$ mit $\Phi(U) = B$ ist im wesentlichen eindeutig, bis auf die Freiheit in der Wahl von ρ im obigen Beweis. Daraus ergibt sich, dass zu jeder Matrix $B \in SO(3)$ genau zwei Matrizen $U \in SU(2)$ existieren mit $\Phi(U) = B$. Diese beiden Möglichkeiten unterscheiden sich nur durch das Vorzeichen. Man sagt auch, $SO(3)$ sei durch $SU(2)$ zweifach überlagert.*

Die Struktur von $SU(2)$ ist relativ einfach zu bestimmen: Ist die Determinante einer Matrix

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{C},$$

gleich 1, so ist ihr Inverses gleich

$$U^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Somit ist U genau dann in $SU(2)$, wenn U von der Form

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \quad \text{mit } |a|^2 + |b|^2 = 1 \quad \text{ist.}$$

Schreiben wir a, b in Real- und Imaginärteil, so erhalten wir

$$SU(2) = \left\{ \begin{pmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{pmatrix} : x_j \in \mathbb{R}, \sum_{j=1}^{4} x_j^2 = 1 \right\}.$$

$SU(2)$ kann als Punktmenge also einfach als dreidimensionale Sphäre in einem vierdimensionalen Euklidschen Raum aufgefasst werden. Man bezeichnet diese als S^3. Dies ist etwas unpräzise: $SU(2)$ hat als Punktmenge auch die gleiche Mächtigkeit wie $\mathbb{R}$, das Intervall $[0,1]$ oder $\mathbb{R}^{100}$, d.h. es gibt bijektive Abbildungen von $SU(2)$ nach $\mathbb{R}$, nach $[0,1]$, bzw. nach $\mathbb{R}^{100}$. Das ist nicht sehr schwer zu sehen, ist jedoch hier nicht gemeint: $SU(2)$ kann nicht „unter Erhalt der Stetigkeitsstruktur" mit $\mathbb{R}$ oder $\mathbb{R}^{100}$ identifiziert werden, wohl aber mit S^3, d.h. es gibt eine bijektive Abbildung $\phi : SU(2) \to S^3$, sodass ϕ und ϕ^{-1} stetig sind. Man nennt eine derartige Abbildung einen **Homöomorphismus.** Der Leser möge sich überlegen, dass wir genau einen derartigen Homöomorphismus konstruiert haben. Man sagt, dass $SU(2)$ „topologisch" mit der dreidimensionalen Sphäre identifiziert werden kann.

Topologisch erhält man $SO(3)$, indem man in S^3 die Antipoden identifiziert. (Man kann sich jedoch zunächst nur schwer vorstellen, wie das gehen soll. Wir können auf eine formal exakte Konstruktion hier nicht eingehen.) Das ist der sogenannte dreidimensionale reelle projektive Raum RP^3. $SO(3)$ ist also topologisch äquivalent zu RP^3.

Die obige Identifikation lässt jedoch die Gruppenstruktur ausser Betracht.

Für $SU(2)$ lassen sich mit Hilfe der Pauli-Matrizen Erzeuger angeben.

Definition 11.9 *G sei eine Gruppe mit Neutralelement e. Eine nichtleere Menge $E \subset G$, $e \notin E$ heisst **Erzeugendensystem** von G, wenn sich jedes Element von G als Produkt von Elementen in E und Inversen von Elementen in E darstellen lässt. Man sagt dann auch einfach, dass E die Gruppe G **erzeugt.** (Per Konvention erzeugt $\emptyset$ die Gruppe $\{e\}$.)*

Lemma 11.14 *Sei A eine Hermitesche $n \times n$-Matrix. Dann gilt*

a) $\exp(iA) \in U(n)$

b) Jedes Element von $U(n)$ lässt sich auf diese Weise darstellen

c) $\operatorname{trace}(A) = 0$ *impliziert* $\exp(iA) \in SU(n)$.

Beweis. Das waren alles (hoffentlich gelöste) Übungsaufgaben. ∎

Da die Pauli-Matrizen alle Hermitesch mit Spur 0 sind, erhalten wir mit Hilfe von ihnen und der Exponentialabbildung Matrizen in $SU(2)$. Eine einfache Rechnung (bitte nachprüfen) ergibt:

$$\exp\left(i\frac{t}{2}\sigma_1\right) = \begin{pmatrix} \cos\frac{t}{2} & i\sin\frac{t}{2} \\ i\sin\frac{t}{2} & \cos\frac{t}{2} \end{pmatrix}, \tag{11.25}$$

$$\exp\left(i\frac{t}{2}\sigma_2\right) = \begin{pmatrix} \cos\frac{t}{2} & \sin\frac{t}{2} \\ -\sin\frac{t}{2} & \cos\frac{t}{2} \end{pmatrix}, \tag{11.26}$$

$$\exp\left(i\frac{t}{2}\sigma_3\right) = \begin{pmatrix} \mathrm{e}^{i\frac{t}{2}} & 0 \\ 0 & \mathrm{e}^{-i\frac{t}{2}} \end{pmatrix}. \tag{11.27}$$

(Der Faktor 1/2 ist nur aus historischen Gründen da.) Nun lässt sich jede Hermitesche 2×2-Matrix mit Spur 0 als Linearkombination der Pauli-Matrizen darstellen: $A = \sum_{j=1}^{3} a_j\sigma_j$. Man könnte dann auf den Gedanken kommen, dass $\exp\left(i\sum_{j=1}^{3} a_j\sigma_j\right) = \prod_{j=1}^{3}\exp\left(ia_j\sigma_j\right)$ ist, sodass dann gezeigt wäre, dass sich jede Matrix in $SU\left(2\right)$ mit Matrizen der obigen Gestalt darstellen lässt. Da die Pauli-Matrizen nicht kommutieren, stimmt diese Gleichung jedoch nicht. Dennoch lässt sich durch eine direkte Rechnung leicht nachweisen, dass sich jede Matrix $\in SU\left(2\right)$, die ja die Form $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ mit $|a|^2+|b|^2=1$ hat, als Produkt von Matrizen der Form (11.25) und (11.27) darstellen lässt. Es gilt nämlich

$$\exp\left(\frac{i\phi}{2}\sigma_3\right)\exp\left(\frac{i\theta}{2}\sigma_1\right)\exp\left(\frac{i\psi}{2}\sigma_3\right) = \begin{pmatrix} \cos\frac{\theta}{2}\mathrm{e}^{i\frac{\phi+\psi}{2}} & i\sin\frac{\theta}{2}\mathrm{e}^{i\frac{\phi-\psi}{2}} \\ i\sin\frac{\theta}{2}\mathrm{e}^{i\frac{\psi-\phi}{2}} & \cos\frac{\theta}{2}\mathrm{e}^{-i\frac{\phi+\psi}{2}} \end{pmatrix}. \tag{11.28}$$

Nun lässt sich jede Matrix $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in SU\left(2\right)$ so darstellen: Sind a und $b\neq 0$, so wählen wir $0\leq\phi<2\pi$, $0<\theta<\pi$, und $-2\pi\leq\psi<2\pi$ so, dass $|a|=\cos\frac{\theta}{2}$, $\arg a=\frac{\phi+\psi}{2}$, $\arg b=\frac{\phi-\psi+\pi}{2}$ ist. In diesem Fall sind diese Winkel eindeutig durch a und b festgelegt. Für den Fall $b=0$ wählen wir $\theta=0$. Dann sind ϕ,ψ nicht eindeutig bestimmt; wir können jedoch einfach $\psi=0$ nehmen. Im Fall $a=0$ nehmen wir $\theta=\pi$ und wieder $\psi=0$. Dann ist ϕ eindeutig bestimmt. Wir sehen also, dass die Matrizen (11.25) und (11.27) $SU\left(2\right)$ erzeugen. Die obigen Winkel θ,ϕ,ψ nennt man die **Euler-Winkel**.

Wir können die Euler-Winkel nun auch für $SO\left(3\right)$ bestimmen. Dazu berechnen wir erst $\Phi\left(\exp\left(i\frac{t}{2}\sigma_1\right)\right)$:

$$\begin{aligned}
\exp\left(i\frac{t}{2}\sigma_1\right)\sigma_1\exp\left(-i\frac{t}{2}\sigma_1\right) &= \sigma_1,\\
\exp\left(i\frac{t}{2}\sigma_1\right)\sigma_2\exp\left(-i\frac{t}{2}\sigma_1\right) &= \sigma_2\cos t-\sigma_3\sin t,\\
\exp\left(i\frac{t}{2}\sigma_1\right)\sigma_3\exp\left(-i\frac{t}{2}\sigma_1\right) &= \sigma_2\sin t+\sigma_3\cos t.
\end{aligned}$$

Damit ist

$$\Phi\left(\exp\left(i\frac{t}{2}\sigma_1\right)\right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -\sin t \\ 0 & \sin t & \cos t \end{pmatrix},$$

d.h. einfach eine Drehung um σ_1 (dem ersten Vektor unserer orthonormierten Basis in H, d.h. im dreidimensionalen Euklidschen Raum) um den Winkel t. Analog zeigt man sofort, dass $\Phi\left(\exp\left(i\frac{t}{2}\sigma_k\right)\right)$, $k = 2, 3$, ebenfalls einfach Rotationen um σ_k um den Winkel t sind. Aus (11.28) und Proposition 11.2 a) ergibt sich dann sehr einfach, dass sich jedes Element von $SO(3)$ als Komposition einer Drehung um σ_3 um den Winkel ψ, dann einer Drehung um σ_1 um den Winkel θ, und wieder einer Drehung um σ_3 um den Winkel ϕ darstellen lässt. Wegen der Identifikation der Antipoden unter Φ kann man sich bei der Wahl von ψ auf das Intervall $[0, 2\pi)$ einschränken (was ohnehin klar ist, da man sich bei einer Drehung immer auf Winkel in $[0, 2\pi)$ einschränken kann).

Die Darstellung einer Drehung in $SO(3)$ kann man natürlich auch einfacher haben: Wir wissen ja schon, dass jedes Element in $SO(3)$ eine Drehung um eine Achse ist. Daraus kann man mit etwas geometrischen Überlegungen die Eulerschen Winkel ebenfalls ablesen. Das obige Argument streicht jedoch den Zusammenhang mit der Gruppe $SU(2)$ deutlich heraus.

11.8 Hamiltonsche Quaternionen

Der Raum H der Hermiteschen 2×2-Matrizen mit Spur 0, der so eine interessante Darstellung des 3-dimensionalen Euklidschen Raumes lieferte, ist nicht abgeschlossen unter Multiplikation: $\sigma_1\sigma_2 = i\sigma_3$ ist nicht Hermitesch, und $\sigma_1^2 = E_2$ hat nicht Spur 0. Aber durch eine einfache Erweiterung erhalten wir einen Raum, in dem die Multiplikation definiert ist:

$$\mathcal{H} := \mathbb{R}E_2 + iH$$

ist abgeschlossen unter Multiplikation. Für die folgende klassische Wahl einer Basis in $\mathcal{H}$,

$$E := \sigma_0 := E_2, \qquad I := -i\sigma_1 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$
$$J := -i\sigma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad K := -i\sigma_3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

ergibt sich die Multiplikationstabelle

$$\begin{aligned} I^2 = J^2 = K^2 = -E, \quad IJ = -JI = K, \\ JK = -KJ = I, \quad KI = -IK = J. \end{aligned} \tag{11.29}$$

Beachte, dass die Multiplikation nichtkommutativ ist! Damit ist

$$\begin{aligned} \mathcal{H} = L[E, I, J, K] &= \left\{ \begin{pmatrix} \alpha - i\delta & -\gamma - i\beta \\ \gamma - i\beta & \alpha + i\delta \end{pmatrix},\ \alpha, \beta, \gamma, \delta \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix} \overline{w} & -z \\ \overline{z} & w \end{pmatrix},\ w, z \in \mathbb{C} \right\} \end{aligned}$$

eine assoziative $\mathbb{R}$-Algebra, vgl. Bemerkung 4.1. Es gilt sogar: In $\mathcal{H}$ gelten alle Körperaxiome bis auf die Kommutativität der Multiplikation:

Satz 11.13 *$\mathcal{H}$ ist ein Schiefkörper.*

Beweis. Vgl. Definition 2.5: Es ist nur zu zeigen, dass jedes Element $h \in \mathcal{H} \setminus \{0\}$ ein multiplikatives Inverses hat. h ist invertierbar $\Leftrightarrow \det h \neq 0$; $\det h = |w|^2 + |z|^2$; also gilt $\det h \neq 0 \Leftrightarrow h \neq 0$. ■

Definition 11.10 *Ein 4-dimensionaler reeller Vektorraum $\mathbb{H}$, in dem eine Basis $(\mathbf{E}, \mathbf{I}, \mathbf{J}, \mathbf{K})$ ausgezeichnet ist und in dem durch die folgende Tabelle*

	E	**I**	**J**	**K**
E	**E**	**I**	**J**	**K**
I	**I**	$-\mathbf{E}$	**K**	$-\mathbf{J}$
J	**J**	$-\mathbf{K}$	$-\mathbf{E}$	**I**
K	**K**	**J**	$-\mathbf{I}$	$-\mathbf{E}$

eine bilineare Multiplikation definiert ist, heisst eine ***Quaternionenalgebra****.*

Wir schreiben die Elemente von $\mathbb{H}$ als Koordinatenvektoren bezüglich der Basis $(\mathbf{E}, \mathbf{I}, \mathbf{J}, \mathbf{K})$: Für $q \in \mathbb{H}$, $q = \alpha\mathbf{E} + \beta\mathbf{I} + \gamma\mathbf{J} + \delta\mathbf{K}$, schreiben wir $q = (\alpha, \beta, \gamma, \delta)$.

Lemma 11.15 *Die Abbildung*

$$F : \mathbb{H} \to \mathcal{H}, \quad (\alpha, \beta, \gamma, \delta) \mapsto \begin{pmatrix} \alpha - i\delta & -\gamma - i\beta \\ \gamma - i\beta & \alpha + i\delta \end{pmatrix},$$

ist ein $\mathbb{R}$-Algebra-Isomorphismus, d.h. F ist ein Isomorphismus mit $F(qq') = F(q)F(q')$ für alle $q, q' \in \mathbb{H}$, und es gilt $F(\mathbf{E}) = E$, $F(\mathbf{I}) = I$, $F(\mathbf{J}) = J$, $F(\mathbf{K}) = K$.

Beweis. F ist offensichtlich linear und bijektiv, und wegen der Linearität genügt es, $F(qq') = F(q)F(q')$ für die Basisvektoren von $\mathbb{H}$ zu zeigen. Dort sind die Relationen aber klar, denn die Multiplikation in $\mathbb{H}$ entspricht genau der in $\mathcal{H}$ gemäss (11.29). ■

Korollar 11.3 *$\mathbb{H}$ ist eine assoziative $\mathbb{R}$-Algebra und ein Schiefkörper.*

$\mathbb{H}$ erweitert $\mathbb{R}$ und $\mathbb{C}$: $\mathbb{R}\mathbf{E}$ ist eine zu $\mathbb{R}$ isomorphe Unteralgebra, und $\mathbb{R}\mathbf{E} + \mathbb{R}\mathbf{I}$ oder $\mathbb{R}\mathbf{E} + \mathbb{R}\mathbf{J}$ oder allgemein jede Ebene in $\mathbb{H}$, die $\mathbb{R}\mathbf{E}$ enthält, ist eine zu $\mathbb{C}$ isomorphe Unteralgebra.

Man kann in $\mathbb{H}$ das kanonische Skalarprodukt einführen: für $q = (\alpha, \beta, \gamma, \delta)$ und $q' = (\alpha', \beta', \gamma', \delta')$ ist

$$\langle q, q' \rangle := \alpha\alpha' + \beta\beta' + \gamma\gamma' + \delta\delta'.$$

Die Norm von $q \in \mathbb{H}$ ist $|q| := \sqrt{\langle q, q\rangle} = \sqrt{\alpha^2+\beta^2+\gamma^2+\delta^2}$. Man hat auch analog wie in $\mathbb{C}$ eine Konjugation, $\overline{q} := (\alpha, -\beta, -\gamma, -\delta)$, für die gilt

$$\overline{\overline{q}} = q, \quad q\overline{q} = \overline{q}q = |q|^2\mathbf{E}, \quad \overline{qq'} = \overline{q'}\overline{q}.$$

Damit ist das Inverse von $q \neq 0$ gegeben durch $q^{-1} = \overline{q}/|q|^2$. Für $q = (\alpha, \beta, \gamma, \delta)$ nennt man $\alpha\mathbf{E}$ den „Realteil“ (oder „skalaren Anteil“) von q und $\beta\mathbf{I} + \gamma\mathbf{J} + \delta\mathbf{K}$ den „Imaginärteil“ (oder „vektoriellen Anteil“) von q.

Der Unterraum der rein imaginären oder vektoriellen Quaternionen $L[\mathbf{I}, \mathbf{J}, \mathbf{K}]$ ist isometrisch zum 3-dimensionalen Euklidschen Raum. Was ist nun das „quaternionische Produkt“ von zwei Vektoren des $\mathbb{R}^3$? Man rechnet nach:

$$\begin{aligned}(0, x_1, x_2, x_3)(0, y_1, y_2, y_3) &= (x_1\mathbf{I} + x_2\mathbf{J} + x_3\mathbf{K})(y_1\mathbf{I} + y_2\mathbf{J} + y_3\mathbf{K}) \\ &= -(x_1y_1 + x_2y_2 + x_3y_3)\mathbf{E} + (x_2y_3 - x_3y_2)\mathbf{I} \\ &\quad +(x_3y_1 - x_1y_3)\mathbf{J} + (x_1y_2 - x_2y_1)\mathbf{K} \\ &= (-\langle x, y\rangle, (x \times y)_1, (x \times y)_2, (x \times y)_3).\end{aligned}$$

Das Euklidsche Skalarprodukt erscheint in der skalaren Komponente, und das Vektorprodukt in den vektoriellen Komponenten. In „physikalischer Notation“ mit den Pauli-Matrizen liest sich diese Gleichung wie folgt:

$$(\vec{x} \cdot \vec{\sigma})(\vec{y} \cdot \vec{\sigma}) = (\vec{x} \cdot \vec{y})\sigma_0 + i(\vec{x} \times \vec{y}) \cdot \vec{\sigma}$$

mit $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ und $\vec{x} \cdot \vec{\sigma} = x_1\sigma_1 + x_2\sigma_2 + x_3\sigma_3$. Mit dieser Darstellung lassen sich viele Rechenregeln für das Vektorprodukt sehr elegant beweisen. (Dies und viele weitere interessante Eigenschaften der Quaternionen und viel zur Geschichte der Quaternionen kann man z.B. nachlesen in Ebbinghaus et al., *Zahlen*, Springer, 1992.)

12 Quadratische Funktionen und affine Quadriken

V sei ein endlichdimensionaler K-Vektorraum, K ein Körper mit Charakteristik ungleich 2.

12.1 Affine Räume

Definition 12.1 *Eine nichtleere Teilmenge $A \subset V$ der Form $A = a_0 + U := \{a_0 + u : u \in U\}$, wobei $a_0 \in V$ und U ein Unterraum von V ist, heisst **affiner Teilraum** von V. Die **Dimension** von A ist gleich der Dimension von U.*

Bemerkung 12.1 *a) U ist durch A eindeutig bestimmt, d.h. für Unterräume U_1, U_2 mit $U_1 \neq U_2$ gilt $a_1 + U_1 \neq a_2 + U_2$ für beliebige $a_1, a_2 \in V$.*
b) $a_0 \in A$ (wegen $0 \in U$).
c) Für beliebige $a \in A$ gilt $a_0 + U = a + U$.
d) Affine Teilräume sind Lösungsmengen von inhomogenen Gleichungssystemen: Genau dann, wenn A ein affiner Teilraum der Dimension $k < n := \dim(V)$ ist, existieren linear unabhängige Elemente $l_1, \ldots, l_{n-k} \in V^*$ und $a_1, \ldots, a_{n-k} \in K$ mit

$$A = \{v \in V : l_1(v) = a_1, \ldots, l_{n-k}(v) = a_{n-k}\}.$$

Die Beweise sind einfache Übungsaufgaben.

Eine nützliche Charakterisierung affiner Teilräume liefert das folgende Lemma:

Lemma 12.1 *Eine nichtleere Teilmenge $A \subset V$ ist genau dann ein affiner Teilraum von V, wenn für je zwei Punkte $a, b \in A$ die gesamte Gerade durch a und b in A enthalten ist.*

Beweis. Seien $a, b \in A$ und $A = a_0 + U = a + U$. Dann ist $b - a \in U$, folglich auch $\lambda(b - a) \in U$ für alle $\lambda \in K$. Damit liegt die Gerade durch a und b, $\{a + \lambda(b - a) : \lambda \in K\}$, in A. Für die Umkehrung wähle einen Punkt $a \in A$ und betrachte $U := \{b - a : b \in A\}$. Dann ist $a + U = A$. Zu zeigen ist also lediglich, dass U ein Unterraum von V ist. (i) Seien $u = b - a \in U$ und $\lambda \in K$. Wir zeigen $\lambda u \in U$. Weil die Gerade durch a und b in A liegt, ist $c = a + \lambda(b - a) \in A$ und damit ist $\lambda u = \lambda(b - a) = c - a \in U$. (ii) Seien $u = b - a \in U$ und $v = c - a \in U$. Wir zeigen $u + v \in U$. Weil die Gerade durch b und c in A liegt, ist $b + \frac{1}{2}(c - b) = \frac{1}{2}b + \frac{1}{2}c \in A$, und damit ist $u + v = b - a + c - a = 2(\frac{1}{2}b + \frac{1}{2}c - a) \in U$ wegen (i). ■

Bemerkung 12.2 *Das abstrakte Konzept eines affinen Raumes ist das folgende: Ein affiner Raum ist ein Tripel $(A, V, +)$, wobei A eine Menge von „Punkten“, V ein K-Vektorraum und $+$ eine Verknüpfung $A \times V \to A$, $(a, v) \mapsto a + v$ ist,*

die die folgenden Eigenschaften hat:
a) $a + (v + w) = (a + v) + w$ *für alle* $a \in A$ *und* $v, w \in V$*,*
b) $a + 0 = a$ *für alle* $a \in A$*,*
c) für alle $a, b \in A$ *existiert genau ein Vektor* $v \in V$ *mit* $a + v = b$*.*

Beispiel 12.1 *Das Tripel* $(V, V, +)$*, wobei* V *ein Vektorraum und* $+$ *die Vektorraumaddition ist, ist ein affiner Raum.*

Bemerkung 12.3 *Das Beispiel 12.1 ist typisch: Jeder affine Raum* $(A, V, +)$ *ist durch Festlegung eines „Ursprungs“* $a_0 \in A$ *mit* $(V, V, +)$ *identifizierbar via die Bijektion*

$$V \ni v \mapsto a_0 + v \in A.$$

Beispiel 12.2 *Ist* A *ein affiner Teilraum von* V*,* $A = a_0 + U$*, so ist* $(A, U, +)$ *ein affiner Raum (wobei* $+$ *die Vektorraumaddition in* V *ist).*

Definition 12.2 *Ein* ***affines Koordinatensystem*** *in einem* n*-dimensionalen Vektorraum* V *ist ein* $n + 1$*-Tupel von Vektoren* $(v_0, v_1, \ldots, v_n)$*, wobei* $v_0 \in V$ *und* $(v_1, \ldots, v_n)$ *eine Basis von* V *ist. Die* ***affinen Koordinaten*** *eines Vektors* $v \in V$ *bilden das* n*-Tupel* $(x_1, \ldots, x_n) \in K^n$*, und sind eindeutig bestimmt durch*

$$v = v_0 + \sum_{i=1}^{n} x_i v_i.$$

12.2 Quadratische Funktionen

Definition 12.3 *Eine Abbildung* $Q : V \to K$ *heisst* ***quadratische Funktion****, falls sie von der Form*

$$Q(v) = q(v - v_0) + l(v - v_0) + c$$

ist, wobei $v_0 \in V$*,* q *eine quadratische Form,* $l \in V^*$ *und* $c \in K$ *ist.*

q nennt man den quadratischen Teil und l den linearen Teil von Q bezüglich v_0. Offenbar ist $c = Q(v_0)$. Wie sieht die Darstellung von Q bezüglich eines anderen Punktes v_0' aus? Man rechnet nach:

Lemma 12.2 *Sei* Q *wie oben und* $v_0' \in V$*, dann ist*

$$Q(v) = q(v - v_0') + l'(v - v_0') + c'$$

mit

$$c' = Q(v_0') \quad \textit{und} \quad l' = l + 2\varphi(\,.\,, v_0' - v_0).$$

Hierbei ist φ die zu q gehörende symmetrische Bilinearform:

$$q(v) = \varphi(v,v) \quad \text{und} \quad \varphi(v,w) = \frac{1}{2}[q(v+w) - q(v) - q(w)].$$

Der quadratische Teil von Q ist also unabhängig von der Wahl von v_0, während der lineare und der konstante Teil transformiert werden. Punkte, bezüglich denen der lineare Teil verschwindet, sind offensichtlich ausgezeichnet:

Definition 12.4 *Q sei eine quadratische Funktion mit quadratischem Teil q. $v_0 \in V$ heisst **Zentralpunkt** von Q, falls*

$$Q(v) = q(v - v_0) + Q(v_0) \quad \textit{für alle } v \in V$$

*ist. Die Menge aller Zentralpunkte von Q heisst das **Zentrum** von Q.*

Bemerkung 12.4 *v_0 ist genau dann ein Zentralpunkt von Q, wenn $Q(v) = Q(v_0 - (v - v_0))$ für alle $v \in V$ ist. Denn $Q(v) - Q(v_0 - (v - v_0)) = 2l(v - v_0)$ (weil $q(v - v_0) = q(v_0 - v)$), und das verschwindet genau dann, wenn v_0 ein Zentralpunkt ist. Die Gleichung $Q(v) = Q(v_0 - (v - v_0))$ für alle $v \in V$ bedeutet, dass Q symmetrisch bezüglich Punktspiegelung an v_0 ist.*

Wir untersuchen nun, wie das Zentrum einer quadratischen Funktion aussehen kann. Zur Erinnerung: Eine quadratische Form q ist nichtdegeneriert genau dann, wenn die zugehörige symmetrische Bilinearform φ nichtdegeneriert ist, d.h. $\ker \varphi = \{0\}$, d.h. $\varphi(v,w) = 0$ für alle $v \in V$ impliziert $w = 0$. Es ist $\ker q := \ker \varphi = \ker(G)$ und $\operatorname{rang} q := \operatorname{rang}(G)$ $(= \dim(V) - \dim(\ker(G)))$, wobei G die Grammatrix von φ ist.

Satz 12.1 *Q sei eine quadratische Funktion mit quadratischem Teil q.*
a) Falls q nichtdegeneriert ist, gibt es genau einen Zentralpunkt von Q.
b) Falls q degeneriert ist, ist das Zentrum von Q entweder leer oder ein affiner Teilraum $v_0 + U$ von V mit $U = \ker q$.

Beweis. Sei zunächst v_0 ein beliebiger Punkt von V und $Q(v) = q(v - v_0) + l(v - v_0) + c$. Gemäss Lemma 12.2 ist v_0' genau dann ein Zentralpunkt von Q, wenn $l = -2\varphi(\,.\,, v_0' - v_0)$ ist. In der Aufgabe 3 vom Übungsblatt 8 haben wir gezeigt, dass die Abbildung $h_\varphi : V \to V^*$, $h_\varphi(v) = \varphi(\,.\,, v)$ genau dann ein Isomorphismus ist, wenn φ nichtdegeneriert ist.

a) Wenn φ nichtdegeneriert ist, gibt es genau ein $u_0 \in V$ mit $\varphi(\,.\,, u_0) = -l/2$. $v_0' = u_0 + v_0$ ist also der eindeutige Zentralpunkt.

b) Wenn φ degeneriert ist, ist h_φ nicht bijektiv, und es gibt zwei Fälle: Entweder $-l/2 \notin \operatorname{im}(h_\varphi)$, dann gibt es keinen Zentralpunkt, oder $-l/2 \in \operatorname{im}(h_\varphi)$. Dann gibt es $u \in V$ mit $\varphi(\,.\,, u) = -l/2$, und $v_0' = u + v_0$ ist ein Zentralpunkt. Seien v_0' und v_0'' Zentralpunkte, d.h. $-l/2 = \varphi(\,.\,, v_0' - v_0) = \varphi(\,.\,, v_0'' - v_0)$. Dann ist $\varphi(\,.\,, v_0' - v_0'') = 0$ und folglich $v_0' - v_0'' \in \ker \varphi$. Und umgekehrt, wenn v_0'

Zentralpunkt und $v_0'' \in v_0' + \ker\varphi$ ist, dann ist $\varphi(\,.\,, v_0'' - v_0) = \varphi(\,.\,, v_0' + k - v_0) = \varphi(\,.\,, k) + \varphi(\,.\,, v_0' - v_0) = 0 - l/2$ mit $k = v_0'' - v_0' \in \ker\varphi$, also ist auch v_0'' ein Zentralpunkt. Folglich ist das Zentrum von Q ein affiner Teilraum $v_0' + \ker\varphi$. ■

Wir untersuchen als nächstes das Problem der „Normalformen“ oder der „kanonischen Formen“ für quadratische Funktionen: Es geht dabei darum, ein affines Koordinatensystem $(v_0, v_1 \ldots, v_n)$ zu finden, bezüglich dem eine quadratische Funktion eine möglichst einfache Form hat. Sind $(x_1, \ldots, x_n) \in K^n$ die affinen Koordinaten von $v \in V$, d.h. $v = v_0 + \sum_{i=1}^n x_i v_i$, so schreiben wir auch $Q(x_1, \ldots, x_n)$ für $Q(v)$.

Satz 12.2 *Q sei eine quadratische Funktion. Dann gibt es ein affines Koordinatensystem, in dem Q eine der folgenden Formen annimmt:*
a) Wenn der quadratische Teil q nichtdegeneriert ist, ist

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^n \lambda_i x_i^2 + c, \quad \lambda_i \in K \setminus \{0\}, i = 1, \ldots, n, \quad c \in K.$$

b) Wenn q degeneriert, $\operatorname{rang} q = r$ *und das Zentrum von Q nichtleer ist, ist*

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^r \lambda_i x_i^2 + c, \quad \lambda_i \in K \setminus \{0\}, i = 1, \ldots, r, \quad c \in K.$$

c) Wenn q degeneriert, $\operatorname{rang} q = r$ *und das Zentrum von Q leer ist, ist*

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^r \lambda_i x_i^2 + x_{r+1}, \quad \lambda_i \in K \setminus \{0\}, i = 1, \ldots, r.$$

Beweis. a) und b): Wähle für v_0 den bzw. einen Zentralpunkt von Q, dann ist $Q(v) = q(v - v_0) + c$. Wähle für $(v_1 \ldots, v_n)$ eine Basis von V, die q diagonalisiert gemäss Satz 10.2 und Korollar 10.3.

c) Wähle für v_0 zunächst einen beliebigen Punkt in V und die Basis $(v_1 \ldots, v_n)$ so, dass der quadratische Teil von Q diagonal ist:

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^r \lambda_i x_i^2 + \sum_{i=1}^n \mu_i x_i + c \quad \text{mit} \quad \mu_i = l(v_i).$$

Es gibt dann mindestens ein $j > r$ mit $\mu_j \neq 0$, denn sonst wäre $Q(x_1, \ldots, x_n) = \sum_{i=1}^r \lambda_i (x_i + \frac{\mu_i}{2\lambda_i})^2 + c'$, und der Punkt $v_0 - \sum_{i=1}^r \frac{\mu_i}{2\lambda_i} v_i$ wäre ein Zentralpunkt im Widerspruch zur Voraussetzung, dass das Zentrum von Q leer ist. Folglich ist $(v_1^*, \ldots, v_r^*, l)$ linear unabhängig in V^*. Ergänze das zu einer Basis von V^* und betrachte die duale Basis $(\widetilde{v_1}, \ldots, \widetilde{v_n})$ von V.

In dem affinen Koordinatensystem $(v_0, \widetilde{v_1}, \ldots, \widetilde{v_n})$ hat $v \in V$ die Darstellung $v = v_0 + \sum_{i=1}^n \widetilde{x_i} \widetilde{v_i}$. Es gilt $l(\widetilde{v_i}) = 0$ für $i \neq r+1$ und $l(\widetilde{v_{r+1}}) = 1$. Folglich ist

$l(v - v_0) = \widetilde{x_{r+1}}$. Für den quadratischen Teil gilt

$$q(v - v_0) = \sum_{i,j=1}^{n} \widetilde{x}_i \widetilde{x}_j \varphi(\widetilde{v}_i, \widetilde{v}_j).$$

Stelle die Vektoren $\widetilde{v}_i$ in der alten Basis dar: $\widetilde{v}_i = \sum_{j=1}^{n} a_{ji} v_j$. Dann ist

$$v_k^*(\widetilde{v}_i) = \delta_{ki} = \sum_{j=1}^{n} a_{ji} v_k^*(v_j) = a_{ki} \quad \text{für } 1 \leq k \leq r \text{ und } 1 \leq i \leq n.$$

Also ist für $1 \leq i \leq r$ $\widetilde{v}_i = v_i + \sum_{j=r+1}^{n} a_{ji} v_j$ und für $r < i \leq n$ ist $\widetilde{v}_i = \sum_{j=r+1}^{n} a_{ji} v_j$. Weil $\sum_{j=r+1}^{n} a_{ji} v_j \in \ker \varphi$ ist, gilt $\varphi(\widetilde{v}_i, \widetilde{v}_j) = \varphi(v_i, v_j) = \lambda_i \delta_{ij}$ für $1 \leq i, j \leq r$ und $\varphi(\widetilde{v}_i, \widetilde{v}_j) = 0$ für $i > r$ oder $j > r$. Insgesamt haben wir nun

$$Q(\widetilde{x}_1, \ldots, \widetilde{x_n}) = \sum_{i=1}^{r} \lambda_i \widetilde{x}_i^{\,2} + \widetilde{x_{r+1}} + c.$$

Es gibt einen Punkt mit $Q = 0$, z.B. den Punkt $(0, \ldots, 0, -c, 0, \ldots 0)$. Wenn man die Konstruktion an diesem Punkt beginnt, erhält man die gewünschte Form mit $c = 0$. ■

Zur Eindeutigkeit der kanonischen Form gilt in den verschiedenen Fällen:

a) $(0, \ldots, 0)$ ist der eindeutige Zentralpunkt von Q, c ist eindeutig bestimmt als der Wert von Q im Zentrum. Die Willkür in der Wahl der Basis, die q diagonalisiert, sowie der Koeffizienten λ_i ist genau wie in Abschnitt 10.2 für die Normalform einer symmetrischen Bilinearform diskutiert. Insbesondere kann man für $K = \mathbb{R}$ die λ_i in $\{\pm 1\}$ wählen, und die Anzahl der $+1$ und der -1 ist eine Invariante. Für $K = \mathbb{C}$ kann man $\lambda_i = 1$ setzen.

b) Der Koordinatenursprung kann irgendwo ins (mindestens eindimensionale) Zentrum gelegt werden, aber c ist immer noch eindeutig bestimmt: Seien v_0 und v_0' Zentralpunkte, dann gilt $Q(v) = q(v - v_0) + c$, $c = Q(v_0)$, und $Q(v_0') = q(v_0' - v_0) + c = c$, weil $v_0' - v_0 \in \ker q$ liegt. Für den quadratischen Teil gilt dasselbe wie im Fall a) mit $\lambda_i = 0$ für $i > r$.

c) Jeder Punkt, an dem Q verschwindet, kann als Koordinatenursprung gewählt werden, und für den quadratischen Teil gilt dasselbe wie bei b).

12.3 Affine Quadriken

Definition 12.5 *Eine **affine Quadrik** ist eine Menge $\{v \in V : Q(v) = 0\}$, wobei Q eine quadratische Funktion auf V ist.*

Beispiel 12.3 *Die Normalformen von nichtleeren affinen Quadriken im $\mathbb{R}^2$ lassen sich folgendermassen aufgliedern:*

a)	$x^2+y^2=0$	*Punkt*
	$x^2+y^2=1$	*Kreis*
	$x^2-y^2=0$	*2 sich schneidende Geraden*
	$x^2-y^2=1$	*Hyperbel*
b) $r=1$	$x^2=0$	*Gerade*
	$x^2=1$	*2 parallele Geraden*
$r=0$	$0=0$	*Ebene* $\mathbb{R}^2$
c) $r=1$	$x^2+y=0$	*Parabel*
$r=0$	$x=0$	*Gerade*

Wir untersuchen nun die Frage, ob verschiedene quadratische Funktionen Q dieselbe Quadrik definieren können. Natürlich ist Q immer nur bis auf Multiplikation mit einem Körperelement $\neq 0$ eindeutig: $Q(v)=0 \Leftrightarrow \lambda Q(v)=0$ für $\lambda \in K \setminus \{0\}$. Wir haben in Beispiel 12.3 aber auch schon Fälle, wo quadratische Funktionen, die nicht skalare Vielfache voneinander sind, dieselbe Quadrik erzeugen: $\{(x,y)\in\mathbb{R}^2 : x^2=0\} = \{(x,y)\in\mathbb{R}^2 : x=0\}$. Noch so ein Beispiel: Die Gleichung $\sum_{i=1}^r x_i^2 = 0$ im $\mathbb{R}^n$ ist äquivalent zu $x_1=\cdots=x_r=0$, und für $r>1$ gibt es viele quadratische Funktionen, die dieselbe Quadrik erzeugen, aber nicht proportional zueinander sind, z.B. $\sum_{i=1}^r \lambda_i x_i^2 = 0$ für beliebige $\lambda_i > 0$, die nicht alle gleich sind. In all diesen Fällen ist die Quadrik ein affiner Teilraum. Tatsächlich ist für $K=\mathbb{R}$ Q bis auf Multiplikation mit $\lambda\neq 0$ eindeutig, wenn die Quadrik kein affiner Teilraum ist:

Satz 12.3 *Eine affine Quadrik X in einem reellen Vektorraum V sei gegeben durch quadratische Funktionen Q_1 und Q_2:*

$$X = \{v\in V : Q_1(v)=0\} = \{v\in V : Q_2(v)=0\}.$$

X sei kein affiner Teilraum von V. Dann gibt es ein $\lambda\in\mathbb{R}$ mit $Q_1=\lambda Q_2$.

Beweis. X ist kein affiner Teilraum von V, also gibt es gemäss Lemma 12.1 zwei verschiedene Punkte $a,b\in X$ mit der Eigenschaft, dass die Gerade durch a und b nicht vollständig in X enthalten ist. Führe ein affines Koordinatensystem $(a,v_1,\ldots,v_n)$ mit $v_n=b-a$ ein. Damit ist

$$\begin{aligned} Q_1(x_1,\ldots,x_n) &= q_1\left(\sum_{i=1}^n x_i v_i\right) + l_1\left(\sum_{i=1}^n x_i v_i\right) \\ &= \lambda x_n^2 + f_1(x_1,\ldots,x_{n-1})x_n + g_1(x_1,\ldots,x_{n-1}), \end{aligned}$$

($c = Q_1(a) = 0$), wobei $\lambda = q_1(v_n)$, f_1 ein Polynom in $x_1,\ldots,x_{n-1}$ vom Grad ≤ 1 und g_1 ein Polynom in $x_1,\ldots,x_{n-1}$ vom Grad ≤ 2 ist. a hat die affinen Koordinaten $(0,\ldots,0)$, b hat die affinen Koordinaten $(0,\ldots,0,1)$, und die Gerade durch a und b ist die Menge der Punkte mit den affinen Koordinaten $(0,\ldots,0,t)$, $t\in\mathbb{R}$. $Q_1(a)=0$ impliziert $g_1(0)=0$, und $Q_1(b)=0$ impliziert $f_1(0)=-\lambda$. Auf

der Geraden durch a und b nimmt Q_1 die Werte $Q_1(0,\ldots,0,t) = \lambda t^2 - \lambda t$ an. Dies ist nicht für alle $t \in \mathbb{R}$ gleich 0, also muss $\lambda \neq 0$ sein, und wir können $\lambda = 1$ setzen. Analog ist

$$Q_2(x_1,\ldots,x_n) = x_n^2 + f_2(x_1,\ldots,x_{n-1})x_n + g_2(x_1,\ldots,x_{n-1}),$$

wobei f_2 ein Polynom vom Grad ≤ 1 und g_2 ein Polynom vom Grad ≤ 2 ist mit $f_2(0) = -1$ und $g_2(0) = 0$.

Q_1 und Q_2 definieren dieselbe affine Quadrik, haben also dieselben Nullstellenmengen. Wir wollen zeigen, dass $Q_1 = Q_2$ ist. Die Lösungen der quadratischen Gleichungen $Q_1 = 0$ bzw. $Q_2 = 0$ sind

$$x_n = -\frac{1}{2}f_i(x_1,\ldots,x_{n-1}) \pm \frac{1}{2}\sqrt{f_i^2(x_1,\ldots,x_{n-1}) - 4g_i(x_1,\ldots,x_{n-1})}, \quad i = 1,2.$$

Bei $(x_1,\ldots,x_{n-1}) = (0,\ldots,0)$ sind $x_n = 0$ und $x_n = 1$ die beiden Lösungen dieser Gleichungen, die in einer Umgebung von $(0,\ldots,0)$ stetig von $(x_1,\ldots,x_{n-1})$ abhängen. Folglich gilt in einer Umgebung von $(0,\ldots,0)$:

$$-f_1 + \sqrt{f_1^2 - 4g_1} = -f_2 + \sqrt{f_2^2 - 4g_2}$$

und

$$-f_1 - \sqrt{f_1^2 - 4g_1} = -f_2 - \sqrt{f_2^2 - 4g_2}.$$

Addition dieser Gleichungen ergibt $f_1 = f_2$, und Subtraktion liefert dann $g_1 = g_2$. Dies gilt zunächst nur in einer Umgebung von $(0,\ldots,0)$. Indem man nun in die allgemeine Form von f_i, $f_i(x_1,\ldots,x_{n-1}) = a_{i0} + \sum_{j=1}^{n-1} a_{ij}x_j$ spezielle Punkte aus dieser Umgebung einsetzt, erhält man die Gleichheit aller Koeffizienten a_{ij} und damit $f_1 = f_2$ auf ganz $\mathbb{R}^{n-1}$. Z.B. $x = (0,\ldots,0) \Rightarrow a_{10} = a_{20}$; $x = (0,\ldots,0,\epsilon,0,\ldots,0)$ mit $x_i = \epsilon$ klein genug $\Rightarrow a_{1i} = a_{2i}$. Analog zeigt man $g_1 = g_2$ auf ganz $\mathbb{R}^{n-1}$ und damit gilt $Q_1 = Q_2$ auf V. ■