Lineare Algebra und Geometrie für LehramtskandidatInnen

(Kapitel 6 – 9)

Wintersemester 2010/11

Andreas Čap

Fakultät für Mathematik, Universität Wien, Nordbergstrasse 15, A–1090 Wien

E-mail address: Andreas.Cap@esi.ac.at

Inhaltsverzeichnis

KAPITEL 6

Determinanten

Als Motivation für die folgenden Überlegungen, erinnern wir uns an einige Tatsachen über den Zusammenhang zwischen Matrizen und linearen Abbildungen, die wir in Kapitel 4 der Vorlesung "Einführung in die Lineare Algebra und Geometrie" kennen gelernt haben. Seien V und W endlichdimensionale Vektorräume über einem Körper $\mathbb{K}$ und sei $f : V \to W$ eine lineare Abbildung. Wählt man eine Basis $\mathcal{B} = \{v_1, \dots, v_n\}$ für V und eine Basis $\mathcal{C} = \{w_1, \dots, w_m\}$ für W, dann kann man die lineare Abbildung f durch ihre Matrixdarstellung $[f]^{\mathcal{B}}_{\mathcal{C}} \in M_{m,n}(\mathbb{K})$ beschreiben. Für jedes Element $v \in V$ gilt nämlich $[f(v)]_{\mathcal{C}} = [f]^{\mathcal{B}}_{\mathcal{C}}[v]_{\mathcal{B}}$, wobei $[v]_{\mathcal{B}}$ der *Koordinatenvektor* von v bezüglich $\mathcal{B}$ und $[f(v)]_{\mathcal{C}}$ der Koordinatenvektor von $f(v)$ bezüglich $\mathcal{C}$ ist. Ist $v = a_1v_1 + \dots + a_nv_n$ die (eindeutige) Darstellung von v als Linearkombination der Elemente von $\mathcal{B}$, dann ist $[v]_{\mathcal{B}} = (a_1, \dots, a_n)$. Insbesondere erhält man im Fall $V = \mathbb{K}^n$ und $W = \mathbb{K}^m$ genau den üblichen Zusammenhang zwischen linearen Abbildungen und Matrizen (siehe Kapitel 3 von [**1**]) wenn man für $\mathcal{B}$ und $\mathcal{C}$ jeweils die Standardbasis verwendet.

Es ist auch leicht zu beschreiben, wie die Matrixdarstellungen bezüglich verschiedener Basen zusammenhängen. Ist $\tilde{\mathcal{B}}$ eine weitere Basis für V, dann kann man die Matrizen zum Basiswechsel bilden, die man in der Notation von oben als $[\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}}$ bzw $[\mathrm{id}]^{\tilde{\mathcal{B}}}_{\mathcal{B}} = ([\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}})^{-1}$ schreiben kann. Analog gibt es zu einer weiteren Basis $\tilde{\mathcal{C}}$ für W die entsprechenden Basiswechselmatrizen, und es gilt

$$[f]^{\tilde{\mathcal{B}}}_{\tilde{\mathcal{C}}} = [\mathrm{id}]^{\mathcal{C}}_{\tilde{\mathcal{C}}}[f]^{\mathcal{B}}_{\mathcal{C}}[\mathrm{id}]^{\tilde{\mathcal{B}}}_{\mathcal{B}} = [\mathrm{id}]^{\mathcal{C}}_{\tilde{\mathcal{C}}}[f]^{\mathcal{B}}_{\mathcal{C}}([\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}})^{-1}.$$

(Wir werden in Kürze sehen, warum die zweite Schreibweise die natürlichere ist.) Schließlich ist noch wichtig zu bemerken, dass für eine gegebene Basis $\mathcal{B}$ für V *jede* invertierbare $n \times n$–Matrix als $[\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}}$ für eine geeignete Basis $\tilde{\mathcal{B}}$ von V geschrieben werden kann.

Damit sieht man, dass für eine gegeben Matrixdarstellung $A \in M_{m,n}(\mathbb{K})$ einer linearen Abbildung f, die Matrixdarstellungen von f bezüglich beliebiger Basen genau die Matrizen der Form SAT^{-1} für invertierbare Matrizen $S \in M_m(\mathbb{K})$ und $T \in M_n(\mathbb{K})$ sind. Entsprechend nennt man zwei rechteckige Matrizen $A, B \in M_{m,n}(\mathbb{K})$ *ähnlich*, wenn es invertierbare Matrizen S und T wie oben gibt, sodass $B = SAT^{-1}$ gilt, siehe Abschnitt 4.18 in [**1**].

Aus diesen Überlegungen können wir einerseits erkennen, wie man Matrizen zum Studium linearer Abbildungen verwenden kann. Jede Eigenschaft einer Matrix, die sich automatisch auf alle ähnlichen Matrizen überträgt kann man als Eigenschaft von linearen Abbildungen betrachten. Um diese Eigenschaft für eine Abbildung f zu überprüfen genügt es dann, sie für eine Matrixdarstellung von f zu verifizieren. Umgekehrt kann man natürlich fragen, wie die einfachste mögliche Matrixdarstellung für eine gegeben lineare Abbildung f aussieht. Wir wissen aus Abschnitt 4.18 von [**1**], dass Ähnlichkeit von Matrizen eine Äquivalenzrelation ist und die suche nach einer möglich einfachen Matrixdarstellung bedeutet, dass man in jeder Äquivalenzklasse einen möglichst einfachen Repräsentanten angeben möchte.

Tatsächlich haben wir diese beiden Probleme in Satz 4.18 von [**1**] einfach lösen können. Einerseits sind zwei Matrizen genau dann ähnlich, wenn sie den gleichen Rang haben. Somit ist der Rang die einzige wesentliche Invariante einer linearen Abbildung zwischen zwei verschiedenen endlichdimensionalen Vektorräumen. Andererseits kann man leicht einen einfachen Repräsentanten für die Matrizen mit Rang r angeben, zum Beispiel die Matrix $\mathbb{J}_r = (a_{ij})$ für die $a_{11} = a_{22} = \dots = a_{rr} = 1$ gilt, während alle anderen Eintragungen Null sind. Wir haben damals schon angedeutet, dass die entsprechenden Probleme für lineare Abbildungen $f : V \to V$, also von einem Vektorraum auf sich selbst, sehr viel schwieriger sind. Tatsächlich werden uns die beiden obigen Fragen in diesem Fall einen Gutteil des Semesters beschäftigen.

6.1. Ähnlichkeit für quadratische Matrizen. Der wesentliche Unterschied im Fall linearer Abbildungen $f : V \to V$ ist natürlich, dass wir uns auf Matrixdarstellungen bezüglich *einer* Basis von von V einschränken können und nicht zwei verschiedene Basen für V verwenden. Für eine Basis $\mathcal{B} = \{v_1, \dots, v_n\}$ von V schreiben wir ab sofort $[f]_{\mathcal{B}}$ statt $[f]^{\mathcal{B}}_{\mathcal{B}}$, und sofern nicht explizit anderes gesagt wird, werden wir uns ab sofort nur noch für solche Matrixdarstellungen interessieren.

Ist $\tilde{\mathcal{B}}$ eine weitere Basis für V, dann erhalten wir die invertierbare Matrix $[\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}}$ und von oben lesen wir ab, dass

$$[f]_{\tilde{\mathcal{B}}} = [\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}}[f]_{\mathcal{B}}([\mathrm{id}]^{\mathcal{B}}_{\tilde{\mathcal{B}}})^{-1}$$

gilt. Im Gegensatz zu vorher muss man also von links mit einer beliebigen invertierbaren Matrix und von rechts mit ihrer Inversen multiplizieren und nicht mit zwei beliebigen invertierbaren Matrizen. Entsprechend adaptiert man den Begriff von Ähnlichkeit für quadratische Matrizen:

Definition 6.1. Sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Zwei quadratische Matrizen $A, B \in M_n(\mathbb{K})$ heißen *ähnlich*, wenn es eine invertierbare Matrix $T \in M_n(\mathbb{K})$ gibt, sodass $B = TAT^{-1}$ gilt. In diesem Fall schreibt man $A \sim B$.

Sofern nicht explizit anderes gesagt wird, werden wir ab sofort nur noch diesen Begriff von Ähnlichkeit und nicht den “alten” Begriff, der auch für rechteckige Matrizen Sinn macht, verwenden.

Die grundlegenden Eigenschaften folgen nun sofort aus bereits bekannten Resultaten bzw. werden ganz analog zu diesen bewiesen:

Proposition 6.1. *(1) Sei V ein endlichdimensionaler Vektorraum über $\mathbb{K}$, $f : V \to V$ eine lineare Abbildung, und $A \in M_n(\mathbb{K})$ eine Matrixdarstellung für f, d.h. $A = [f]_{\mathcal{B}}$ für eine Basis $\mathcal{B}$ von V.*

Dann ist eine Matrix $B \in M_n(\mathbb{K})$ genau dann eine Matrixdarstellung von f, wenn sie ähnlich zu A im Sinne von Definition 6.1 ist.

(2) Ähnlichkeit quadratischer Matrizen ist eine Äquivalenzrelation. Ähnliche Matrizen haben den gleichen Rang, es gibt aber Matrizen mit gleichem Rang, die nicht zueinander ähnlich sind.

Beweis. (1) folgt sofort aus den obigen Überlegungen und Lemma 4.18 von [**1**], und den Anfang von (2) beweist man völlig analog zu Bemerkung 4.18 (2) aus [**1**]. Die Details auszuführen ist eine gute Übung. Dass ähnliche Matrizen gleichen Rang haben folgt aus Satz 4.18 von [**1**]. Umgekehrt betrachten wir $\mathbb{K} = \mathbb{R}$ und für $t \in \mathbb{R}$ die Matrix $t\mathbb{I}_n$, wobei $\mathbb{I}_n$ die Einheitsmatrix bezeichnet. Ist $T \in M_n(\mathbb{R})$ invertierbar, dann ist $T(t\mathbb{I}_n)T^{-1} = tT\mathbb{I}_nT^{-1} = tTT^{-1} = t\mathbb{I}_n$. Somit sind für $t \neq s$ die Matrizen $t\mathbb{I}_n$ und $s\mathbb{I}_n$ nicht ähnlich, obwohl sie für $t, s \neq 0$ beide Rang n haben. $\square$

Bemerkung 6.1. (1) Analog zu den Überlegungen von oben können wir nun lineare Abbildungen $f : V \to V$ über ihre Matrixdarstellungen studieren. Man kann einfach jede Eigenschaft quadratischer Matrizen, die sich automatisch auf ähnliche Matrizen überträgt, als Eigenschaft von linearen Abbildungen auffassen. Umgekehrt kann man versuchen in jeder Äquivalenzklasse ähnlicher Matrizen einen möglichst einfachen Repräsentanten zu finden, eine sogenannte *Normalform*. Diese stellt dann eine ausgezeichnete "einfache" Matrixdarstellung für eine Klasse von linearen Abbildungen dar. Wie schon bemerkt, sind diese Fragen hier wesentlich interessanter und schwieriger als im Fall von Abbildungen zwischen verschiedenen Vektorräumen und sie werden uns auf längere Zeit beschäftigen.

(2) Im letzten Semester haben elementare Zeilenoperationen eine zentrale Rolle gespielt, insbesondere beim Studium linearer Gleichungssysteme. Dabei war es wichtig, dass jede Folge elementarer Zeilenoperationen durch Multiplikation von links mit einer invertierbaren Matrix dargestellt werden kann. Damit führt jede Folge elementarer Zeilenoperationen von einer Matrix A zu einer Matrix, die im "alten" Sinn ähnlich zu A ist. Das gilt aber für den neuen Begriff von Ähnlichkeit aus Definition 6.1 *nicht*! Daher werden elementare Zeilenoperationen im weiteren keine so große Rolle mehr spielen.

Existenz der Determinante

Der erste Schritt zum Verständnis quadratischer Matrizen ist der Begriff der Determinante einer Matrix. Um den allgemeinen Begriff zu motivieren besprechen wir zunächst den Fall der Determinante von 2×2–Matrizen. In diesem Fall ist der Begriff schon aus der Schule bekannt und man kann alle wesentlichen Eigenschaften ganz einfach nachrechnen.

6.2. Die Determinante von 2×2–Matrizen. Sei $\mathbb{K}$ ein Körper und $M_2(\mathbb{K})$ der Raum der 2×2–Matrizen über $\mathbb{K}$. Dann definieren wir die *Determinantenfunktion* $\det : M_2(\mathbb{K}) \to \mathbb{K}$ durch $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc$. Wie schon im ersten Teil der Vorlesung ist es auch hier oft günstig, die Matrix als Familie ihrer Spaltenvektoren zu betrachten. Wir werden daher det auch als Funktion $\mathbb{K}^2 \times \mathbb{K}^2 \to \mathbb{K}$ betrachten und als $\det(v_1, v_2)$ für $v_1, v_2 \in \mathbb{K}^2$ schreiben. Die grundlegenden Eigenschaften der Determinantenfunktion können wir nun sofort ablesen:

(1) Für $r \in \mathbb{K}$ gilt $\det(rv_1, v_2) = \det(v_1, rv_2) = r\det(v_1, v_2)$ und für $v_1', v_2' \in \mathbb{K}^2$ gelten $\det(v_1+v_1', v_2) = \det(v_1, v_2)+\det(v_1', v_2)$ sowie $\det(v_1, v_2+v_2') = \det(v_1, v_2)+\det(v_1, v_2')$. Man sagt, die Determinante ist *linear in jeder Spalte*. Die Bedingungen besagen ja gerade, dass $v_1 \mapsto \det(v_1, v_2)$ für fixes v_2 und $v_2 \mapsto \det(v_1, v_2)$ für fixes v_1 lineare Abbildungen $\mathbb{K}^2 \to \mathbb{K}$ sind.
(2) Für beliebiges $v \in \mathbb{K}^2$ ist $\det(v, v) = 0$. Man sagt, die Determinante ist *alternierend*.
(3) Für die Einheitsmatrix (bzw. für die Elemente der Standardbasis) gilt $\det(\mathbb{I}) = \det(e_1, e_2) = 1$. Man sagt, die Determinante ist *normiert*.

Wie schon aus der Schule bekannt kann man im Fall $\mathbb{K} = \mathbb{R}$ den Betrag der Determinante als Fläche des von den Spaltenvektoren aufgespannten Parallelogramms interpretieren.

Die erste zentrale Eigenschaft der Determinante ist ihr Bezug zur Invertierbarkeit, der im Fall der hier ganz einfach explizit nachgerechnet werden kann. Es gilt nämlich

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = (ad-bc)\mathbb{I}_2.$$

Ist also $A \in M_2(\mathbb{K})$ so, dass $\det(A) \neq 0$ gilt, dann ist A invertierbar, und wir können die inverse Matrix einfach angeben. Umgekehrt zeigt eine direkte Rechnung, dass für $A, B \in M_2(\mathbb{K})$ die Gleichung $\det(AB) = \det(A)\det(B)$ gilt. Ist A invertierbar, dann gibt es eine Matrix B, sodass $AB = BA = \mathbb{I}$ gilt. Damit ist aber $\det(A)\det(B) = \det(\mathbb{I}) = 1$, also insbesondere $\det(A) \neq 0$.

Es ist bemerkenswert, dass diese Rechnung nicht nur über Körpern funktioniert sondern ganz allgemein über kommutativen Ringen funktioniert. Man muss dann nur statt $\det(A) \neq 0$ verlangen, dass es ein Element r gibt, sodass $r\det(A) = 1$ gilt. Damit kann man dieses Kriterium insbesondere über den ganzen Zahlen $\mathbb{Z}$ verwenden. Wir sehen also etwa, dass eine 2×2–Matrix mit Eintragungen in $\mathbb{Z}$ genau eine inverse Matrix mit Eintragungen aus $\mathbb{Z}$ besitzt, wenn ihre Determinante diese Bedingung erfüllt. In $\mathbb{Z}$ bedeutet das aber gerade, dass $\det(A) = \pm 1$ gelten muss. Tatsächlich kann man die ganze Theorie der Determinanten ohne größere Änderungen über kommutativen Ringen mit Einselement entwickeln, wir werden das aber nicht tun.

Nehmen wir nun an, dass $A \in M_2(\mathbb{K})$ invertierbar ist, also $\det(A) \neq 0$ gilt. Betrachten wir nun das lineare Gleichungssystem $Ax = y$, dann ist $x = A^{-1}y$ für jedes $y \in \mathbb{K}^2$ die eindeutige Lösung. Ist $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, dann erhalten wir mit der Formel für A^{-1} von oben gerade $x_1 = \det(A)^{-1}(dy_1 - by_2)$ und $x_2 = \det(A)^{-1}(-cy_1 + ay_2)$. Bezeichnen wir die Spaltenvektoren von A mit v_1 und v_2, dann kann man das als $x_1 = \det(A)^{-1}\det(y, v_2)$ und $x_2 = \det(A)^{-1}\det(v_1, y)$ schreiben. Das ist der einfachste Fall der sogenannten *Cramer'schen Regel*, die explizite Lösungsformeln für lineare Gleichungssysteme liefert.

Betrachten wir schließlich ähnliche Matrizen $A, B \in M_2(\mathbb{K})$. Dann gibt es nach Definition eine invertierbare Matrix $T \in M_2(\mathbb{K})$, sodass $B = TAT^{-1}$ gilt. von oben wissen wir, dass $\det(T)\det(T^{-1}) = 1$ gilt. Damit erhalten wir aber aus der obigen Formel für Determinanten von Produkten $\det(B) = \det(T)\det(A)\det(T^{-1}) = \det(A)$, also haben ähnliche Matrizen die selbe Determinante. Damit kann man aber die Determinante für lineare Abbildungen von einem zweidimensionalen Vektorraum auf sich selbst als die Determinante einer beliebigen Matrixdarstellung definieren.

6.3. Determinantenfunktionen. Sei $\mathbb{K}$ ein Körper. Wie in 6.2 werden wir weiterhin eine Matrix auch als Familie ihrer Spaltenvektoren betrachten, also den Raum $M_n(\mathbb{K})$ der $n \times n$–Matrizen über $\mathbb{K}$ auch als $\mathbb{K}^n \times \ldots \times \mathbb{K}^n$ (n Faktoren) betrachten.

Definition 6.3. (1) Eine Funktion $F : M_n(\mathbb{K}) = \mathbb{K}^n \times \ldots \times \mathbb{K}^n \to \mathbb{K}$ heißt eine *Determinantenfunktion* wenn sie folgende Bedingungen erfüllt:

- F ist linear in jeder Spalte, d.h. für jedes $i = 1, \ldots, n$ und beliebige fixe Elemente v_j für $j \neq i$ ist $v_i \mapsto F(v_1, \ldots, v_i, \ldots, v_n)$ eine lineare Abbildung $\mathbb{K}^n \to \mathbb{K}$.
- Ist $v_i = v_j$ für ein $i \neq j$, dann ist $F(v_1, \ldots, v_n) = 0$.

(2) Eine Determinantenfunktion $F : M_n(\mathbb{K}) \to \mathbb{K}$ heißt normiert, wenn $F(\mathbb{I}_n) = F(e_1, \ldots, e_n) = 1$ gilt.

Bemerkung 6.3. (1) Die Funktion $\det : M_2(\mathbb{K}) \to \mathbb{K}$ aus 6.2 ist eine normierte Determinantenfunktion. Für $n > 2$ müssen wir erst beweisen, dass Determinantenfunktionen überhaupt existieren.

(2) Zu den elementaren Zeilenoperationen aus Abschnitt 3.6 von [**1**] gibt es natürlich analoge *elementare Spaltenoperationen*. Diese sind gegeben, indem man zwei Spalten vertauscht, eine Spalte mit einem Skalar ungleich Null multipliziert, oder zu einer Spalte ein beliebiges Vielfaches einer anderen Spalte addiert. Aus der Definition ergibt sich sofort, wie sich eine Determinantenfunktion F unter diesen Operationen verhält:

Addiert man zur i–ten Spalte das r–fache der j–ten Spalte, dann erhält man wegen der Linearität in der i–ten Spalte

$$F(v_1, \dots, v_i + rv_j, \dots, v_j, \dots, v_n) = F(v_1, \dots, v_n) + rF(v_1, \dots, v_j, \dots, v_j, \dots, v_n)$$

und der zweite Summand verschwindet, weil zwei Spalten gleich sind. Bei dieser Art von Spaltenoperationen bleibt also der Wert jeder Determinantenfunktion unverändert. Multipliziert man eine Spalte mit einem Skalar $r \in \mathbb{K}$, dann wird wegen der Linearität in dieser Spalte auch der Wert von F mit r multipliziert. Schließlich behaupten wir, dass F bei Vertauschung von zwei Spalten das Vorzeichen wechselt. Dazu schreiben wir in die i–te und die j–te Spalte $v_i + v_j$, und erhalten nach Definition $0 = F(v_1, \dots, v_i + v_j, \dots, v_i + v_j, \dots, v_n)$. Nach der Linearität in der i–ten Spalte können wir die rechte Seite als $F(v_1, \dots, v_i, \dots, v_i + v_j, \dots, v_n) + F(v_1, \dots, v_j, \dots, v_i + v_j, \dots, v_n)$ schreiben. Da F verschwindet, wenn zwei Spalten gleich sind, bleibt vom ersten Summanden nur $F(v_1, \dots, v_i, \dots, v_j, \dots, v_n)$ und vom zweiten nur $F(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$ übrig, also erhalten wir $F(v_1, \dots, v_j, \dots, v_i, \dots, v_n) = -F(v_1, \dots, v_i, \dots, v_j, \dots, v_n)$. Wir werden später sehen, dass für jede Determinantenfunktion F und jede Matrix $A \in M_n(\mathbb{K})$ die Gleichung $F(A^t) = F(A)$ gilt, wobei A^t die transponierte Matrix bezeichnet. Daraus folgt dann, dass ein analoges Verhalten unter elementaren Zeilenoperationen gilt.

Wir können nun direkt beweisen, dass Determinantenfunktionen für Matrizen beliebiger Größe tatsächlich existieren:

Satz 6.3 (Existenzsatz). *Für jeden Körper $\mathbb{K}$ und jedes $n \in \mathbb{N}$ gibt es eine normierte Determinantenfunktion* $\det : M_n(\mathbb{K}) \to \mathbb{K}$.

Beweis. Wir beweisen den Satz durch Induktion nach n und definieren die Determinantenfunktion induktiv. Für $n = 1$ ist die Identität $\mathrm{id}_{\mathbb{K}} : M_1(\mathbb{K}) = \mathbb{K} \to \mathbb{K}$ eine normierte Determinantenfunktion. Für $n = 2$ ist die Funktion det aus 6.2 eine normierte Determinantenfunktion. Nehmen wir induktiv an, dass wir bereits eine normierte Determinantenfunktion $\det : M_{n-1}(\mathbb{K}) \to \mathbb{K}$ definiert haben. Für $A = (a_{ij}) \in M_n(\mathbb{K})$ sei $A_j \in M_{n-1}(\mathbb{K})$, die $(n-1) \times (n-1)$–Matrix die entsteht, wenn man in A die erste Zeile und die j–te Spalte weglässt. Anders gesagt, ist $A = (v_1, \dots, v_n)$, dann ist $A_j = (\tilde{v}_1, \dots, \tilde{v}_{j-1}, \tilde{v}_{j+1}, \dots, \tilde{v}_n)$, wobei $\tilde{v}_i$ aus v_i durch weglassen der ersten Komponente entsteht. Nun definieren wir $\det(A) := \sum_{j=1}^n (-1)^{j+1} a_{1j} \det(A_j)$.

Wir müssen nun die definierenden Eigenschaften einer normierten Determinantenfunktion verifizieren. Für $A = (v_1, \dots, v_n)$ betrachte $B = (v_1, \dots, rv_i, \dots v_n)$. Dann ist $b_{1i} = ra_{1i}$ und $B_i = A_i$, also wird der i–te Summand in der Definition von det mit r multipliziert. Für $j \neq i$ ist $b_{1j} = a_{1j}$, aber eine Spalte von B_j ist gerade das r–fache der entsprechenden Spalte von A_j, also $\det(B_j) = r\det(A_j)$ nach Induktionsvoraussetzung. Somit werden auch alle anderen Summanden mit r multipliziert, und wir erhalten $\det(B) = r\det(A)$.

Betrachte zu $A = (v_1, \dots, v_n)$ die Matrizen $B = (v_1, \dots, v_i', \dots, v_n)$ und $C = (v_1, \dots, v_i + v_i', \dots, v_n)$, dann ist $c_{1i} = a_{1i} + b_{1i}$ und $C_i = A_i = B_i$ und damit $c_{1i}\det(C_i) = a_{1i}\det(A_i) + b_{1i}\det(B_i)$. Für $j \neq i$ erhalten wir $c_{1j} = a_{1j} = b_{1j}$, aber in der Matrix C_j ist gerade eine Spalte gleich der Summe der entsprechenden Spalten von A_j und B_j, während alle anderen Spalten in allen drei Matrizen gleich sind. Nach Induktionsvoraussetzung impliziert das $\det(C_j) = \det(A_j) + \det(B_j)$ und damit auch $c_{1j}\det(C_j) = a_{1j}\det(A_j) + b_{1j}\det(B_j)$. Damit erhalten wir aber $\det(C) = \det(A) + \det(B)$, und somit ist det linear in jeder Spalte.

Nehmen wir nun an, dass in $A = (v_1, \dots, v_n)$ zwei Spalten gleich sind, etwa $v_i = v_j = v$ mit $i < j$. Für $k \neq i, j$ sind dann zwei Spalten von A_k gleich $\tilde{v}$, und damit reduziert sich die definierende Formel für $\det(A)$ zu $(-1)^{i+1}a_{1i}\det(A_i) + (-1)^{j+1}a_{1j}\det(A_j)$. Nach Definition gilt

$$\begin{aligned} A_i &= (\tilde{v}_1, \dots, \tilde{v}_{i-1}, \tilde{v}_{i+1}, \dots, \tilde{v}_{j-1}, \tilde{v}, \tilde{v}_{j+1}, \dots, \tilde{v}_n) \\ A_j &= (\tilde{v}_1, \dots, \tilde{v}_{i-1}, \tilde{v}, \tilde{v}_{i+1}, \dots, \tilde{v}_{j-1}, \tilde{v}_{j+1}, \dots, \tilde{v}_n). \end{aligned}$$

Nach Induktionsvoraussetzung ist det auf $(n-1) \times (n-1)$–Matrizen eine Determinantenfunktion, also wissen wir aus Bemerkung 6.3 (2), dass bei Vertauschen von zwei Spalten der Wert von det das Vorzeichen wechselt. Nun erhält man aber A_i aus A_j indem man die Spalte $\tilde{v}$ der Reihe nach mit den $j-i-1$ Spalten $\tilde{v}_{i+1}, \dots, \tilde{v}_{j-1}$ vertauscht. Damit ist aber $\det(A_i) = (-1)^{j-i-1}\det(A_j)$, also $(-1)^{i+1}\det(A_i) = -(-1)^{j+1}\det(A_j)$ und somit $\det(A) = 0$.

Die Tatsache, dass det normiert ist, ist ganz einfach zu zeigen: Ist $A = \mathbb{I}_n$ die $n \times n$–Einheitsmatrix, dann ist $a_{11} = 1$ und $A_1 = \mathbb{I}_{n-1}$ und $a_{1i} = 0$ für alle $i > 1$. Damit ist aber nach Definition $\det(\mathbb{I}_n) = 1\det(\mathbb{I}_{n-1})$ und nach Induktionsvoraussetzung ist $\det(\mathbb{I}_{n-1}) = 1$. □

Beispiel 6.3. (1) Wir hätten im Beweis den Fall $n = 2$ gar nicht extra behandeln müssen. Die Funktion det aus 6.2 entsteht nämlich aus der Identität (die normierte Determinantenfunktion für $n = 1$) durch die im Beweis angegebene Konstruktion. Ist nämlich $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dann ist $A_1 = d$ und $A_2 = c$ (jeweils als 1×1–Matrizen betrachtet). Die Formel aus dem Beweis vereinfacht sich also zu $a\det(d) - b\det(c) = ad - bc$.

(2) Wir wollen die Formel für die Determinante einer 3×3–Matrix $A = (a_{ij})$ explizit berechnen. Aus der Definition von det erhalten wir

$$a_{11}\det\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} - a_{12}\det\begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13}\det\begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

und setzt man die 2×2–Determinanten ein, dann erhält man

$$a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Diese Formel kann man sich einfach mit der sogenannten *Regel von Sarrus* merken. Dazu bildet man eine 5×3–Matrix, indem man die ersten beiden Spalten der Matrix A nochmals hinten anhängt: $\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{pmatrix}$. Dann addiert man die Produkte über die drei "Hauptdiagonalen" (von links oben nach rechts unten) mit positivem Vorzeichen und die Produkte über die drei "Nebendiagonalen" (von rechts oben nach links unten) mit negativem Vorzeichen.

Vorsicht: Für größere Matrizen (ab 4×4) gibt es kein Analogon der Regel von Sarrus! Versuche, Analoga so einer Regel zu verwenden sind ein Zeichen für schlimmes Unverständnis.

6.4. Die Cramer'sche Regel. Aus den elementare Eigenschaften der Determinantenfunktion det können wir sofort eine Anwendung auf lineare Gleichungssysteme folgern:

Satz 6.4. *Ist $\mathbb{K}$ ein Körper, $A \in M_n(\mathbb{K})$ eine $n \times n$–Matrix über $\mathbb{K}$ mit Spaltenvektoren $v_1, \dots, v_n$ und $b \in \mathbb{K}^n$, dann gilt: Ist $x = (x_1, \dots, x_n) \in \mathbb{K}^n$ eine Lösung des linearen Gleichungssystems $Ax = b$, dann ist*

$$x_j \det(v_1, \dots, v_n) = \det(v_1, \dots, v_{j-1}, b, v_{j+1}, \dots, v_n)$$

Beweis. In Termen der Spaltenvektoren $v_1, \dots, v_n$ von A bedeutet $Ax = b$ gerade $x_1v_1 + \dots + x_nv_n = b$. Betrachten wir nun $\det(v_1, \dots, b, \dots, v_n)$, wobei wir b anstelle von v_j eingesetzt haben, dann erhalten wir

$$\det(v_1, \dots, b, \dots, v_n) = \det(v_1, \dots, x_1v_1 + \dots + x_nv_n, \dots, v_n).$$

Nach der Linearität in der j–ten Spalte ist das gleich $\sum_{i=1}^n x_i \det(v_1, \dots, v_i, \dots, v_n)$, wobei v_i an der j–ten Stelle steht. Für $i \neq j$ kommt aber in der Determinante zwei mal der selbe Spaltenvektor vor (nämlich v_i an der i–ten und der j–ten Stelle), also bleibt nur der j–te Summand übrig, indem in der j–ten Spalte v_j steht. Damit folgt die Behauptung des Satzes sofort. □

Korollar 6.4. *Ist $\det(A) \neq 0$, dann sind die Spaltenvektoren v_i von A linear unabhängig, A ist invertierbar, und für jedes $b \in \mathbb{K}^n$ ist die eindeutige Lösung $x = (x_1, \dots, x_n)$ des linearen Gleichungssystems $Ax = b$ gegeben durch*

$$x_j = \frac{\det(v_1, \dots, v_{j-1}, b, v_{j+1}, \dots, v_n)}{\det(A)}$$

Beweis. Sind $x_1, \dots, x_n \in \mathbb{K}$ so, dass $x_1v_1 + \dots + x_nv_n = 0$ gilt, dann ist natürlich $x = (x_1, \dots, x_n)$ eine Lösung des linearen Gleichungssystems $Ax = 0$. Natürlich ist $\det(v_1, \dots, v_{j-1}, 0, v_{j+1}, \dots, v_n) = 0$ für alle j, also folgt aus dem Satz $x_j \det(A) = 0$ für alle j. Ist $\det(A) \neq 0$, dann folgt $x_j = 0$ für alle j, und damit die lineare Unabhängigkeit der Spaltenvektoren von A.

Nach Korollar 4.5 (6) von [**1**] bilden die v_i dann eine Basis für $\mathbb{K}^n$ und nach Satz 4.10 (4) von [**1**] ist A invertierbar. Damit hat das Gleichungssystem $Ax = b$ für jedes $b \in \mathbb{K}^n$ die eindeutige Lösung $x = A^{-1}b$. Da $\det(A) \neq 0$ ist folgt die Formel für x_j direkt aus dem Satz. □

Bemerkung 6.4. (1) Wie wir schon bemerkt haben, kann man die Theorie der Determinantenfunktionen ohne Änderungen über kommutativen Ringen mit Einselement entwickeln. Satz 6.4 gilt in dieser Form ohne Änderungen. Die Folgerungen entsprechend Korollar 6.4 sind allerdings etwas komplizierter, wie aus dem Beweis ersichtlich ist: Um die lineare Unabhängigkeit der Spaltenvektoren zu folgern muss man verlangen, dass $\det(A)$ kein Nullteiler ist (es also kein Element $\neq 0$ gibt, dass mit $\det(A)$ multipliziert Null ergibt). In $\mathbb{Z}$ oder $\mathbb{R}[x]$ ist das äquivalent zu $\det(A) \neq 0$, im Allgemeinen ist es aber eine stärkere Einschränkung. Andererseits impliziert diese Eigenschaft noch lange nicht, dass es ein multiplikativ inverses Element zu $\det(A)$ gibt, was man benötigt, um tatsächlich Lösungen des linearen Gleichungssystems zu erhalten. In $\mathbb{Z}$ haben etwa nur die Elemente ± 1 ein multiplikativ Inverses.

(2) Für die praktische Lösung von linearen Gleichungssystemen ist die Cramer'sche Regel nicht besonders gut geeignet, weil die Berechnung der vielen Determinanten sehr aufwändig ist. Daher lösen Computerprogramme lineare Gleichungssysteme nicht mit dieser Methode. Um das zu sehen, bestimmen wir, wie viele Rechenoperationen zur

Lösung eines linearen Gleichungssystems mit n Gleichungen in n Unbekannten nötig sind. Wir werden uns dabei auf die Multiplikationen und Divisionen beschränken (die mehr Rechenaufwand benötigen) und Additionen, Subtraktionen und Vertauschungen von Zeilen oder Spalten außer Acht lassen. Die Formel für eine 2×2–Determinante besteht aus zwei Summanden, von denen jeder ein Produkt von zwei Zahlen ist. Nach Definition muss man n mal ein Element mit einer $(n-1) \times (n-1)$–Determinante multiplizieren, um eine $n \times n$–Determinante zu berechnen. Eine 3×3–Determinante hat also 6 Summanden, von denen jeder ein Produkt von 3 Zahlen ist, man benötigt also 12 Multiplikationen für so eine Determinante. Induktiv sieht man, dass eine $n \times n$–Determinante aus $n! = n(n-1) \cdots 3 \cdot 2$ Summanden besteht, von denen jeder ein Produkt von n Zahlen ist, also $n!(n-1)$ Multiplikationen benötigt.

Um ein $n \times n$–Gleichungssystem nach der Cramer'schen Regel zu berechnen, muss man $n+1$ Determinanten von $n \times n$–Matrizen berechnen, benötigt als $(n+1)n!(n-1) = (n+1)!(n-1)$ Multiplikationen. Anschließend braucht man noch n Divisionen, was aber kaum mehr ins Gewicht fällt. Berechnet man das explizit, dann braucht man für ein 3×3–System 48 Multiplikationen, ein 4×4–System benötigt 360 Multiplikationen, für 5×5–Systeme sind 2880 Multiplikationen nötig und bei einem 10×10–System sind es schon 359251200 Multiplikationen.

Versuchen wir auf ähnliche Weise den Gauß'schen Algorithmus zu analysieren, dann müssen wir nur bedenken, dass man nach Satz 3.9 von [**1**] jede invertierbare $n \times n$–Matrix (der einzige Fall in dem die Cramer'sche Regel funktioniert) durch elementare Zeilenoperationen in die Einheitsmatrix umgewandelt werden kann, was genau äquivalent zur Lösung des Systems ist. Betrachten wir also die erweiterte Matrix (A, b) des Systems. Da wir Vertauschungen von Zeilen ignorieren, dürfen wir annehmen, dass das die erste Zeile von A mit einem Element ungleich Null beginnt. Mit n Divisionen erreichten wir, dass die erste Zeile mit 1 beginnt. Um in den weiteren Zeilen das Element in der ersten Spalte zu Null zu machen, benötigen wir pro Zeile n Multiplikationen. Somit sind wir mit n Divisionen und $(n-1)n$ Multiplikationen so weit, dass in der ersten Spalte der erweiterten Matrix der erste Einheitsvektor e_1 steht. Damit das zweite Element der zweiten Zeile gleich Eins ist, brauchen wir $(n-1)$ Divisionen, und mit $(n-1)(n-1)$ Multiplikationen erreichen wir, dass in der zweiten Spalte der zweite Einheitsvektor e_2 steht. Induktiv sehen wir, dass wir $n + (n-1) + \cdots + 2 + 1 = \frac{1}{2}n(n+1)$ Divisionen und $(n-1)(n + (n-1) + \cdots + 2 + 1) = \frac{1}{2}(n-1)n(n+1)$ Multiplikationen benötigen, und ein $n \times n$–Gleichungssystem mit dem Gauß'schen Algorithmus zu lösen. Für ein 3×3–System sind das 6 Divisionen und 12 Multiplikationen, bei einem 4×4–System 10 Divisionen und 30 Multiplikationen und bei einem 5×5–System 15 Divisionen und 60 Multiplikationen. Bei einem 10×10–System erhält man die moderate Zahl von 55 Divisionen und 495 Multiplikationen.

Die Cramer'sche Regel ist aber von einem theoretischen Standpunkt aus interessant, weil sie in einfacher Weise beschreibt, wie die eindeutige Lösung des linearen Gleichungssystems $Ax = b$ (für invertierbares A) von der Matrix A und vom Vektor b abhängt, siehe Bemerkung 6.10

Eindeutigkeit der Determinante und die Leibniz–Formel

Unser nächstes Hauptziel ist zu zeigen, dass es nur eine normierte Determinantenfunktion gibt. Dazu müssen wir einige Grundtatsachen über die sogenannten Permutationsgruppen, also die Gruppen von Bijektionen einer endlichen Mengen beweisen.

6.5. Permutationen. Für $n \in \mathbb{N}$ bezeichnen wir mit $\mathfrak{S}_n$ die Menge aller Bijektionen der Menge $\{1, \dots, n\}$. Für zwei bijektive Funktionen $\sigma, \tau \in \mathfrak{S}_n$ ist natürlich auch die Komposition $\sigma \circ \tau$ eine Bijektion, liegt also wieder in $\mathfrak{S}_n$. Wir werden im weiteren meist einfach $\sigma\tau$ statt $\sigma \circ \tau$ schreiben. Zu $\sigma \in \mathfrak{S}_n$ ist auch die inverse Funktion σ^{-1} bijektiv und liegt damit ebenfalls in $\mathfrak{S}_n$. Nach Definition gilt $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \mathrm{id}$ und $\sigma \circ \mathrm{id} = \mathrm{id} \circ \sigma = \sigma$ und da die Komposition von Funktionen immer assoziativ ist, ist $\mathfrak{S}_n$ eine Gruppe mit neutralem Element id. Diese Gruppe ist allerdings *nicht* kommutativ.

Ist $\sigma \in \mathfrak{S}_n$, also $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ eine bijektive Funktion, dann können wir σ einfach beschreiben, indem wir das n–Tupel $(\sigma(1), \dots, \sigma(n))$ angeben. Klarerweise ist eine Funktion $f : \{1, \dots, n\} \to \{1, \dots, n\}$ genau dann injektiv, wenn sie surjektiv ist. Die möglichen n–Tupel zu Bijektionen $\sigma \in \mathfrak{S}_n$ sind also genau die, in denen jede der Zahlen $\{1, \dots, n\}$ einmal vorkommt. Somit hat man aber n Möglichkeiten $\sigma(1)$ zu wählen, es bleiben $(n-1)$ Möglichkeiten für $\sigma(2)$, und so weiter bis zu $\sigma(n)$, das dann schon eindeutig festgelegt ist. Daraus folgt aber, dass $\mathfrak{S}_n$ genau $n!$ Elemente besitzt.

Schließlich bemerken wir noch, dass wir $\mathfrak{S}_{n-1}$ in natürlicher Weise als Teilmenge von $\mathfrak{S}_n$ betrachten können. Betrachten wir nämlich eine Permutation $\sigma \in \mathfrak{S}_n$, für die $\sigma(n) = n$ gilt, dann ist $\sigma(i) \in \{1, \dots, n-1\}$ für alle $i \in \{1, \dots, n-1\}$, also liefert σ eine Funktion $\{1, \dots, n-1\} \to \{1, \dots, n-1\}$, und diese ist offensichtlich injektiv, also bijektiv, also ein Element von $\mathfrak{S}_{n-1}$. Umgekehrt kann man aus jedem $\sigma \in \mathfrak{S}_{n-1}$ eine Bijektion von $\{1, \dots, n\}$ machen, indem man n auf sich selbst abbildet. Natürlich ist der Wechsel zwischen den beiden Bildern mit der Komposition verträglich, also ist $\{\sigma \in \mathfrak{S}_n : \sigma(n) = n\}$ eine *Untergruppe* von $\mathfrak{S}_n$, die wir mit $\mathfrak{S}_{n-1}$ identifizieren können.

Für $n = 1$ gibt es natürlich nur eine Bijektion der Menge $\{1\}$, nämlich die Identität. Für $n = 2$ gibt es neben der Identität nur noch eine Bijektion, die dem geordneten Paar $(2, 1)$ entspricht und gerade die beiden Elemente vertauscht. Für $n = 3$ entsprechen die 6 möglichen Bijektionen gerade den Tripeln $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$ und $(3, 2, 1)$, und so weiter. Das erste und das dritte Tripel entsprechen gerade den beiden Elementen der Untergruppe $\mathfrak{S}_2 \subset \mathfrak{S}_3$.

Besonders einfache Permutationen sind die sogenannten *Transpositionen* oder Vertauschungen. Für $n \in \mathbb{N}$ und $i, j \in \{1, \dots, n\}$ mit $i \neq j$ definieren wir die Transposition $(i, j) \in \mathfrak{S}_n$ als die bijektive Abbildung die i auf j, j auf i und alle anderen Elemente von $\{1, \dots, n\}$ auf sich selbst abbildet. (i, j) vertauscht also gerade die Elemente i und j. Offensichtlich ist $(i, j)^{-1} = (i, j)$. Was wir nun benötigen ist, dass man jeder Permutation σ ein sogenanntes *Signum* $\mathrm{sgn}(\sigma) \in \{1, -1\}$ zuordnen kann, sodass $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ gilt und so, dass das Signum einer Transposition -1 ist. Zunächst beweisen wir:

Satz 6.5. *Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:*

(1) Man kann jede Permutation $\sigma \in \mathfrak{S}_n$ als Produkt von höchstens n Transpositionen schreiben.

(2) Sind τ_i für $i = 1, \dots, k$ und τ'_j für $j = 1, \dots, \ell$ Transpositionen und ist $\tau_1 \cdots \tau_k = \tau'_1 \cdots \tau'_\ell$, dann sind die Zahlen k und ℓ entweder beide gerade oder beide ungerade.

Beweis. (1) Wir verwenden Induktion nach n. Für $n = 2$ haben wir nur die Transposition $(1, 2)$ und die Identität. Wie wir aber bereits bemerkt haben, ist $(1, 2)^{-1} = (1, 2)$, also $(1, 2)(1, 2) = \mathrm{id}$. Nehmen wir induktiv an, dass $n \geq 3$ gilt, und wir den Satz für $\mathfrak{S}_{n-1}$ bereits bewiesen haben. Zu $\sigma \in \mathfrak{S}_n$ betrachte $\sigma(n) \in \{1, \dots, n\}$. Ist $\sigma(n) = n$, dann ist σ ein Element der Untergruppe $\mathfrak{S}_{n-1} \subset \mathfrak{S}_n$, kann also nach Induktionsvoraussetzung als Produkt von höchstens $n - 1$ Transpositionen geschrieben werden. Ist andererseits $\sigma(n) = k \neq n$, dann betrachten wir $(k, n)\sigma$. Das bildet n auf n ab, also gibt nach Induktionsvoraussetzung eine Zahl $s \leq n-1$ und Transpositionen $\tau_1, \dots, \tau_s$, sodass $(k,n)\sigma = \tau_1 \cdots \tau_s$ gilt. Damit ist aber $\sigma = (k,n)(k,n)\sigma = (k,n)\tau_1 \cdots \tau_s$ ein Produkt von höchstens n Transpositionen.

(2) Sei $\{e_1, \dots, e_n\}$ die Standardbasis für den $\mathbb{R}$–Vektorraum $\mathbb{R}^n$, sei $\sigma = \tau_1 \cdots \tau_k = \tau_1' \cdots \tau_\ell'$ und betrachte $\det(e_{\sigma(1)}, \dots, e_{\sigma(n)})$, wobei det die normierte Determinantenfunktion aus Satz 6.3 bezeichnet. Nach Konstruktion ist $\det(e_1, \dots, e_n) = 1$, und nach Bemerkung (2) von 6.3 wechselt die Determinante das Vorzeichen, wenn man zwei Spalten vertauscht. Damit folgt aber aus $\sigma = \tau_1 \cdots \tau_k$ sofort, dass $\det(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = (-1)^k$ gelten muss. Analog folgt aus $\sigma = \tau_1' \cdots \tau_\ell'$, dass diese Determinante gleich $(-1)^\ell$ sein muss, also folgt die Behauptung. □

Bemerkung 6.5. (1) Die Darstellung als Produkt von Transpositionen ist nicht eindeutig. So gilt etwa in $\mathfrak{S}_3$ zum Beispiel trivialerweise $(1,3) = (1,2)(1,2)(1,3)$ aber auch die nichttriviale Gleichung $(1,2)(2,3)(1,2) = (1,3)$.

(2) Die induktive Methode aus dem Beweis von Teil (1) des Satzes kann man verwenden, um eine explizite Darstellung einer gegebenen Permutation als Produkt von Transpositionen zu erhalten. Betrachten wir etwa die Permutation $\sigma \in \mathfrak{S}_4$, die gegeben ist durch $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 2$ und $\sigma(4) = 1$. Betrachten wir nun $(1,4)\sigma$, dann bildet das 1 auf 3, 2 auf 1, 3 auf 2 und 4 auf 4 ab. Damit vertauscht $(2,3)(1,4)\sigma$ die Elemente 2 und 1 und lässt 3 und 4 fix, also ist $(2,3)(1,4)\sigma = (1,2)$ und somit $\sigma = (1,4)(2,3)(1,2)$.

(3) Bei Rechnungen mit Permutationsgruppen ist immer Vorsicht geboten, weil diese Gruppen nicht kommutativ sind. Betrachten wir etwa $\mathfrak{S}_3$, dann bildet $(1,2)(2,3)$ das Element 3 auf 1 ab, während $(2,3)(1,2)$ klarerweise 3 auf 2 abbildet.

Definition 6.5. Sei $\sigma \in \mathfrak{S}_n$ eine Permutation. Dann definieren wir das *Signum* $\operatorname{sgn}(\sigma) \in \{-1, 1\}$ von σ als $(-1)^k$ falls es eine Darstellung von σ als Produkt von k Transpositionen gibt. Nach Teil (1) des Satzes kann man σ immer als Produkt von Transpositionen schreiben und nach Teil (2) des Satzes ist $\operatorname{sgn}(\sigma)$ wohldefiniert, weil sich für verschiedene Darstellungen der selben Permutation immer der selbe Wert für $\operatorname{sgn}(\sigma)$ ergibt.

Wir erhalten nun leicht die Eigenschaften der Signumfunktion:

Proposition 6.5. *Für $n \geq 2$ hat die Signumfunktion* $\operatorname{sgn} : \mathfrak{S}_n \to \{-1, 1\}$ *folgende Eigenschaften:*

(1) sgn *ist ein Gruppenhomomorphismus, d.h.* $\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma')$.

(2) Ist τ eine Transposition, dann ist $\operatorname{sgn}(\tau) = -1$.

(3) $\operatorname{sgn}(\mathrm{id}) = 1$ *und für jedes $\sigma \in \mathfrak{S}_n$ ist* $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

Beweis. (1) Sind $\sigma = \tau_1 \cdots \tau_k$ und $\sigma' = \tau_1' \cdots \tau_\ell'$ Darstellungen von σ und σ' als Produkte von Transpositionen, dann ist $\tau_1 \cdots \tau_k \cdot \tau_1' \cdots \tau_\ell'$ eine Darstellung von $\sigma\sigma'$ als Produkt von Transpositionen. Damit ist aber nach Definition $\operatorname{sgn}(\sigma\sigma') = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma')$.

(2) folgt direkt aus der Definition.

(3) Weil $\mathrm{id} = (1,2)(1,2)$ gilt ist $\operatorname{sgn}(\mathrm{id}) = 1$, also gilt $\operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\mathrm{id}) = 1$ nach Teil (1), also ist $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$. □

6.6. Eindeutigkeit der Determinante. Mit den obigen Resultaten über Permutation können wir beweisen, dass es nur eine normierte Determinantenfunktion gibt. Gleichzeitig erhalten wir eine allgemeine Formel für die Determinante, die sogenannte

Leibniz–Formel, die zwar für die praktische Berechnung von Determinanten zu kompliziert ist, aber theoretisch in vielen Fällen nützlich ist. Aus diesen beiden Ergebnissen werden wir rasch alle weiteren Resultate über Determinanten erhalten.

Wir können nun nämlich sofort das Verhalten von Determinantenfunktionen unter Permutation der Spaltenvektoren beschreiben. Ist $F : M_n(\mathbb{K}) \to \mathbb{K}$ eine Determinantenfunktion und $\sigma \in \mathfrak{S}_n$ eine Permutation, dann kann man σ als Produkt von Transpositionen schreiben, und bei Vertauschung von zwei Spalten wechselt F nach Bemerkung (2) von 6.3 das Vorzeichen. Somit ist aber $F(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \operatorname{sgn}(\sigma)F(v_1, \dots, v_n)$ für beliebige Elemente $v_1, \dots, v_n \in \mathbb{K}^n$.

Satz 6.6. *Sei $\mathbb{K}$ ein Körper, $F : M_n(\mathbb{K}) \to \mathbb{K}$ eine Determinantenfunktion und $\mathbb{I} \in M_n(\mathbb{K})$ die $n \times n$–Einheitsmatrix. Dann gilt für $A = (a_{ij}) \in M_n(\mathbb{K})$ die Formel*

$$F(A) = F(\mathbb{I}) \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

Insbesondere ist $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$ *und* $F(A) = F(\mathbb{I}) \det(A)$.

Beweis. Sei $\{e_1, \dots, e_n\}$ die Standardbasis von $\mathbb{K}^n$. Dann kann man den i–ten Spaltenvektor von A als $a_{1i}e_1 + \dots + a_{ni}e_n$ schreiben. Somit ist

$$F(A) = F(a_{11}e_1 + \dots + a_{n1}e_n, \dots, a_{1n}e_1 + \dots + a_{nn}e_n).$$

Wegen der Linearität von F in jeder Spalte zerfällt das in eine riesige Summe wobei in jedem Summanden in jeder Spalte nur mehr ein e_j steht. Ist $f : \{1, \dots, n\} \to \{1, \dots, n\}$ definiert dadurch, dass in der j–ten Spalte gerade $e_{f(j)}$ steht, dann erhalten wir

$$F(A) = \sum_f a_{f(1)1} \dots a_{f(n)n} F(e_{f(1)}, \dots, e_{f(n)}),$$

wobei die Summe über alle Funktionen $f : \{1, \dots, n\} \to \{1, \dots, n\}$ geht. Ist nun f nicht injektiv, dann kommen im entsprechenden Summanden zwei gleiche Vektoren in zwei verschiedene Spalten von F vor, also verschwindet der entsprechende Summand. Daher müssen wir nur über die bijektiven Funktionen, also über $\mathfrak{S}_n$, summieren. Für $\sigma \in \mathfrak{S}_n$ haben wir aber bereits festgestellt, dass $F(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \operatorname{sgn}(\sigma)F(e_1, \dots, e_n)$ gilt. Offensichtlich ist $F(e_1, \dots, e_n) = F(\mathbb{I})$ also folgt die erste Formel für $F(A)$. Wegen $\det(\mathbb{I}) = 1$ erhalten wir daraus sofort die Formel für $\det(A)$ und daraus folgt sofort die zweite Formel für $F(A)$. □

Dieser Satz liefert nun eine vollständige Beschreibung aller Determinantenfunktionen $F : M_n(\mathbb{K}) \to \mathbb{K}$. Ist nämlich $r \in \mathbb{K}$ beliebig, dann ist offensichtlich $A \mapsto r \det(A)$ eine Determinantenfunktion, und nach dem Satz ist jede Determinantenfunktion von dieser Form, wobei $r = F(\mathbb{I})$ gilt.

Wir können diesen Satz (oder besser gesagt den Beweis) verwenden um zu zeigen, dass eine Matrix genau dann invertierbar ist, wenn ihre Determinante ungleich Null ist. Als weiteres Beispiel einer unmittelbaren Anwendung dieses Satzes betrachten wir sogenannte *obere Dreiecksmatrizen.* Eine $n \times n$–Matrix $A = (a_{ij}) \in M_n(\mathbb{K})$ heißt eine obere Dreiecksmatrix, wenn $a_{ij} = 0$ für alle $i > j$ gilt, d.h. wenn unterhalb der Hauptdiagonale von A nur Nullen stehen.

Korollar 6.6. *(1) Eine Matrix $A \in M_n(\mathbb{K})$ ist genau dann invertierbar, wenn* $\det(A) \neq 0$ *gilt.*

(2) Sei $A = (a_{ij}) \in M_n(\mathbb{K})$ eine obere Dreiecksmatrix. Dann ist $\det(A) = a_{11} \dots a_{nn}$.

Beweis. (1) aus Korollar 6.4 wissen wir schon, dass $\det(A) \neq 0$ die Invertierbarkeit von A impliziert, es bleibt also zu zeigen, dass für eine invertierbare Matrix A immer $\det(A) \neq 0$ gelten muss. Sind $\{v_1, \dots, v_n\}$ die Spaltenvektoren einer invertierbaren Matrix A, dann bilden diese Vektoren nach Satz 4.10 von [**1**] eine Basis für $\mathbb{K}^n$. Damit findet man für $i, j = 1, \dots, n$ Skalare $b_{ij} \in \mathbb{K}$ sodass $e_i = \sum_j b_{ij} v_j$ gilt. Damit erhalten wir

$$1 = \det(\mathbb{I}) = \det(e_1, \dots, e_n) = \det(b_{11}v_1 + \dots + b_{1n}v_n, \dots, b_{n1}v_1 + \dots + b_{nn}v_n)$$

Wie im Beweis des Satzes sehen wir nun, dass die rechte Seite durch

$$\det(v_1, \dots, v_n) \sum_{\sigma \in \mathfrak{S}_n} b_{\sigma(1)1} \cdots b_{\sigma(n)n}$$

gegeben ist. Insbesondere folgt $\det(A) = \det(v_1, \dots, v_n) \neq 0$.

(2) Nach der allgemeinen Formel ist $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$. Ist $\sigma(j) > j$, für ein j, dann nach Voraussetzung $a_{\sigma(j)j} = 0$, also bleiben nur Summanden zu solchen Permutationen über, die $\sigma(j) \leq j$ für alle $j = 1, \dots, n$ erfüllen. Daraus folgt aber $\sigma(1) = 1$, damit $\sigma(2) = 2$ und so weiter, sodass nur der Summand zu $\sigma = \mathrm{id}$ übrig bleibt. □

6.7. Determinante der Transponierten, Entwicklungssätze. Betrachten wir die Formel $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$. In jedem Summanden kommt nach Definition genau ein Eintrag aus jeder Spalte vor. Weil aber σ eine Bijektion ist, kommt auch aus jeder Zeile genau ein Eintrag vor, und das lässt eine gewisse Symmetrie zwischen Zeilen und Spalten vermuten. Aus Definition 5.3 (5) von [**1**] kennen wir die Operation des Transponierens einer Matrix, die Zeilen und Spalten vertauscht. Nach Definition ist für $A = (a_{ij}) \in M_n(\mathbb{K})$ die transponierte Matrix $A^t = (b_{ij}) \in M_n(\mathbb{K})$ gegeben durch $b_{ij} := a_{ji}$. Dies bedeutet gerade, dass der k–te Spaltenvektor von A^t gerade mit dem k–ten Zeilenvektor von A übereinstimmt, wenn man beide einfach als Elemente von $\mathbb{K}^n$ betrachtet, und umgekehrt (wegen $(A^t)^t = A$).

Satz 6.7. *Sei $\mathbb{K}$ ein Körper. Dann gilt $\det(A) = \det(A^t)$ für alle $A \in M_n(\mathbb{K})$.*

Beweis. Nach Satz 6.5 ist $\det(A^t) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$. Weil σ bijektiv ist, kann man das Produkt $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ als $a_{\sigma^{-1}(1)1} \dots a_{\sigma^{-1}(n)n}$ schreiben. Nach Proposition 6.5 ist $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$, also folgt $\det(A^t) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma^{-1}) a_{\sigma^{-1}(1)1} \dots a_{\sigma^{-1}(n)n}$. Wenn σ durch alle Permutationen in $\mathfrak{S}_n$ läuft, dann kommt als σ^{-1} jedes Element von $\mathfrak{S}_n$ genau ein mal vor, also können wir die Summe auch als $\sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n} = \det(A)$ schreiben. □

In der Definition von det haben wir die Berechnung von $n \times n$–Determinanten auf die Berechnung von $(n-1) \times (n-1)$–Determinanten zurückgeführt, wobei wir durch die Elemente der ersten Zeile gelaufen sind und jeweils eine Spalte der verbleibenden $(n-1) \times n$–Matrix weggelassen haben ("Entwicklung nach der ersten Zeile"). Mit Hilfe unserer jetzigen Resultate können wir leicht zeigen, dass man nach jeder beliebigen Zeile und auch nach jeder beliebigen Spalte entwickeln kann. Außerdem können wir den Zusammenhang der Determinante mit elementaren Zeilenoperationen klären, was uns auch eine effektive Methode zur Berechnung von Determinanten liefert. Dazu benötigen wir noch eine Notation. Für $A \in M_n(\mathbb{K})$ sei $A_{ij} \in M_{n-1}(\mathbb{K})$ die Matrix, die entsteht, wenn man in A die i–te Zeile und die j–te Spalte weglässt.

Korollar 6.7. *(1) Die Funktion* $\det : M_n(\mathbb{K}) \to \mathbb{K}$ *ist linear in jeder Zeile der Matrix und verschwindet, falls zwei Zeilen gleich sind. Addiert man zu einer Zeile ein*

Vielfaches einer anderen Zeile, dann bleibt der Wert der Determinante unverändert. Vertauscht man zwei Zeilen, dann wechselt die Determinante ihr Vorzeichen.

(2) Für $A = (a_{ij}) \in M_n(\mathbb{K})$ gelten die Formeln

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \quad \text{“\textit{Entwicklung nach der } i\text{\textit{–ten Zeile}”}}$$

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \quad \text{“\textit{Entwicklung nach der } j\text{\textit{–ten Spalte}”}}$$

Beweis. (1) Da $\det(A) = \det(A^t)$ gilt, folgt die Linearität in jeder Zeile aus der Linearität in jeder Spalte. Sind in A zwei Zeilen gleich, dann sind in A^t zwei Spalten gleich, also gilt $\det(A^t) = 0$, also $\det(A) = 0$. Daraus folgt sofort, dass sich die Determinante nicht ändert, wenn man zu einer Zeile ein Vielfaches einer anderen Zeile addiert. Vertauschen von zwei Zeilen in A entspricht genau Vertauschen der entsprechenden Spalten in A^t, also wechselt die Determinante ihr Vorzeichen.

(2) Im Beweis von Satz 6.3 haben wir det durch $\det(A) = \sum_{j=1}^{n} (-1)^{j+1} a_{1j} \det(A_{1j})$ definiert. Sei $\tilde{A} = (\tilde{a}_{ij})$ die Matrix, die aus A entsteht, indem man die i–te Zeile ganz nach oben tauscht. Das kann man realisieren, indem man die i–te Zeile mit der $(i-1)$-ten, dann mit der $(i-2)$–ten und so weiter bis zur ersten Zeile vertauscht, also ist $\det(\tilde{A}) = (-1)^{i-1} \det(A)$ nach Teil (1). Andererseits ist $\tilde{A}_{1j} = A_{ij}$ für alle $j = 1, \dots, n$. Damit erhalten wir

$$\det(\tilde{A}) = \sum_{j=1}^{n} (-1)^{j+1} \tilde{a}_{1j} \det(\tilde{A}_{1j}) = \sum_{j=1}^{n} (-1)^{j+1} a_{ij} \det(A_{ij})$$

und somit $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$.

Ist andererseits $B = (b_{ij}) = A^t$, dann ist nach der zuletzt bewiesenen Formel $\det(B) = \sum_{j=1}^{n} (-1)^{i+j} b_{ij} \det(B_{ij})$. Nun gilt aber $\det(B) = \det(A)$ und $b_{ij} = a_{ji}$, sowie $B_{ij} = A_{ji}^t$, also erhalten wir $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ji} \det(A_{ji}^t)$, und wegen $\det(A_{ji}^t) = \det(A_{ji})$ liefert das die letzte behauptete Formel. □

Beispiel 6.7. (1) In manchen Fällen führt die Entwicklung nach einer Zeile oder einer Spalte schnell zur Berechnung einer Determinante. Betrachten wir etwa die Matrix $A = \begin{pmatrix} 5 & 0 & 3 & 2 \\ 3 & 2 & 4 & 5 \\ 4 & 0 & 0 & 1 \\ 6 & 0 & 1 & 3 \end{pmatrix} \in M_4(\mathbb{R})$. Entwickeln nach der zweiten Spalte liefert $\det(A) = 2 \det \begin{pmatrix} 5 & 3 & 2 \\ 4 & 0 & 1 \\ 6 & 1 & 3 \end{pmatrix}$. Entwickelt man diese Determinante nach der zweiten Zeile, dann erhält man $\det(A) = -8 \det \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix} - 2 \det \begin{pmatrix} 5 & 3 \\ 6 & 1 \end{pmatrix} = -8 \cdot 7 + 2 \cdot 13 = -30$.

(2) In den meisten Fällen ist der beste Weg zur Berechnung einer Determinante die Anwendung von elementaren Zeilen– oder Spaltenoperationen. Betrachten wir als Beispiel die Matrix $A = \begin{pmatrix} 1 & 1 & -2 & 4 \\ 0 & 1 & 1 & 3 \\ 2 & -1 & 1 & 0 \\ 3 & 1 & 2 & 5 \end{pmatrix}$. Subtrahieren wir von der dritten Zeile das doppelte der ersten, und von der vierten Zeile das dreifache der ersten, dann ändert das die

Determinante nicht, also ist $\det(A)$ gleich der Determinante von $\begin{pmatrix} 1 & 1 & -2 & 4 \\ 0 & 1 & 1 & 3 \\ 0 & -3 & 5 & -8 \\ 0 & -2 & 8 & -7 \end{pmatrix}$. Addieren wir nun zur dritten Zeile das dreifache der zweiten und zur vierten Zeile das doppelte der zweiten, dann ändert das die Determinante wieder nicht, und wir erhalten die Matrix $\begin{pmatrix} 1 & 1 & -2 & 4 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 8 & 1 \\ 0 & 0 & 10 & -1 \end{pmatrix}$. Subtrahieren wir nun noch von der vierten Zeile $\frac{10}{8}$ mal die dritte Zeile, dann wird diese Zeile zu $(0,0,0,-\frac{18}{8})$, und die entstehende Matrix hat immer noch die selbe Determinante wie A. Nun habe wir aber eine obere Dreiecksmatrix vor uns, und nach Korollar 6.6 erhalten wir $\det(A) = -18$.

(3) Zum Abschluss wollen wir noch einen wichtigen Spezialfall einer Determinante besprechen, nämlich die sogenannte *Vandermonde–Determinante*. Dazu betrachten wir Elemente $x_1, \dots, x_n \in \mathbb{K}$ und bilden die $n \times n$–Matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix}$$

Wir behaupten, dass die Determinante dieser Matrix gegeben ist durch $\prod_{i<j}(x_j - x_i)$. Wir beweisen das durch Induktion nach n. Für $n = 2$ ist $\det \begin{pmatrix} 1 & 1 \\ x_1 & x_2 \end{pmatrix} = x_2 - x_1$, also stimmt die Behauptung. Nehmen wir also an, dass wir die Formel für $(n-1) \times (n-1)$–Matrizen bereits bewiesen haben. Nun subtrahieren wir von der letzten (n–ten) Zeile das x_1–fache der vorletzten ($n-1$-ten) Zeile. Wir erhalten als neue letzte Zeile $(0, (x_2 - x_1)x_2^{n-2}, \dots, (x_n - x_1)x_n^{n-2})$ und die Determinante bleibt unverändert. Subtrahieren wir nun von der $(n-1)$–ten Zeile das x_1–fache der $(n-2)$–ten, dann bleibt die Determinante unverändert und die vorletzte Zeile wird zu $(0, (x_2-x_1)x_2^{n-3}, \dots, (x_n-x_1)x_n^{n-3})$. Das setzten wir nun so lange fort, bis wir von der zweiten Zeile das x_1–fache der ersten Zeile abgezogen haben. Dann sehen wir, das unsere ursprüngliche Determinante übereinstimmt mit der Determinante der Matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & (x_2 - x_1) & \dots & (x_n - x_1) \\ 0 & (x_2 - x_1)x_2 & \dots & (x_n - x_1)x_n \\ \vdots & \vdots & & \vdots \\ 0 & (x_2 - x_1)x_2^{n-2} & \dots & (x_n - x_1)x_n^{n-2} \end{pmatrix}.$$

Entwickeln nach der ersten Spalte zeigt nun, dass wir in der Berechnung der Determinante einfach die erste Zeile und die erste Spalte weglassen können. Dann können wir aber aus der (neuen) ersten Spalte $(x_2 - x_1)$ aus der nächsten Spalte $(x_3 - x_1)$ und so weiter bis $(x_n - x_1)$ herausheben und sehen, dass unsere Determinante gegeben ist durch

$$(x_n - x_1) \dots (x_2 - x_1) \det \begin{pmatrix} 1 & \dots & 1 \\ x_2 & \dots & x_n \\ \vdots & & \vdots \\ x_2^{n-2} & \dots & x_n^{n-2} \end{pmatrix}.$$

Nach Induktionsvoraussetzung liefert die verbleibende Determinante $\prod_{2\leq i<j\leq n}(x_j - x_i)$ und somit folgt die Behauptung.

6.8. Determinante und die inverse Matrix. Die Entwicklungssätze für Determinanten erlauben uns im Fall einer Matrix A mit $\det(A) \neq 0$ die inverse Matrix explizit anzugeben. Diese Formel für die Inverse wird oft auch als Cramer'sche Regel bezeichnet.

Satz 6.8. *Sei $\mathbb{K}$ ein Körper. Für eine Matrix $A = (a_{ij}) \in M_n(\mathbb{K})$ sei $A_{ij} \in M_{n-1}(\mathbb{K})$ die Matrix, die entsteht, wenn man in A die i–te Zeile und die j–te Spalte streicht. Definiert man $B = (b_{ij}) \in M_n(\mathbb{K})$ durch $b_{ij} = (-1)^{i+j}\det(A_{ji})$, dann ist $AB = BA = \det(A)\mathbb{I}$. Ist $\det(A) \neq 0$, dann ist $A^{-1} = \det(A)^{-1}B$.*

Beweis. Für das Produkt $AB = (c_{ij})$ gilt nach Definition der Matrizenmultiplikation

$$c_{ij} = \sum_k a_{ik}b_{kj} = \sum_k (-1)^{k+j}a_{ik}\det(A_{jk}).$$

Für $i = j$ ist $c_{ii} = \det(A)$ nach der Formel für die Entwicklung der Determinante nach der i–ten Zeile aus Korollar 6.7(2). Nehmen wir andererseits an, dass $j \neq i$ gilt. Sei $\tilde{A} = (\tilde{a}_{ij})$ die Matrix, die aus A entsteht, indem man statt der j–ten Zeile nochmals die i–te Zeile einsetzt. Dann ist natürlich $\det(\tilde{A}) = 0$, weil $\tilde{A}$ zwei gleiche Zeilen hat. Entwickelt man nun diese Determinante nach der i–ten Zeile, dann erhält man $0 = \sum_k (-1)^{i+k}\tilde{a}_{ik}\det(\tilde{A}_{ik})$. Nun ist aber $\tilde{a}_{ik} = a_{ik}$. Andererseits unterscheidet sich $\tilde{A}_{ik}$ von A_{jk} nur durch eine Vertauschung von Zeilen, also $\det(\tilde{A}_{ik})$ von $\det(A_{jk})$ nur durch ein Vorzeichen, dass außerdem unabhängig von k ist. Damit gilt aber $c_{ij} = 0$ für $i \neq j$, also $AB = \det(A)\mathbb{I}$.

Betrachten wir andererseits das Produkt $BA = (d_{ij})$. Wiederum nach Definition ist $d_{ij} = \sum_k a_{kj}(-1)^{i+k}\det(A_{ki})$. Für $i = j$ gilt wieder $d_{ii} = \det(A)$ nach der Formel für die Entwicklung nach der i–ten Spalte aus Korollar 6.7(2). Analog zu den obigen Überlegungen beweist man, dass $d_{ij} = 0$ für $i \neq j$ gilt, indem man die Matrix betrachtet, die aus A entsteht, indem man die i–te Spalte durch eine Kopie der j–ten Spalte ersetzt.

□

6.9. Determinante und Produkte. Aus der Eindeutigkeit der Determinante können wir leicht schließen, dass die Determinante mit Produkten verträglich ist.

Satz 6.9. *Sei $\mathbb{K}$ ein Körper und $F : M_n(\mathbb{K}) \to \mathbb{K}$ eine Determinantenfunktion. Dann gilt $F(Av_1, \dots, Av_n) = \det(A)F(v_1, \dots, v_n)$ für alle $A \in M_n(\mathbb{K})$ und $v_1, \dots, v_n \in \mathbb{K}^n$. Ist $B \in M_n(\mathbb{K})$ eine weitere Matrix, dann ist $\det(AB) = \det(A)\det(B)$.*

Beweis. Betrachte die Funktion $F_A(v_1, \dots, v_n) := F(Av_1, \dots, Av_n)$. Da $v \mapsto Av$ linear und F linear in jeder Spalte ist auch F_A linear in jeder Spalte. Ist $v_i = v_j$ für $i \neq j$, dann ist $Av_i = Av_j$, also ist $F_A(v_1, \dots, v_n) = 0$, weil F eine Determinantenfunktion ist. Nach Satz 6.6 ist damit $F_A(v_1, \dots, v_n) = F_A(e_1, \dots, e_n)\det(v_1, \dots, v_n)$. Nun ist aber nach Definition $F_A(e_1, \dots, e_n) = F(Ae_1, \dots, Ae_n)$, und $Ae_1, \dots, Ae_n$ sind gerade die Spaltenvektoren von A, also ist $F_A(e_1, \dots, e_n) = F(A) = F(\mathbb{I})\det(A)$, wobei wir für die zweite Gleichung wieder Satz 6.6 verwendet haben. Wegen $F(\mathbb{I})\det(v_1, \dots, v_n) = F(v_1, \dots, v_n)$ erhalten wir $F_A(v_1, \dots, v_n) = \det(A)F(v_1, \dots, v_n)$. Sind $v_1, \dots, v_n$ die Spaltenvektoren einer Matrix B, dann sind $Av_1, \dots, Av_n$ die Spaltenvektoren von AB und wir erhalten

$$\det(AB) = \det(Av_1, \dots, Av_n) = \det(A)\det(v_1, \dots, v_n) = \det(A)\det(B).$$

□

Diese Produktformel hat eine ganz wichtige Konsequenz:

Korollar 6.9. *Für ähnliche Matrizen* $A, B \in M_n(\mathbb{K})$ *gilt* $\det(A) = \det(B)$. *Insbesondere kann man für einen endlichdimensionalen* $\mathbb{K}$*–Vektorraum* V *und eine lineare Abbildung* $f : V \to V$ *die Determinante* $\det(f)$ *von* f *als die Determinante einer beliebigen Matrixdarstellung von* f *definieren.*

Beweis. Ist $B = TAT^{-1}$ für eine invertierbare Matrix $T \in M_n(\mathbb{K})$, dann ist nach dem Satz $\det(B) = \det(T)\det(A)\det(T^{-1})$. Das ist ein Produkt von Elementen von $\mathbb{K}$, also spielt die Reihenfolge keine Rolle und nach dem Satz ist $\det(T)\det(T^{-1}) = \det(TT^{-1}) = 1$. □

Bemerkung 6.9. Wir haben in Bemerkung 3.4 von [**1**] festgestellt, dass die Menge $GL(n, \mathbb{K})$ aller invertierbaren $n \times n$–Matrizen über einem Körper $\mathbb{K}$ eine Gruppe unter der Matrizenmultiplikation bildet. Nach Korollar 6.6 liegt eine Matrix A genau dann in $GL(n, \mathbb{K})$, wenn $\det(A) \neq 0$ gilt. Betrachten wir nun die Teilmenge $SL(n, \mathbb{K}) := \{A \in GL(n, \mathbb{K}) : \det(A) = 1\}$. Dann ist natürlich $\mathbb{I} \in SL(n, \mathbb{K})$ und für $A, B \in SL(n, \mathbb{K})$ liegen nach der Produktformel auch AB und A^{-1} in $SL(n, \mathbb{K})$. Das bedeutet aber gerade, dass $SL(n, \mathbb{K})$ eine Untergruppe der Gruppe $GL(n, \mathbb{K})$ ist, sie sogenannte *spezielle lineare Gruppe*. Man kann das auch elegant dadurch sehen, dass die Produktformel bedeutet, dass det ein Homomorphismus von $GL(n, \mathbb{K})$ in die Gruppe $(\mathbb{K} \setminus \{0\}, \cdot)$ ist. Nach Definition besteht $SL(n, \mathbb{K})$ genau aus jenen Elementen, die durch diesen Homomorphismus auf das neutrale Element 1 abgebildet werden, ist also der Kern dieses Homomorphismus. Damit ist $SL(n, \mathbb{K})$ sogar eine *normale Untergruppe* in $GL(n, \mathbb{K})$, d.h. für $A \in SL(n, \mathbb{K})$ und $B \in GL(n, \mathbb{K})$ gilt $BAB^{-1} \in SL(n, \mathbb{K})$.

Für spezielle Körper liefert die Produktformel weitere Untergruppen von $GL(n, \mathbb{K})$. So erhält man etwa für $\mathbb{K} = \mathbb{R}$ die Gruppe $\{A \in GL(n, \mathbb{R}) : \det(A) > 0\}$ und für $\mathbb{K} = \mathbb{C}$ die Gruppe $\{A \in GL(n, \mathbb{C}) : |\det(A)| = 1\}$.

6.10. Bemerkung. Zum Abschluss möchte ich noch kurz einige Beobachtungen zu den in diesem Kapitel entwickelten Begriffen im Fall $\mathbb{K} = \mathbb{R}$ machen, die insbesondere in den Anwendungen dieser Begriffe in der Analysis wichtig sind (wo lineare Abbildungen insbesondere als Ableitungen auftreten). Wie schon in Abschnitt 3.1 von [**1**] kann man den Raum $M_n(\mathbb{R})$ einfach als $\mathbb{R}^{n^2}$ betrachten, und in diesem Bild sind die Koordinaten einfach durch die Eintragungen der Matrix gegeben. Die Leibnizformel aus 6.6 drückt nun die Determinante $\det(A)$ einfach als eine Summe von Produkten von Matrixeintragungen aus. Damit folgt aber aus elementaren Resultaten der Analysis, dass $\det : \mathbb{R}^{n^2} \to \mathbb{R}$ stetig und sogar beliebig oft differenzierbar ist. Das bedeutet aber, dass für eine Matrix A mit $\det(A) \neq 0$, Matrizen die sehr nahe bei A liegen, ebenfalls Determinante ungleich Null haben müssen. In der Nähe einer invertierbaren Matrix befinden sich also nur invertierbare Matrizen. (Technisch gesagt ist die Menge der invertierbaren Matrizen offen.) Diese Tatsache spielt eine wichtige Rolle beim Beweis des inversen Funktionensatzes in der Analysis.

Für eine invertierbare Matrix $A \in M_n(\mathbb{R})$ und einen Vektor $b \in \mathbb{R}^n$ kann man nach der Cramer'schen Regel aus 6.4 die eindeutige Lösung des Gleichungssystems $Ax = b$ durch Determinanten beschreiben. Das impliziert aber, dass diese eindeutige Lösung sowohl von der Matrix A als auch von dem Vektor b stetig abhängt, was wiederum in vielen Anwendungen wichtig ist. Analog zeigt die Formel für die inverse Matrix aus 6.8, dass die Funktion $A \mapsto A^{-1}$ auf der (offenen) Teilmenge der invertierbaren Matrizen stetig und beliebig oft differenzierbar ist.

KAPITEL 7

Charakteristisches Polynom, Eigenwerte und Diagonalisierbarkeit

Nachdem wir nun die Determinante als Hilfsmittel zur Verfügung haben, beginnen wir lineare Abbildungen von einem Vektorraum auf sich selbst genauer zu studieren. Insbesondere versuchen wir, zu einer gegebenen linearen Abbildung eine Basis zu finden, bezüglich der wir eine besonders einfach Matrixdarstellung erhalten. Ein wesentlicher Schritt dahin wird sein, jeder linearen Abbildung (bzw. jeder quadratischen Matrix) das sogenannte charakteristische Polynom zuzuordnen. Damit können dann algebraische Resultate über Polynome auf das Studium von linearen Abbildungen bzw. von Matrizen angewandt werden, was im weiteren eine zentrale Rolle spielen wird.

Eigenwerte und Eigenräume – Diagonalisierbarkeit

7.1. Grundlegende Definitionen. Sie $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung. Wir wollen versuchen, eine Basis für V zu finden, in der f besonders einfach aussieht. Äquivalent kann man das natürlich so formulieren, dass wir zu einer gegebenen $n \times n$–Matrix A eine möglichst einfache ähnliche Matrix suchen. Wir werden im weiteren öfters zwischen den Sichtweisen der Matrizen und der linearen Abbildungen hin und her schalten.

Als Anfang sollten wir vielleicht überlegen, was man eigentlich mit "besonders einfach aussehen" meinen könnte, bzw. Beispiele für besonders einfach lineare Abbildungen und Matrizen geben. Eine Klasse von besonders einfachen Matrizen sind die sogenannten *Diagonalmatrizen*, also Matrizen $A = (a_{ij})$, für die $a_{ij} = 0$ für $i \neq j$ gilt. Eine Diagonalmatrix hat also nur auf der Hauptdiagonale nichttriviale Eintragungen. Geometrisch bedeutet das, dass die Elemente der Standardbasis durch die Matrix A nur in ihrer Länge, aber nicht in ihrer Richtung geändert werden. Man kann nun natürlich für eine allgemeine lineare Abbildung Vektoren suchen, bei denen nur die Länge und nicht die Richtung verändert wird. Das führt sofort zu den zentralen Begriffen dieses Kapitels:

Definition 7.1. Sei $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung.

(1) Ein Element $\lambda \in \mathbb{K}$ heißt ein *Eigenwert* von f, falls es einen Vektor $v \in V$ mit $v \neq 0$ gibt, sodass $f(v) = \lambda v$ gilt. Ist das der Fall, so heißt v ein *Eigenvektor für f zum Eigenwert λ*.

(2) Ist λ ein Eigenwert von f, dann heißt $V^f_\lambda := \{v \in V : f(v) = \lambda v\}$ der *Eigenraum von f zum Eigenwert λ*.

(3) Die lineare Abbildung f heißt *diagonalisierbar* falls es eine Basis $\{v_i\}$ für V gibt, sodass jedes v_i ein Eigenvektor für f ist.

(4) Analog definieren wir die Begriffe Eigenwert, Eigenvektor, Eigenraum und Diagonalisierbarkeit für eine Matrix $A \in M_n(\mathbb{K})$, indem wir die lineare Abbildung $\mathbb{K}^n \to \mathbb{K}^n$ benutzen, die durch $x \mapsto Ax$ gegeben ist.

Bemerkung 7.1. Sei V ein endlichdimensionaler $\mathbb{K}$–Vektorraum, $f : V \to V$ eine diagonalisierbare lineare Abbildung und $\mathcal{B} = \{v_1, \dots, v_n\}$ eine Basis für V, die aus Eigenvektoren für f besteht. Sind $\lambda_1, \dots, \lambda_n$ die zugehörigen Eigenwerte, dann gilt nach Definition $f(v_i) = \lambda_i v_i$. Nach Definition bedeutet das aber für die Matrixdarstellung $[f]_{\mathcal{B}} = (a_{ij})$ von f bezüglich der Basis $\mathcal{B}$ gerade $a_{ii} = \lambda_i$ und $a_{ij} = 0$ für $i \neq j$, also ist $[f]_{\mathcal{B}}$ eine Diagonalmatrix.

Ist umgekehrt $f : V \to V$ linear, und $\mathcal{B} = \{v_1, \dots, v_n\}$ eine Basis von V, sodass $[f]_{\mathcal{B}}$ eine Diagonalmatrix ist, dann ist nach Definition $f(v_i) = a_{ii}v_i$, also v_i ein Eigenvektor zum Eigenwert a_{ii}. Damit ist f diagonalisierbar.

Somit sehen wir, dass eine lineare Abbildung genau dann diagonalisierbar ist, wenn sie bezüglich einer geeigneten Basis durch eine Diagonalmatrix dargestellt werden kann. Analog ist eine $n \times n$–Matrix A genau dann diagonalisierbar, wenn sie ähnlich zu einer Diagonalmatrix ist, d.h. wenn es eine invertierbare Matrix $T \in M_n(\mathbb{K})$ gibt, sodass TAT^{-1} eine Diagonalmatrix ist.

Beispiel 7.1. Zur Illustration des Begriffes betrachten wir zunächst drei Beispiele im $\mathbb{R}$–Vektorraum $\mathbb{R}^2$:

(1) Betrachte die Drehung um den Winkel $\varphi \in [0, 2\pi)$, d.h.

$$f(x, y) = (x\cos(\varphi) - y\sin(\varphi), x\sin(\varphi) + y\cos(\varphi)).$$

Ist $\varphi \neq 0, \pi$, dann hat f offensichtlich keine Eigenwerte und kann daher auch nicht diagonalisierbar sein. Für $\varphi = 0$ ist $f = \mathrm{id}$, also jedes $(x, y) \neq (0, 0)$ ein Eigenvektor zum Eigenwert 1, und für $\varphi = \pi$ ist $f = -\mathrm{id}$, also jeder Vektor (außer Null) ein Eigenvektor zum Eigenwert -1.

(2) Betrachte die lineare Abbildung $f(x, y) = (2x, x+y)$. Offensichtlich ist $f(0, y) = (0, y)$, also jeder Vektor dieser Form ein Eigenvektor zum Eigenwert 1. Andererseits ist $f(x, x) = (2x, 2x)$ also ist jeder Vektor mit gleichen Komponenten ein Eigenvektor zum Eigenwert 2. Damit ist f diagonalisierbar, weil etwa $\mathcal{B} = \{(1, 1), (0, 1)\}$ eine Basis aus Eigenvektoren ist. Offensichtlich gilt dann $[f]_{\mathcal{B}} = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(3) Betrachte die lineare Abbildung $f(x, y) = (x, x + y)$. Offensichtlich ist wieder jeder Vektor der Form $(0, y)$ ein Eigenvektor zum Eigenwert Eins. Es kann aber keine weiteren Eigenvektoren geben. Wäre nämlich $f(x, y) = (x, x+y) = (\lambda x, \lambda y)$ und $x \neq 0$, dann müsste natürlich $\lambda = 1$ gelten. Die zweite Komponenten liefert aber dann $y = x+y$, also $x = 0$, ein Widerspruch. Insbesondere kann f nicht diagonalisierbar sein, weil je zwei Eigenvektoren für f linear abhängig sind.

(4) Das Konzept von Eigenvektoren ist auch für unendlichdimensionale Vektorräume sehr wichtig. Betrachte den Raum $C^\infty(\mathbb{R}, \mathbb{R})$ der beliebig oft differenzierbaren Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. In der Analysis lernt man, dass $(f + g)' = f' + g'$ und $(\lambda f)' = \lambda f'$ für alle $f, g \in C^\infty(\mathbb{R}, \mathbb{R})$ und $\lambda \in \mathbb{R}$ gilt, also definiert die Ableitung $D(f) = f'$ eine lineare Abbildung $D : C^\infty(\mathbb{R}, \mathbb{R}) \to C^\infty(\mathbb{R}, \mathbb{R})$. Wie ebenfalls aus der Analysis bekannt, ist für jedes $\lambda \in \mathbb{R}$ die Funktion $x \mapsto e^{\lambda x}$ beliebig oft differenzierbar, und $(e^{\lambda x})' = \lambda e^{\lambda x}$. Somit ist für jedes $\lambda \in \mathbb{R}$ die Funktion $e^{\lambda x}$ ein Eigenvektor von D zum Eigenwert λ.

7.2. Geometrische Vielfachheit. Sei V ein endlichdimensionaler Vektorraum über $\mathbb{K}$, und $f : V \to V$ eine lineare Abbildung. Ist λ ein Eigenwert von f, dann betrachten wir den zugehörigen Eigenraum $V_\lambda := V_\lambda^f$. Ist $v \in V_\lambda$ und $\mu \in \mathbb{K}$, dann ist $f(\mu v) = \mu f(v) = \mu\lambda v = \lambda\mu v$, also $\mu v \in V_\lambda$. Sind andererseits $v, w \in V_\lambda$, dann ist $f(v + w) = f(v) + f(w) = \lambda v + \lambda w = \lambda(v + w)$, also ist V_λ ein Teilraum vom V.

Definition 7.2. Die *geometrische Vielfachheit* eines Eigenwerts λ einer linearen Abbildung $f : V \to V$ ist die Dimension des zugehörigen Eigenraumes V_λ^f.

Damit können wir nun relativ einfach zu einer (allerdings in der Praxis noch nicht sehr nützlichen) Charakterisierung diagonalisierbarer Abbildungen kommen. Zunächst zeigen wir, dass Eigenvektoren zu verschiedenen Eigenwerten automatisch linear unabhängig sind.

Lemma 7.2. *Sei V ein Vektorraum über $\mathbb{K}$, $f : V \to V$ eine lineare Abbildung und seien $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ verschiedene Eigenwerte von f. Ist $v_i \in V$ ein Eigenvektor zum Eigenwert λ_i für jedes $i = 1, \dots, k$, dann sind die Vektoren $v_1, \dots, v_k$ linear unabhängig.*

Beweis. Durch Induktion nach k. Ist $k = 1$, dann ist v_1 ein Eigenvektor, also $v_1 \neq 0$, also ist $\{v_1\}$ linear unabhängig. Nehmen wir also an, dass $k \geq 2$ gilt, und dass wir die Behauptung für $k - 1$ Eigenvektoren zu verschiedenen Eigenwerten bereits bewiesen haben. Seien $a_1, \dots, a_k \in \mathbb{K}$ so, dass $a_1v_1 + \dots + a_kv_k = 0$ gilt. Wenden wir auf diese Gleichung f an, dann erhalten wir wegen der Linearität $a_1f(v_1)+\dots+a_kf(v_k) = 0$, und nach Definition der v_i erhalten wir $a_1\lambda_1v_1+\dots+a_k\lambda_kv_k = 0$. Subtrahieren wir von dieser Gleichung das λ_k–fache der ursprünglichen Gleichung $a_1v_1+\dots+a_kv_k = 0$, dann erhalten wir $a_1(\lambda_1-\lambda_k)v_1+\dots+a_{k-1}(\lambda_{k-1}-\lambda_k)v_{k-1}+0 = 0$. Nach Induktionsvoraussetzung sind die Vektoren $v_1, \dots, v_{k-1}$ linear unabhängig, also ist $a_i(\lambda_i - \lambda_k) = 0$ für $i = 1, \dots, k-1$. Da die λ_i alle verschieden sind, ist $\lambda_i - \lambda_k \neq 0$, also $a_i = 0$ für alle $i = 1, \dots, k - 1$. Damit ist $a_kv_k = 0$, also $a_k = 0$ weil v_k ein Eigenvektor und damit nicht der Nullvektor ist, und die Behauptung folgt. □

Satz 7.2. *Sei V ein n–dimensionaler Vektorraum über einem Körper $\mathbb{K}$ und $f : V \to V$ eine lineare Abbildung. Dann gilt:*

(1) f hat höchstens n verschiedene Eigenwerte.

(2) Sind $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von f und ist n_i die geometrische Vielfachheit von λ_i für $i = 1, \dots, k$, dann ist $\sum_{j=1}^k n_j \leq n$ und $\sum n_j = n$ gilt genau dann, wenn f diagonalisierbar ist.

Beweis. (1) Zu jedem Eigenwert gibt es nach Definition mindestens einen Eigenvektor, und nach Lemma 7.2 sind Eigenvektoren zu verschiedenen Eigenwerten linear unabhängig. Da eine linear unabhängige Teilmenge von V nach Korollar 4.5 (4) von [**1**] höchstens $\dim(V) = n$ Elemente haben kann, folgt die Behauptung.

(2) Für $i = 1, \dots, k$ sei $\{v_1^{(i)}, \dots, v_{n_i}^{(i)}\}$ eine Basis für den Eigenraum $V_{\lambda_i}^f$. Dann behaupten wir, dass die Vektoren $v_1^{(1)}, \dots, v_{n_1}^{(1)}, \dots, v_1^{(k)}, \dots, v_{n_k}^{(k)}$ linear unabhängig sind. Seien also $a_i^j \in \mathbb{K}$ für $j = 1, \dots, k$ und $i = 1, \dots, n_k$ so, dass $\sum_{i,j} a_i^jv_i^{(j)} = 0$ gilt. Dann können wir diese endliche Summe als $\sum_{j=1}^k v^{(j)} = 0$ schreiben, wobei $v^{(j)} := \sum_{i=1}^{n_j} a_i^jv_i^{(j)}$. Nach Konstruktion ist $v^{(j)} \in V_{\lambda_j}^f$. Nach Lemma 7.2 ist aber $\sum v^{(j)} = 0$ nur möglich, wenn $v^{(j)} = 0$ für alle j gilt.

Damit ist aber $\sum_{i=1}^{n_j} a_i^jv_i^{(j)} = 0$ für alle j, was $a_i^j = 0$ für alle i und j impliziert, weil nach Konstruktion $v_1^{(j)}, \dots, v_{n_j}^{(j)}$ für alle j linear unabhängig sind. Damit ist die $\sum n_j$–elementige Teilmenge $\{v_1^{(1)}, \dots, v_{n_k}^{(k)}\}$ von V linear unabhängig, also folgt $\sum n_j \leq n$ wieder aus Korollar 4.5 (4) von [**1**].

Falls $\sum n_j = n$ gilt, dann ist diese Menge nach Korollar 4.5 (6) von [**1**] eine Basis von V also ist f diagonalisierbar. Ist umgekehrt f diagonalisierbar, dann finden wir eine Basis $\{v_1, \dots, v_n\}$ aus Eigenvektoren. Elemente dieser Basis, die Eigenvektoren zu einem fixen Eigenwert λ sind, bilden eine linear unabhängige Teilmenge von V_λ^f, also ist ihre Anzahl höchstens gleich der geometrischen Vielfachheit von λ. Damit folgt aber sofort $\sum n_j \geq n$. □

Insbesondere impliziert der Satz dass eine lineare Abbildung $f : V \to V$, die $\dim(V)$ viele verschieden Eigenwerte hat, automatisch diagonalisierbar ist.

Das charakteristische Polynom

Wir wissen an dieser Stelle noch nicht, wie wir zeigen können, dass eine gegebene lineare Abbildung Eigenwerte hat, bzw. wie man Eigenwerte bestimmen könnte. Aus Beispiel (1) von 7.1 wissen wir sogar, dass es im Allgemeinen keine Eigenwerte geben muss. Um diese Fragen zu studieren kommt uns die Theorie der Polynome zur Hilfe.

7.3. Eigenwerte und Determinanten. Zunächst können wir die Eigenräume einer linearen Abbildung leicht als Kern interpretieren. Damit kommen wir der Frage der Bestimmung von Eigenwerten einen großen Schritt näher:

Proposition 7.3. *Sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$ und $f : V \to V$ eine lineare Abbildung. Dann ist eine Zahl $\lambda \in \mathbb{K}$ genau dann ein Eigenwert von f, wenn $\det(f - \lambda\,\mathrm{id}) = 0$ gilt. Ist λ ein Eigenwert, dann ist der Eigenraum V^f_λ genau der Kern von $f - \lambda\,\mathrm{id}$.*

Beweis. Nach Abschnitt 2.5 von [**1**] betrachten wir auf $L(V, V)$ die punktweise Addition und Skalarmultiplikation, also $(f - \lambda\,\mathrm{id})(v) = f(v) - \lambda v$. Daher gilt $f(v) = \lambda v$ genau dann, wenn $(f - \lambda\,\mathrm{id})(v) = 0$ gilt. Somit ist $\lambda \in \mathbb{K}$ genau dann ein Eigenwert, wenn es ein Element $v \neq 0$ mit dieser Eigenschaft gibt, also genau dann wenn $(f - \lambda\,\mathrm{id})$ nicht injektiv ist. Da $f - \lambda\,\mathrm{id}$ eine lineare Abbildung von V auf sich selbst ist, ist nicht injektiv zu sein äquivalent zu nicht invertierbar zu sein, siehe Satz 4.11 von [**1**]. Nach Korollar 6.6 (1) ist das äquivalent zu $\det(f - \lambda\,\mathrm{id}) = 0$. Für einen Eigenwert λ gilt dann offensichtlich $V^f_\lambda = \mathrm{Ker}(f - \lambda\,\mathrm{id})$. □

Betrachten wir diese Charakterisierung von Eigenwerten im Bild von Matrizen, dann ist also für eine Matrix $A = (a_{ij}) \in M_n(\mathbb{K})$ eine Zahl $\lambda \in \mathbb{K}$ genau dann ein Eigenwert, wenn die Matrix $B = A - \lambda\mathbb{I}$, d.h. $b_{ii} = a_{ii} - \lambda$ und $b_{ij} = a_{ij}$ für $i \neq j$ Determinante Null hat.

An dieser Stelle können wir Polynome ins Spiel bringen. Wir haben Polynome vom Grad $\leq N$ in Abschnitt 2.6 von [**1**] als formale Ausdrücke der Form $\sum_{k=0}^N a_k t^k$ für Koeffizienten a_k aus einem Körper $\mathbb{K}$ und eine Variable t kennen gelernt. Diese Ausdrücke kann man einfach koeffizientenweise addieren und mit Skalaren aus $\mathbb{K}$ multiplizieren, und erhält so einen $\mathbb{K}$–Vektorraum $\mathbb{K}_N[t]$ der Dimension $N + 1$. Explizit bedeutet das, dass für $p = \sum a_k t^k$ und $q = \sum b_\ell t^\ell$ und $r \in \mathbb{K}$ die Gleichungen $p+q = \sum(a_k+b_k)t^k$ und $rp = \sum(ra_k)t^k$ gelten. Natürlich kann man ein Polynom vom Grad N auch als Polynom höheren Grades betrachtet, indem man die Koeffizient a_k für $k > N$ Null setzt. Damit kann man dann den (unendlichdimensionalen) Vektorraum $\mathbb{K}[t]$ aller Polynome bilden.

Insbesondere ist $\mathbb{K}[t]$ eine kommutative Gruppe unter der Addition. Man kann aber auf den Polynomen auch eine natürliche Multiplikation definieren. Diese ist dadurch charakterisiert, dass $t^k t^\ell = t^{k+\ell}$ gilt und die Multiplikation mit einem fixen Polynom eine lineare Abbildung ist. Explizit ist für $p = \sum a_k t^k$ und $q = \sum b_\ell t^\ell$ das Produkt $pq = \sum c_k t^k$ gegeben durch $c_k = \sum_{i=0}^k a_i b_{k-i}$. Daraus sieht man sofort, dass diese Multiplikation kommutativ ist, also $pq = qp$ gilt, und dass das Polynom 1 ein multiplikativ neutrales Element ist. Durch (teilweise etwas aufwändige) direkte Rechnungen verifiziert man, dass die Multiplikation von Polynomen assoziativ und distributiv bezüglich der Addition ist (siehe Übungen). Damit bildet aber $\mathbb{K}[t]$ einen *kommutativen Ring mit Einselement.*

Kehren wir nun zu den Matrizen zurück, dann können wir für $A = (a_{ij}) \in M_n(\mathbb{K})$ einfach die Matrix $A - t\mathbb{I}$ bilden, die in der Hauptdiagonale $a_{ii} - t$ und außerhalb davon a_{ij} als Eintragung hat. Dann können wir für jedes $i = 1, \dots, n$ den Ausdruck $a_{ii} - t$ als Polynom (vom Grad 1) betrachten, während für $i \neq j$ die Zahl $a_{ij} \in \mathbb{K}$ einfach als Polynom vom Grad Null betrachtet werden kann. Damit können wir aber, wenn wir die Determinante von $A - t\mathbb{I}$ auf irgend eine der in Kapitel 6 vorgestellten Arten berechnen, alle Summen und Produkte im Raum $\mathbb{K}[t]$ der Polynome interpretieren. Damit kann man aber $\det(A - t\mathbb{I})$ als Polynom $p_A \in \mathbb{K}[t]$ auffassen. Dieses Polynom heißt das *charakteristische Polynom* der Matrix A und stellt einen der zentralen Begriffe der linearen Algebra dar.

Bemerkung 7.3. Wie wir in Kapitel 6 bemerkt haben, kann man die Theorie der Determinanten ohne Änderungen für kommutative Ringe mit Einselement entwickeln. Wenn man das macht, dann kann man $A - t\mathbb{I}$ einfach als $n \times n$–Matrix über dem Polynomring $\mathbb{K}[t]$ betrachten, und so ihre Determinante als Element von $\mathbb{K}[t]$ bilden. Insbesondere zeigt das, dass verschiedene Möglichkeiten, die Determinante von $A - t\mathbb{I}$ zu berechnen alle zum gleichen charakteristischen Polynom p_A führen.

Damit wir das charakteristische Polynom gut verwenden können, müssen wir einige allgemeine Resultate über Polynome herleiten. Wir bemerken hier zunächst nur eine grundlegende Eigenschaft. Dazu erinnern wir uns, dass man ein Polynom $p \in \mathbb{K}[t]$ auch als Funktion $\mathbb{K} \to \mathbb{K}$ auffassen kann, indem man für t einfach Elemente von $\mathbb{K}$ einsetzt und die Potenzen, Produkte und Summen als Operationen in $\mathbb{K}$ interpretiert, siehe Abschnitt 2.6 von [**1**]. Wir schreiben weiter $p(\lambda)$ für den Wert dieser Funktion bei $\lambda \in \mathbb{K}$. Aus den Abschnitten 2.6 und 4.12 von [**1**] wissen wir auch, dass die algebraischen Operationen auf Polynomen genau den algebraischen Operationen auf Funktionen entsprechen. Für $p, q \in \mathbb{K}[t]$ und Skalare $r, \lambda \in \mathbb{K}$ gilt also $(p + q)(\lambda) = p(\lambda) + q(\lambda)$, $(rp)(\lambda) = r(p(\lambda))$ und $(pq)(\lambda) = p(\lambda)q(\lambda)$. Ist nun $A \in M_n(\mathbb{K})$ eine Matrix mit charakteristischem Polynom p_A, dann folgt aus diesen Überlegungen sofort, dass $p_A(\lambda) \in \mathbb{K}$ genau die Determinante der Matrix $A - \lambda\mathbb{I} \in M_n(\mathbb{K})$ ist. Damit erhalten wir:

Korollar 7.3. *Sei $A \in M_n(\mathbb{K})$ eine $n \times n$–Matrix. Dann sind die Eigenwerte der linearen Abbildung $x \mapsto Ax$ genau die Nullstellen des charakteristischen Polynoms, d.h. $\lambda \in \mathbb{K}$ ist genau dann ein Eigenwert, wenn $p_A(\lambda) = 0$ gilt.*

Beispiel 7.3. Betrachten wir die 2×2–Matrizen zu den Beispielen aus 7.1. Für die Drehung um den Winkel φ erhalten wir die Matrixdarstellung $A = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$. Daraus ergibt sich $p_A = (\cos(\varphi) - t)^2 + \sin^2(\varphi) = t^2 - 2\cos(\varphi)t + 1$. Nach der üblichen Formel für die Lösung von quadratischen Gleichungen ergibt sich als Nullstellen $\lambda_{1,2} = \cos(\varphi) \pm \sqrt{\cos^2(\varphi) - 1} = \cos(\varphi) \pm i\sin(\varphi)$. Somit existieren Nullstellen in $\mathbb{R}$ nur für $\sin(\varphi) = 0$, also $\varphi = k\pi$ mit $k \in \mathbb{Z}$, und das liefert nur die Fälle $A = \pm\mathbb{I}$. Wir werden später sehen, wie man die komplexen Nullstellen benutzen kann.

Für die zweite lineare Abbildung erhalten wir $A = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$ und damit das charakteristische Polynom $p_A = (2 - t)(1 - t)$ woraus schon offensichtlich ist, dass die Nullstellen gerade 2 und 1 sind.

Im Fall der Scherung erhalten wir schließlich $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ und damit das charakteristische Polynom $p_A = (1-t)^2$. Hier ist also 1 eine doppelte Nullstelle des charakteristischen Polynoms, obwohl es nur einen Eigenvektor zum Eigenwert 1 gibt.

7.4. Charakteristisches Polynom und Ähnlichkeit. Bevor wir uns allgemein mit Polynomen beschäftigen, wollen wir noch zeigen, dass ähnliche Matrizen das selbe charakteristische Polynom haben.

Satz 7.4. *Seien $A, B \in M_n(\mathbb{K})$ ähnliche $n \times n$–Matrizen über einem Körper $\mathbb{K}$. Dann haben A und B das gleiche charakteristische Polynom.*

Beweis. Nach Definition gibt es eine invertierbare Matrix $T \in M_n(\mathbb{K})$, sodass $B = TAT^{-1}$ gilt. Für jedes $\lambda \in \mathbb{K}$ ist natürliche $T(\lambda\mathbb{I})T^{-1} = \lambda T\mathbb{I}T^{-1} = \lambda\mathbb{I}$, also ist $B - \lambda\mathbb{I} = T(A - \lambda\mathbb{I})T^{-1}$ für alle $\lambda \in \mathbb{K}$. Damit folgt aus Korollar 6.9 sofort, dass $p_B(\lambda) = p_A(\lambda)$ für alle $\lambda \in \mathbb{K}$ gilt. Für unendliche Körper folgt daraus schon $p_B = p_A$.

Allgemein muss man benutzen, dass auch $B - t\mathbb{I} = T(A - t\mathbb{I})T^{-1}$ als Gleichung für Matrizen von Polynomen gilt. Dann folgt die Aussage aus der Version von Korollar 6.9 für kommutative Ringe mit Einselement. □

Mit Hilfe dieses Satzes können wir nun die Definition des charakteristischen Polynoms auf beliebige lineare Abbildungen $f : V \to V$ ausdehnen, wobei V ein endlichdimensionaler $\mathbb{K}$–Vektorraum ist. Dazu definieren wir einfach $p_f \in \mathbb{K}[t]$ als das charakteristische Polynom der Matrixdarstellung $[f]_{\mathcal{B}}$ bezüglich einer beliebigen Basis $\mathcal{B}$ von V. Wählen wir eine andere Basis, dann erhalten wir nach 6.1 als Matrixdarstellung eine Matrix, die ähnlich zu $[f]_{\mathcal{B}}$ ist, und damit nach dem obigen Satz das gleiche charakteristische Polynom.

Insbesondere folgt daraus, dass jeder Koeffizient des charakteristischen Polynoms p_f von f eine Invariante der linearen Abbildung f ist. Wir werden später auf diesen Gesichtspunkt zurück kommen. Natürlich sind die Nullstellen des charakteristischen Polynoms von f genau die Eigenwerte.

Polynome und ihre Nullstellen

Wie schon angekündigt müssen wir als nächsten Schritt etwas allgemeine Theorie über Polynome entwickeln.

7.5. Der Euklidische Algorithmus. Wie wir uns in 7.3 schon erinnert haben ist der Raum $\mathbb{K}[t]$ aller Polynome mit Koeffizienten in $\mathbb{K}$ nicht nur ein Vektorraum über $\mathbb{K}$ sondern auch ein kommutativer Ring mit Einselement. Das andere offensichtliche Beispiel eines kommutativen Ringes mit Einselement bilden die natürlichen Zahlen $\mathbb{Z}$. Viele der Anwendungen von Polynomen, die wir im weiteren kennen lernen werden beruhen darauf, dass die die Analogie zwischen $\mathbb{K}[t]$ und $\mathbb{Z}$ noch viel weiter geht. So gibt es in $\mathbb{K}[t]$ Analoga von Primzahlen und der eindeutigen Primfaktorzerlegung, die eine große Rolle spielen werden. Die Basis für diese Analogie ist, dass es in beiden Fällen möglich ist, mit Rest zu dividieren (was für Polynome auch schon aus der Schule bekannt ist). Dazu benötigt man (um auszudrücken, dass der Rest klein ist) einen Ersatz für die Ordnung auf $\mathbb{Z}$, den der Grad von Polynomen bildet.

Definition 7.5. Sei $p = \sum a_k t^k \in \mathbb{K}[t]$ ein Polynom mit $p \neq 0$. Dann gibt es nach Definition einen maximalen Index $n \in \mathbb{N}$, sodass $a_n \neq 0$ gilt. Dieses n heißt der *Grad* $\deg(p)$ von p und der Koeffizient a_n heißt der *führende Koeffizient* von p. Äquivalent ist

$\deg(p) = n$ genau dann, wenn $p \in \mathbb{K}_n[t]$ aber $p \notin \mathbb{K}_{n-1}[t]$ gilt. Man nennt ein Polynom $p \in \mathbb{K}[t]$ *monisch*, wenn sein führender Koeffizient 1 ist.

Die Verträglichkeit des Grades von Polynomen mit den algebraischen Operationen ist leicht zu analysieren: Für Polynome $p = \sum a_k t^k$ und $q = \sum b_\ell t^\ell$ ist das Polynome $p + q = \sum c_i t^i$ bestimmt durch $c_i = a_i + b_i$. Damit folgt sofort, dass $\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$, wobei Gleichheit gelten muss, wenn die beiden Grade verschieden sind. Analog ist für $r \in \mathbb{K}$ mit $r \neq 0$ natürlich $\deg(rp) = \deg(p)$. Für das Produkt $pq = \sum d_i t^i$ gilt ja $d_k = \sum_{i=0}^k a_i b_{k-i}$. Ist $\deg(p) = n$ und $\deg(q) = m$, dann ist für $k > n + m$ in dieser Summe natürlich entweder $i > n$ also $a_i = 0$ oder $k - i > m$ also $b_{k-i} = 0$ und es folgt $d_k = 0$. In der Summe, die d_{n+m} definiert sind offensichtlich alle Summanden gleich Null, außer $a_n b_m \neq 0$. Damit gilt für $p, q \neq 0$ offensichtlich $\deg(pq) = \deg(p) + \deg(q)$ und der führende Koeffizient eines Produkts ist das Produkt der führenden Koeffizienten der beiden Faktoren. Damit können wir nun das Resultat über Division von Polynomen mit Rest formulieren ("Euklidischer Algorithmus"), das eigentlich schon aus der Schule bekannt ist:

Lemma 7.5. *Seien $p_1, p_2 \in \mathbb{K}[t]$ Polynome, $p_2 \neq 0$. Dann gibt es eindeutige Polynome $q, r \in \mathbb{K}[t]$, sodass $p_1 = qp_2 + r$ und $r = 0$ oder $\deg(r) < \deg(p_2)$ gilt.*

Beweis. Wir beweisen zunächst die Existenz der Zerlegung. Falls $p_1 = 0$ ist oder $\deg(p_1) < \deg(p_2)$ gilt, dann setzen wir $q = 0$ und $r = p_1$ und beide Eigenschaften sind erfüllt.

Sei also $n := \deg(p_1) \geq \deg(p_2) =: m$. Wir führen wir den Beweis durch Induktion nach n. Seien a_n und b_m die führenden Koeffizienten der beiden Polynome. Dann betrachten wir $\tilde{p}_1 = p_1 - \frac{a_n}{b_m} t^{n-m} p_2$. Nach Konstruktion ist $\deg(\tilde{p}_1) \leq n$. Die Terme in $\tilde{p}_1$, die t^n enthalten sind aber gerade $a_n t^n - \frac{a_n}{b_m} t^{n-m} b_m t^m = 0$, also ist $\deg(\tilde{p}_1) < n$. Nach Induktionsvoraussetzung finden wir Polynome $\tilde{q}$ und $\tilde{r}$, sodass $\tilde{p}_1 = \tilde{q}p_2 + \tilde{r}$ und $\tilde{r} = 0$ oder $\deg(\tilde{r}) < \deg(p_2)$ gelten. Damit ist aber $p_1 - \frac{a_n}{b_m} t^{n-m} p_2 = \tilde{q}p_2 + \tilde{r}$, und setzt man $q = \tilde{q} + \frac{a_n}{b_m} t^{n-m}$ und $r = \tilde{r}$, dann erhält man $p_1 = qp_2 + r$ mit den gewünschten Eigenschaften.

Zur Eindeutigkeit: Ist $qp_2 + r = \tilde{q}p_2 + \tilde{r}$, wobei r und $\tilde{r}$ Null sind oder kleineren Grad als q_2 haben, dann erhalten wir $r - \tilde{r} = (\tilde{q} - q)p_2$. Die linke Seite dieser Gleichung ist entweder Null oder hat Grad $< \deg(p_2)$. Wäre $\tilde{q} - q \neq 0$, dann hätte die rechte Seite Grad $\deg(p_2) + \deg(\tilde{q} - q) \geq \deg(p_2)$ ein Widerspruch. Somit muss $\tilde{q} - q = 0$, also $q = \tilde{q}$ gelten. Daraus folgt sofort $\tilde{r} = r$. □

Beispiel 7.5. Der Induktionsbeweis des Satzes entspricht genau dem aus der Schule bekannten Algorithmus zur Division von Polynomen mit Rest. Betrachten wir zum Beispiel die Division $(t^3 + 2t^2 - t + 1) : (t + 3)$ Im ersten Schritt erhält man t^2 für den Quotienten, und zieht man $t^2(t + 3)$ vom Dividenden ab, dann erhält man $-t^2 - t + 1$. Damit erhält man $-t$ für den Quotienten und Abziehen von $-t(t + 3)$ liefert $2t + 1$. Somit erhält man noch 2 für den Quotienten und $2t + 1 - 2(t + 3) = -5$ für den Rest. Also gilt $t^3 + 2t^2 - t + 1 = (t^2 - t + 2)(t + 3) - 5$.

Mit diesem Resultat können wir aber nun eine Charakterisierung der Nullstellen $\lambda \in \mathbb{K}$ eines Polynoms $p \in \mathbb{K}[t]$ finden:

Satz 7.5. *Sei $p \in \mathbb{K}[t]$ ein Polynom, $p \neq 0$. Dann ist eine Zahl $\lambda \in \mathbb{K}$ genau dann eine Nullstelle von p, wenn das Polynom $t - \lambda$ das Polynom p teilt, d.h. wenn es ein Polynom $q \in \mathbb{K}[t]$ gibt, sodass $p = (t - \lambda)q$ gilt.*

Beweis. Wenden wir den Euklidischen Algorithmus auf p und $(t-\lambda)$ an, dann erhalten wir Polynome $q, r \in \mathbb{K}[t]$ mit $p = (t-\lambda)q+r$ und $r = 0$ oder $\deg(r) < \deg(t-\lambda)$. Damit muss aber r einfach ein Skalar sein. Setzten wir nun in dieser Gleichung λ für t ein, dann erhalten wir $p(\lambda) = 0q(\lambda) + r = r$, und die Behauptung folgt. □

7.6. Vielfachheit von Nullstellen. Der letzte Satz liefert uns sofort einen alternativen Beweise für die Tatsache, dass ein Polynom $p \in \mathbb{K}_n[t]$, $p \neq 0$ höchsten n verschiedene Nullstellen haben kann. Seien nämlich $\lambda_1, \dots, \lambda_k$ verschiedene Nullstellen eines Polynoms $0 \neq p \in \mathbb{K}[t]$. Nach Satz 7.5 gibt es ein Polynom q_1, sodass $p = (t-\lambda_1)q_1$ gilt. Setzen wir nun λ_2 ein, dann erhalten wir $0 = p(\lambda_2) = (\lambda_2 - \lambda_1)q_1(\lambda_2)$. Da $\lambda_2 \neq \lambda_1$ gilt, ist $\lambda_2 - \lambda_1 \neq 0$, also muss $q_1(\lambda_2) = 0$ gelten. Nach Satz 7.5 gibt es somit ein Polynom $q_2 \in \mathbb{K}[t]$, sodass $q_1 = (t-\lambda_2)q_2$ und damit $p = (t-\lambda_1)(t-\lambda_2)q_2$ gilt. Induktiv sehen wir, dass es ein Polynom $q_k \in \mathbb{K}[t]$ geben muss, sodass $p = (t-\lambda_1)(t-\lambda_2)\cdots(t-\lambda_k)q_k$ gilt, was insbesondere $\deg(p) = k + \deg(q_k)$, also $\deg(p) \geq k$ impliziert.

Die algebraische Sichtweise erlaubt uns aber eine feinere Analyse von Nullstellen, indem wir den Begriff der *Vielfachheit* einer Nullstelle einführen. Ist $p \in \mathbb{K}[t]$, $p \neq 0$ und λ eine Nullstelle von p, dann sagt man λ ist eine *k–fache Nullstelle* von p, wenn es ein Polynom $q \in \mathbb{K}[t]$ mit $q(\lambda) \neq 0$ gibt, sodass $p = (t-\lambda)^k q$ gilt. Die Vielfachheit einer Nullstelle ist also gerade die höchste Potenz von $(t-\lambda)$, die das Polynom p noch teilt.

Proposition 7.6. *Sei $p \in \mathbb{K}[t]$ ein Polynom $p \neq 0$, seien $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ verschiedene Nullstellen von p und sei m_j die Vielfachheit von λ_j für $j = 1, \dots, k$. Dann gibt es ein Polynom $q \in \mathbb{K}[t]$, sodass*

$$p = (t-\lambda_1)^{m_1}(t-\lambda_2)^{m_2}\cdots(t-\lambda_k)^{m_k}q$$

gilt. Insbesondere ist $\sum_{j=1}^k m_j \leq \deg(p)$, also kann ein Polynom vom Grad n, mit Vielfachheit gezählt, nur höchstens n Nullstellen haben.

Beweis. Wir beweisen die Aussage durch Induktion nach k. Nach Definition gibt es ein Polynom $q_1 \in \mathbb{K}[t]$, sodass $p = (t-\lambda_1)^{m_1}q_1$ gilt. Nehmen wir induktiv an, dass $i \geq 2$ gilt, und wir ein Polynom q_{i-1} gefunden haben, sodass $p = (t-\lambda_1)^{m_1}\cdots(t-\lambda_{i-1})^{m_{i-1}}q_{i-1}$ gilt. Nun ist aber $p(\lambda_i) = 0$, und wenn wir λ_i in die rechte Seite einsetzen, dann erhalten wir einen Faktor ungleich Null mal $q_{i-1}(\lambda_i)$. Also muss $q_{i-1}(\lambda_i) = 0$ und damit $q_{i-1} = (t-\lambda_i)q_{i,1}$ für ein Polynom $q_{i,1} \in \mathbb{K}[t]$ gelten. Ist $m_i = 1$, dann können wir einfach $q_i := q_{i,1}$ setzen und erhalten $q_{i-1} = (t-\lambda_i)^{m_i}q_i$.

Ist $m_i > 1$, dann wissen wir nach Definition der Vielfachheit, dass es ein Polynom $\tilde{q}$ gibt, sodass $p = (t-\lambda_i)^{m_i}\tilde{q}$ gilt. Setzen wir oben für q_{i-1} ein, dann erhalten wir

$$p = (t-\lambda_i)(t-\lambda_1)^{m_1}\cdots(t-\lambda_{i-1})^{m_{i-1}}q_{i,1} = (t-\lambda_i)(t-\lambda_i)^{m_i-1}\tilde{q}.$$

Wegen der Eindeutigkeit in Lemma 7.5 folgt

$$(t-\lambda_1)^{m_1}\cdots(t-\lambda_{i-1})^{m_{i-1}}q_{i,1} = (t-\lambda_i)^{m_i-1}\tilde{q}.$$

Die rechte Seite hat λ_i als Nullstelle, also können wir wie oben $q_{i,1}(\lambda_i) = 0$, also $q_{i,1} = (t-\lambda_i)q_{i,2}$ und damit $q_{i-1} = (t-\lambda_i)^2 q_{i,2}$ für ein Polynom $q_{i,2} \in \mathbb{K}[t]$ folgern. Ist $m_i = 2$, dann setzen wir $q_i = q_{i,2}$ und erhalten $q_{i-1} = (t-\lambda_i)^{m_i}q_i$. Sonst können wir weiter Faktoren $(t-\lambda_i)$ abspalten, bis wir ein Polynom $q_i := q_{i,m_i}$ erreichen, für das $q_{i-1} = (t-\lambda_i)^{m_i}q_i$. Damit folgt die Darstellung von p mittels Induktion und die zweite Aussage ist eine unmittelbare Konsequenz. □

7.7. Existenz von Nullstellen. Nachdem wir gesehen haben, dass die Anzahl (mit Vielfachheit gezählt) der Nullstellen eines Polynoms durch den Grad des Polynoms beschränkt ist, wenden wir uns der (viel schwierigeren) Frage der Existenz von Nullstellen zu. Insbesondere hängt die Existenz von Nullstellen stark von dem Körper ab, den wir betrachten. Zum Beispiel können wir ein Polynom $p \in \mathbb{Q}[t]$ auch als Polynom mit Koeffizienten in $\mathbb{R}$ oder $\mathbb{C}$ betrachten. Das Polynom $t^2 - 2$ zum Beispiel hat in $\mathbb{R}$ die Nullstellen $\sqrt{2}$ und $-\sqrt{2}$, aber es hat keine Nullstellen in $\mathbb{Q}$, weil $\sqrt{2}$ irrational ist. Natür lich sind diese beiden Nullstellen auch die einzigen Nullstellen in $\mathbb{C}$. Das Polynom $t^2 + 1 \in \mathbb{Q}[t]$ hat weder in $\mathbb{Q}$ noch in $\mathbb{R}$ Nullstellen, währen in $\mathbb{C}$ die Nullstellen i und $-i$ sind.

Überraschenderweise kommen Existenzresultate für Nullstellen eher aus der Analysis als aus der Algebra. So können wir zum Beispiel leicht sehen, dass ein Polynom $p \in \mathbb{R}[t]$ mit $\deg(p) = 3$ in $\mathbb{R}$ immer eine Nullstelle haben muss. Betrachten wir so ein Polynom, dann können wir natürlich durch den führenden Koeffizienten dividieren ohne die Nullstellen zu ändern, also genügt es, ein Polynom der Form $p = t^3 + at^2 + bt + c$ für $a, b, c \in \mathbb{R}$ zu betrachten. Betrachten wir p als Funktion $p : \mathbb{R} \to \mathbb{R}$, dann behaupten wir, dass $\lim_{\lambda \to \pm\infty} p(\lambda) = \pm\infty$ gilt. Das folgt ganz einfach, weil wir für $\lambda \neq 0$ den Wert $p(\lambda)$ als $\lambda^3(1 + \frac{a}{\lambda} + \frac{b}{\lambda^2} + \frac{c}{\lambda^3})$ schreiben können und für $\lambda \to \pm\infty$ die Klammer gegen Eins geht. Insbesondere bedeutet das, dass es Zahlen $\lambda_1, \lambda_2 \in \mathbb{R}$ mit $\lambda_1 < 0$ und $\lambda_2 > 0$ gibt, die außerdem $p(\lambda_1) < 0$ und $p(\lambda_2) > 0$ erfüllen. Nach dem Zwischenwertsatz der Analysis muss die stetige Funktion p auf dem Intervall (λ_1, λ_2) auch alle Werte annehmen, die zwischen $p(\lambda_1)$ und $p(\lambda_2)$ liegen, also muss insbesondere zwischen λ_1 und λ_2 eine Nullstelle von p liegen. Analog sieht man die Existenz mindestens einer Nullstelle für jedes Polynom ungeraden Grades über $\mathbb{R}$.

Der wichtigste Satz über Nullstellen von Polynomen ist der *Fundamentalsatz der Algebra*, der zeigt, dass über dem Körper $\mathbb{C}$ keine Probleme mit Nullstellen auftreten. Über $\mathbb{C}$ kann jedes Polynom als Produkt von Polynomen ersten Grades geschrieben werden und damit hat ein Polynom $p \in \mathbb{C}[t]$ vom Grad n genau n Nullstellen (mit Vielfachheit gezählt). Auch bei diesem Satz ist der Beweis eher analytisch. Daher passt er nicht wirklich in die Vorlesung und wird hier nur der Vollständigkeit halber präsentiert. Wir setzen im Beweis einige Kenntnisse aus der Analysis voraus.

Satz 7.7 (Fundamentalsatz der Algebra). *Sei $p \in \mathbb{C}[t]$ ein Polynom mit $\deg(p) \geq 1$. Dann besitzt p mindestens eine Nullstelle in $\mathbb{C}$.*

Beweis. Die Vorschrift $f(z) := |p(z)|$ definiert eine stetige Funktion $f : \mathbb{C} \to \mathbb{R}$, und $f(z) \geq 0$ für alle $z \in \mathbb{C}$. Der erste Schritt des Beweises ist zu zeigen, dass diese Funktion ein globales Minimum besitzt, d.h. ein $z_0 \in \mathbb{C}$ existiert, sodass $f(z_0) \leq f(z)$ für alle $z \in \mathbb{C}$ gilt. Falls p eine Nullstelle hat ist das offensichtlich, also nehmen wir an, dass $f(z) > 0$ für alle z gilt.

Für eine reelle Zahl $R > 0$ betrachten wir die Teilmenge $B_R := \{z \in \mathbb{C} : |z| \leq R\} \subset \mathbb{C} = \mathbb{R}^2$. Diese Teilmenge ist beschränkt und abgeschlossen, also kompakt, also besitzt die Einschränkung der stetigen Funktion f auf B_R nach dem Satz vom Maximum ein Maximum und ein Minimum. Schreiben wir andererseits $p = a_n t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0$, dann gilt für $z \in \mathbb{C} \setminus \{0\}$ die Gleichung

$$p(z) = a_n z^n \left(1 + \frac{a_{n-1}}{a_n z} + \dots + \frac{a_1}{a_n z^{n-1}} + \frac{a_0}{a_n z^n}\right).$$

Nehmen wir den Betrag der rechten Seite, dann erhalten wir $|a_n||z|^n|(1 + \dots)|$, und für $|z| \to \infty$ geht das gegen ∞. Somit gibt es für jedes $C > 0$ eine Zahl $R > 0$, sodass

$f(z) > C$ für alle $z \in \mathbb{C}$ mit $|z| > R$ gilt. Sei nun $\tilde{z}_0$ der Punkt, an dem die Einschränkung von f auf B_1 ihr Minimum annimmt und sei $C := f(\tilde{z}_0) > 0$ dieses Minimum. Dann gibt es dazu einen entsprechenden Wert $\tilde{R}$. Sei nun $R := \max\{1, \tilde{R}\}$ und $z_0 \in B_R$ ein Punkt, an dem die Einschränkung von f auf B_R ihr Minimum annimmt. Weil $R \geq 1$ ist, ist $f(z_0) \leq C$. Nach Definition ist $f(z_0) \leq f(z)$ für alle $z \in B_R$. Andererseits ist nach Konstruktion $f(z) > C = f(z_0)$ für alle $z \in \mathbb{C}$ mit $|z| > R$. Damit ist aber $f(z_0) \leq f(z)$ für alle $z \in \mathbb{C}$, also nimmt f ein absolutes Minimum bei z_0 an.

Der zweite Schritt des Beweises besteht nun darin zu zeigen, dass ein positiver Wert niemals ein globales Minimum von f sein kann. Nehmen wir zunächst an, dass $z_0 = 0$ gilt. Natürlich ist $a_0 = p(0) \neq 0$. Weil der Grad von p mindestens Eins ist, gibt es einen kleinsten Index $m \in \{1, \dots, n\}$, sodass $a_m \neq 0$ ist. Dann ist $p = a_0 + a_m t^m + t^{m+1}q$, wobei $q \in \mathbb{C}[t]$ gegeben ist durch $a_{m+1} + a_{m+2}t + \dots + a_n t^{n-m-1}$. Wir können $-\frac{a_0}{a_m} \in \mathbb{C}$ in Polarkoordinaten schreiben, also finden wir eine eindeutige reelle Zahl $r > 0$ und einen eindeutigen Winkel $\varphi \in [0, 2\pi)$, sodass $-\frac{a_0}{a_m} = re^{i\varphi}$ gilt. Setzen wir $z_1 = r^{1/m}e^{i(\varphi/m)}$, dann ist $z_1^m = -\frac{a_0}{a_m}$. Für $\lambda \in [0,1] \subset \mathbb{R}$ betrachten wir nun $p(\lambda z_1) = a_0 + a_m\lambda^m z_1^m + \lambda^{m+1}z_1^{m+1}q(\lambda z_1)$. Nach Konstruktion ist der zweite Summand gerade $-a_0\lambda^m$, und wir erhalten

$$p(\lambda z_1) = a_0 \left(1 - \lambda^m + a_0^{-1}\lambda^{m+1}z_1^{m+1}q(\lambda z_1)\right).$$

Aus Stetigkeitsgründen gibt es eine Zahl $C > 0$, sodass $|a_0^{-1}z_1^{m+1}q(\lambda z_1)| < C$ für alle $\lambda \in [0,1]$ gilt. Damit erhalten wir aber $|p(\lambda z_1)| \leq |a_0||(1 - \lambda^m + C\lambda^{m+1})|$. Für $0 < \lambda < 1/C$ ist aber $0 < 1 - C\lambda < 1$, und damit sicher auch $0 < 1 - \lambda^m(1 - C\lambda) < 1$. Damit ist aber $|p(\lambda z_1)| < |a_0| = p(0)$, also 0 kein globales Minimum.

Im Fall von beliebigem $z_0 \in \mathbb{C}$ bemerken wir, dass es Koeffizienten $b_0, \dots, b_n$ gibt, sodass $a_n z^n + \dots + a_0 = b_n(z - z_0)^n + b_{n-1}(z - z_0)^{n-1} + \dots + b_1(z - z_0) + b_0$ gilt. Dazu muss man nur $z = z_0 + (z - z_0)$ zu den Potenzen $2, \dots, n$ erheben, und dann einsetzen. Insbesondere sehen wir, dass $b_0 = p(z_0)$ gelten muss. Die Tatsache, dass $z \mapsto |a_n z^n + \dots + a_1 z + a_0|$ ein globales Minimum bei z_0 hast, übersetzt sich nun natürlich direkt in die Tatsache, dass $z \mapsto |b_n z^n + \dots + b_1 z + b_0|$ ein globales Minimum bei 0 hat. Nach dem letzten Schritt folgt daraus aber $0 = b_0 = p(z_0)$. □

Korollar 7.7. *Sei $p \in \mathbb{C}[t]$ ein Polynom mit $\deg(p) = n > 0$. Dann gibt es Elemente $a_n \in \mathbb{C} \setminus \{0\}$, $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ und $m_1, \dots, m_k \in \mathbb{N}$ mit $m_1 + \dots + m_k = n$, sodass $p = a_n(t - \lambda_1)^{m_1} \cdots (t - \lambda_k)^{m_k}$. Insbesondere zerfällt jedes solche Polynom in ein Produkt von Polynomen ersten Grades und es hat genau $\deg(p)$ viele Nullstellen, wenn man die Nullstellen mit Vielfachheit zählt.*

Beweis. Durch Induktion nach n. Für $n = 1$ ist $p = a_1 t + a_0$ mit $a_1 \neq 0$, und das können wir als $a_1(t - \lambda_1)$ schreiben, wobei $\lambda_1 = -\frac{a_0}{a_1}$.

Nehmen wir also an, dass $n > 1$ gilt und der Satz für Polynome vom Grad $n - 1$ schon bewiesen wurde. Dann hat p nach dem Satz eine Nullstelle $\lambda \in \mathbb{C}$, also gibt es nach Satz 7.5 ein Polynom $q \in \mathbb{C}[t]$ vom Grad $n - 1$, sodass $p = (t - \lambda)q$ gilt. Wendet man auf q die Induktionsvoraussetzung an, dann folgt die Behauptung. □

Bemerkung 7.7. (1) Ein Körper $\mathbb{K}$ in dem jedes Polynom $p \in \mathbb{K}[t]$ in ein Produkt von Polynomen ersten Grades zerfällt heißt *algebraisch abgeschlossen*. Der Fundamentalsatz der Algebra sagt also gerade, dass $\mathbb{C}$ algebraisch abgeschlossen ist. Die Körper $\mathbb{Q}$ und $\mathbb{R}$ sind nicht algebraisch abgeschlossen, weil etwa das Polynom $t^2 + 1$ in diesen Körpern keine Nullstelle besitzt. Auch die Körper $\mathbb{Z}_p$ für p eine Primzahl sind nicht algebraisch abgeschlossen.

(2) Der Beweis des Fundamentalsatzes der Algebra ist nicht konstruktiv. Er gibt uns also keinen Hinweis, wie wir Nullstellen eines gegebenen Polynoms über $\mathbb{C}$ konkret finden können. Im Allgemeinen ist das auch ein schwieriges Problem. Für quadratische Polynome gibt es natürlich die schon aus der Schule bekannte Formel: Wir können durch den führenden Koeffizienten dividieren ohne die Nullstellen zu ändern, also dürfen wir ohne Beschränkung der Allgemeinheit ein Polynom der Form $t^2 + at + b$ betrachten. Ist das gleich $(t - \lambda_1)(t - \lambda_2)$, dann folgt sofort $a = -(\lambda_1 + \lambda_2)$ und $b = \lambda_1\lambda_2$. Damit ist aber $(\lambda_1 - \lambda_2)^2 = (\lambda_1 + \lambda_2)^2 - 4\lambda_1\lambda_2 = a^2 - 4b$. Daraus erhalten wir aber sofort $\lambda_{1,2} = \frac{\lambda_1+\lambda_2}{2} \pm \frac{\lambda_1-\lambda_2}{2} = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$.

Für Polynome dritten und vierten Grades gibt es noch allgemeine (aber deutlich kompliziertere) Lösungsformeln. Für Polynome vom Grad ≥ 5 wurde um 1820 von N.H. Abel und E. Galois bewiesen, das man Lösungen nicht durch endlich Anwendung der Grundrechnungsarten und des Wurzelziehens bilden kann. Insbesondere gibt es also keine allgemeinen Lösungsformeln, die nur diese Operationen benutzen. Diese Beweise beruhen auf der (heute so genannten) Galois–Theorie, die eine Verbindung zwischen der Theorie der Körper, der Theorie der Polynome und der Gruppentheorie darstellt.

Wir werden uns nicht weiter mit dem Problem des Findens von Nullstellen komplexer Polynome beschäftigen, weil die vielen verfügbaren (algebraischen und/oder numerischen) Methoden zum Finden solcher Nullstellen über den Rahmen dieser Vorlesung weit hinausgehen würden. Im Fall von Polynomen vom Grad ≥ 3 werden wir uns auf Beispiele beschränken, in denen man genügend viele Nullstellen erraten kann, um das Problem durch Divisionen auf quadratische Polynome zurückführen zu können.

7.8. Nullstellen reeller Polynome. Der Fundamentalsatz der Algebra liefert uns auch Informationen über reelle Polynome. Ist nämlich $p \in \mathbb{R}[t]$ ein Polynom vom Grad $n \geq 1$, dann können wir p wegen $\mathbb{R} \subset \mathbb{C}$ natürlich auch als komplexes Polynom auffassen. Nach Korollar 7.7 finden wir als n (nicht notwendig verschiedene) komplexe Zahlen $\lambda_1, \dots, \lambda_n$ und $a_n \in \mathbb{C}$, sodass $p = a_n(t - \lambda_1)\cdots(t - \lambda_n)$ gilt. Aus dieser Formel ist offensichtlich, dass a_n gerade der führende Koeffizient von p ist, also gilt $a_n \in \mathbb{R}$. Ist nun $p = a_nt^n + \cdots + a_1t + a_0$, dann ist $a_i \in \mathbb{R}$, also $\bar{a}_i = a_i$. Ist $\lambda \in \mathbb{C}$ eine Nullstelle von p, dann gilt $0 = a_n\lambda^n + \cdots + a_1\lambda + a_0$. Da die komplexe Konjugation mit allen Körperoperationen auf $\mathbb{C}$ verträglich ist, erhalten wir daraus

$$0 = \bar{0} = \bar{a}_n\bar{\lambda}^n + \cdots + \bar{a}_1\bar{\lambda} + \bar{a}_0 = a_n\bar{\lambda}^n + \cdots + a_1\bar{\lambda} + a_0,$$

also ist mit λ automatisch auch $\bar{\lambda}$ eine Nullstelle von p. Andererseits ist $(t-\lambda)(t-\bar{\lambda}) = t^2-(\lambda+\bar{\lambda})t+\lambda\bar{\lambda}$, und $\lambda+\bar{\lambda} = 2\operatorname{Re}(\lambda) \in \mathbb{R}$ und $\lambda\bar{\lambda} = |\lambda|^2 \in \mathbb{R}$, also hat dieses Polynom reelle Koeffizienten. Somit erhalten wir

Korollar 7.8. *Sei $p \in \mathbb{R}[t]$ ein Polynom vom Grad $n \geq 1$. Dann gibt es eine Zahl $k \leq n$, sodass $n-k$ gerade ist, k (nicht notwendig verschiedene) Zahlen $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ und $\ell := \frac{n-k}{2}$ monische Polynome $q_1, \dots, q_\ell \in \mathbb{R}[t]$ mit $\deg(q_i) = 2$, sodass*

$$p = a_n(t - \lambda_1)\cdots(t - \lambda_k)q_1\cdots q_\ell.$$

Ein Polynom $p \in \mathbb{R}[t]$ zerfällt also genau dann in in Produkt von Polynomen ersten Grades, wenn alle Nullstellen des komplexen Polynoms p im Teilkörper $\mathbb{R} \subset \mathbb{C}$ liegen. Die Sprechweise "alle Nullstellen von p liegen in $\mathbb{K}$", anstatt "p zerfällt in ein Produkt von Polynomen ersten Grades" ist auch für allgemeine Körper üblich. Der Grund dafür ist, dass man zu einem beliebigen Körper $\mathbb{K}$ einen (im wesentlichen eindeutigen) algebraisch abgeschlossenen Körper $\tilde{\mathbb{K}}$ konstruieren kann, der $\mathbb{K}$ als Teilkörper enthält.

Dieser Körper heißt der *algebraische Abschluss* von $\mathbb{K}$. Über $\tilde{\mathbb{K}}$ zerfällt dann jedes Polynom $p \in \mathbb{K}[t]$ in ein Produkt von Polynomen ersten Grades und das gilt genau dann auch über $\mathbb{K}$ wenn alle Nullstellen von p im Teilkörper $\mathbb{K} \subset \tilde{\mathbb{K}}$ liegen. Der Beweis für die Existenz des algebraischen Abschlusses geht weit über den Rahmen dieser Vorlesung hinaus, wir werden diese Tatsache aber gelegentlich noch verwenden.

Anwendung auf das charakteristische Polynom

Wir wollen nun unser allgemeinen Resultate über Polynome im Spezialfall von charakteristischen Polynomen anwenden. Wir werden die Resultate oft entweder nur für Matrizen oder nur für lineare Abbildungen formulieren, die nötige Umformulierung für den jeweils anderen Fall ist offensichtlich.

7.9. Zunächst können wir aus der Definition sofort den Grad des charakteristischen Polynoms, sowie seinen höchsten Koeffizienten und den konstanten Koeffizienten bestimmen.

Satz 7.9. *Sei $A \in M_n(\mathbb{K})$ eine $n \times n$–Matrix über einem Körper $\mathbb{K}$ mit charakteristischem Polynom $p_A \in \mathbb{K}[t]$. Dann ist $\deg p_A = n$, der führende Koeffizient von p_A ist $(-1)^n$ und der konstante Koeffizient ist $\det(A)$.*

Beweis. Sei $B = (b_{ij}) = (A - t\mathbb{I})$ als Matrix von Polynomen betrachtet. Dann ist $\deg(b_{ij}) = 0$ für $i \neq j$ und $\deg(b_{ii}) = 1$ für alle i und der führende Koeffizient von b_{ii} ist -1. Nach Satz 6.6 ist

$$p_A = \det(B) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) b_{\sigma(1)1} \cdots b_{\sigma(n)n},$$

wobei $\mathfrak{S}_n$ die Menge aller Permutationen der Menge $\{1, \dots, n\}$ bezeichnet. Für $\sigma = \mathrm{id}$ erhalten wir ein Produkt von n Polynomen ersten Grades also ein Polynom vom Grad n, und nach Definition des Produktes von Polynomen ist der führende Koeffizient eines Produktes das Produkt der führenden Koeffizienten. Damit erhalten wir $(-1)^n$ als führenden Koeffizienten dieses Summanden. In allen anderen Summanden treten auch Faktoren auf, die Grad Null besitzen, also erhalten wir Polynome vom Grad $< n$, also hat die Summe Grad n und führenden Koeffizienten $(-1)^n$. Wegen $p_A(\lambda) = \det(A - \lambda\mathbb{I})$ erhalten wir natürlich sofort $p_A(0) = \det(A)$, und das ist der konstante Koeffizient von p_A. □

Bemerkung 7.9. Das charakteristische Polynom liefert überraschende weitere Informationen über die Struktur der Teilmenge $GL(n, \mathbb{R})$ aller invertierbaren $n \times n$–Matrizen des Vektorraumes $M_n(\mathbb{R}) = \mathbb{R}^{n^2}$. Aus 6.10 wissen wir ja schon, dass $GL(n, \mathbb{R})$ eine offene Teilmenge von $\mathbb{R}^{n^2}$ ist. Jetzt können wir beweisen, dass diese Menge auch *dicht* ist, also beliebig nahe bei einer gegeben Matrix A invertierbare Matrizen liegen.

Ist nämlich $A \in M_n(\mathbb{R})$ beliebig, dann betrachten wir das charakteristische Polynom p_A von A als Funktion $\mathbb{R} \to \mathbb{R}$. Falls $p_A(\lambda) \neq 0$ ist, dann ist $\det(A - \lambda\mathbb{I}) \neq 0$, also $A - \lambda\mathbb{I}$ eine invertierbare Matrix. Da aber p_A ein Polynom vom Grad $n \geq 1$ ist, hat es nach Proposition 7.6 höchstens n verschiedene Nullstellen. Insbesondere bedeutet das, dass es zu jedem $\varepsilon > 0$ eine Zahl λ mit $|\lambda| < \varepsilon$ gibt, sodass $p_A(\lambda) \neq 0$ gilt. Das bedeutet aber gerade, dass beliebig nahe bei A invertierbare Matrizen liegen. Insbesondere hat das die nützliche Konsequenz, dass eine stetige Funktion $F : M_n(\mathbb{R}) \to \mathbb{R}^m$, die $F(A) = 0$ für jede invertierbare Matrix A erfüllt, schon identisch Null sein muss.

An dieser Stelle stellt sich die Frage, ob die charakteristischen Polynome von Matrizen spezielle Eigenschaften haben (die etwa beim Finden von Nullstellen helfen könnten). Das ist aber (abgesehen vom führenden Koeffizienten, den wir in Satz 7.9 bestimmt haben) nicht der Fall:

Proposition 7.9. *Sei $\mathbb{K}$ ein Körper und sei $p = (-1)^n t^n + b_{n-1}t^{n-1} + \dots + b_1 t + b_0 \in \mathbb{K}[t]$ ein Polynom vom Grad n mit führendem Koeffizienten $(-1)^n$. Dann gibt es eine Matrix $A \in M_n(\mathbb{K})$ mit charakteristischem Polynom $p_A = p$.*

Beweis. Betrachten wir die Matrix $A = (a_{ij})$, die gegeben ist durch $a_{i+1,i} = 1$ für $i = 2, \dots, n$, $a_{jn} = (-1)^{n-1} b_{j-1}$ für $j = 1, \dots, n$ und alle anderen $a_{ij} = 0$. Wir beweisen mit Induktion nach n, dass $p_A = (-1)^n t^n + b_{n-1}t^{n-1} + \dots + b_1 t + b_0$ gilt.

Für den Induktionsanfang betrachten wir den Fall $n = 2$, also die Matrix $\left(\begin{smallmatrix} 0 & -b_0 \\ 1 & -b_1 \end{smallmatrix}\right)$. Das charakteristische Polynom dieser Matrix ist offensichtlich $(-t)(-b_1 - t) - (-b_0) = t^2 + b_1 t + b_0$.

Nehmen wir also induktiv an, dass $n \geq 3$ gilt, und die Behauptung für $(n-1) \times (n-1)$–Matrizen schon bewiesen ist. Entwickeln wir nun die Determinante von $A - t\mathbb{I}$ nach der ersten Zeile, so erhalten wir nur zwei Summanden. Der erste dieser Summanden ist $(-t)$ mal die Determinante der Matrix die entsteht, wenn man in $A - t\mathbb{I}$ die erste Zeile und die erste Spalte streicht. Nach Induktionsvoraussetzung ist diese Determinante aber $(-1)^{n-1}t^{n-1} - b_{n-1}t^{n-2} - \dots - b_2 t - b_1$, also liefert dieser Summand schon $p - b_0$. Der andere Summand ist aber gerade $(-1)^{n+1}(-1)^{n-1}b_0 = b_0$ mal der Determinante der Matrix die entsteht, wenn man in $A - t\mathbb{I}$ die erste Zeile und die letzte Spalte streicht. Die resultierende Matrix ist aber eine obere Dreiecksmatrix mit lauter Einsen auf der Hauptdiagonale, hat also nach Korollar 6.6 (2) Determinante Eins. □

Dieses Resultat zeigt, dass Finden von Eigenwerten von beliebigen Matrizen über $\mathbb{K}$ äquivalent zum Finden von Nullstellen von beliebigen Polynomen über $\mathbb{K}$, und somit ein schwieriges Problem ist.

7.10. Die algebraische Vielfachheit. Da wir ja wissen, dass die Nullstellen des charakteristischen Polynoms genau die Eigenwerte einer linearen Abbildung (oder einer Matrix) sind, können wir nun natürlich das Konzept der Vielfachheit einer Nullstelle auf Eigenwerte übertragen.

Definition 7.10. Die *algebraische Vielfachheit* eines Eigenwertes λ einer Matrix $A \in M_n(\mathbb{K})$ bzw. einer linearen Abbildung f ist die Vielfachheit der Nullstelle λ des charakteristischen Polynoms p_A bzw. p_f.

Satz 7.10. *Sei V ein n–dimensionaler $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung. Dann gilt:*

(1) Für jeden Eigenwert λ von f ist die algebraische Vielfachheit zumindest so groß wie die geometrischen Vielfachheit aus 7.2.

(2) Die Summe der algebraischen Vielfachheiten aller Eigenwerte von f ist $\leq n$ und falls das charakteristische Polynome von f in ein Produkt von Polynomen ersten Grades zerfällt, ist die Summe der algebraischen Vielfachheiten gleich n.

Beweis. (1) Sei V_λ^f der Eigenraum zum Eigenwert λ. Seine Dimension ist nach Definition die geometrische Vielfachheit von λ. Ist diese geometrische Vielfachheit gleich k, dann betrachten wir eine Basis $\{v_1, \dots, v_k\}$ für V_λ^f und erweitern diese zu einer Basis $\mathcal{B} := \{v_1, \dots, v_n\}$ von V. Nach Konstruktion ist dann $f(v_i) = \lambda v_i$ für $i = 1, \dots, k$, also hat die Matrixdarstellung $[f]_\mathcal{B}$ von f bezüglich dieser Basis die Blockform $\begin{pmatrix} \lambda\mathbb{I}_k & A \\ 0 & B \end{pmatrix}$

für $A \in M_{k,n-k}(\mathbb{K})$ und $B \in M_{n-k,n-k}(\mathbb{K})$. Berechnen wir nun das charakteristische Polynom dieser Matrix, dann können wir k–mal nach der ersten Spalte entwickeln, und erhalten $p_f = (\lambda - t)^k \det(B - t\mathbb{I})$. Somit sehen wir, dass die algebraische Vielfachheit von λ zumindest gleich k ist.

(2) folgt sofort aus Proposition 7.6. □

7.11. Charakterisierung von Diagonalisierbarkeit. Mit Hilfe unserer Resultate über charakteristische Polynome können wir nun eine vollständige Charakterisierung diagonalisierbarer linearer Abbildungen beweisen:

SATZ 7.11. *Sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$. Dann ist eine lineare Abbildung $f : V \to V$ genau dann diagonalisierbar über $\mathbb{K}$, wenn*

(a) *das charakteristische Polynom p_f von f über $\mathbb{K}$ in ein Produkt von Polynomen ersten Grades zerfällt und*

(b) *für jeden Eigenwert von f die algebraische Vielfachheit mit der geometrischen Vielfachheit übereinstimmt.*

BEWEIS. Ist f diagonalisierbar, dann sei $\mathcal{B}$ eine Basis aus Eigenvektoren. Die Matrixdarstellung $[f]_{\mathcal{B}}$ ist dann eine Diagonalmatrix. Sind $\lambda_1, \dots, \lambda_n$ die Eintragungen auf der Hauptdiagonale, dann ist das charakteristische Polynom dieser Matrix (also das charakteristische Polynom von f) gegeben durch $(\lambda_1 - t) \cdots (\lambda_n - t)$ und zerfällt somit in Produkt von Polynomen ersten Grades. Ist λ einer der Eigenwerte, dann ist die Anzahl der Basisvektoren, die diesem Eigenwert entsprechen, genau die algebraische Vielfachheit des Eigenwertes und diese Vektoren sind linear unabhängig. Somit muss die Dimension des Eigenraumes V_f^λ mindestens gleich der algebraischen Vielfachheit von λ sein, und damit folgt Bedingung (b) aus Satz 7.10(1).

Nehmen wir umgekehrt an, dass die Bedingungen (a) und (b) erfüllt sind. Seien $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von f und sie m_i die algebraische Vielfachheit von λ_i. Aus Bedingung (a) und Satz 7.10(2) folgt nun, dass $\sum m_i = n$ gilt, und wegen Bedingung (b) ist m_i gleich der geometrischen Vielfachheit von λ_i. Damit ist aber f nach Satz 7.2 diagonalisierbar. □

Damit können wir nun ein vollständiges Schema angeben, wie man entscheidet, ob eine Matrix $A \in M_n(\mathbb{K})$ diagonalisierbar ist, und wie man sie explizit diagonalisiert, d.h. eine invertierbare Matrix T findet, sodass TAT^{-1} eine Diagonalmatrix ist.

(i) Berechne das charakteristische Polynom $p_A \in \mathbb{K}[t]$ und finde seine Nullstellen. Zerfällt dieses Polynom nicht in ein Produkt von Polynomen ersten Grades, dann kann A nicht diagonalisierbar sein. Ansonsten seien λ_i die verschiedenen Eigenwerte von A und m_i ihre algebraischen Vielfachheiten.

(ii) Sind alle $m_i = 1$, also alle λ_i verschieden, dann ist A diagonalisierbar, also ähnlich zu einer Diagonalmatrix mit den Eintragungen $\lambda_1, \dots, \lambda_n$ auf der Hauptdiagonale. Ist das nicht der Fall, dann bestimme für jene m_i, die größer als 1 sind, die geometrische Vielfachheit n_i von λ_i. Diese Vielfachheit ist die Dimension des Kerns der linearen Abbildung $A - \lambda_i\mathbb{I}$, also gilt $n_i = n - \operatorname{rg}(A - \lambda\mathbb{I})$ und dieser Rang kann mit Hilfe des Gauß'schen Algorithmus bestimmt werden. Die Matrix A ist nun genau dann diagonalisierbar, wenn $n_i = m_i$ für alle i mit $m_i > 1$ gilt.

(iii) Möchte man für diagonalisierbares A eine invertierbare Matrix $T \in M_n(\mathbb{K})$ finden, sodass TAT^{-1} diagonal ist, dann geht man wie folgt vor: Für jeden Eigenwert λ_i bestimme mit Hilfe des Gauß'schen Algorithmus eine Basis $\{v_1^i, \dots, v_{n_i}^i\}$ für den Raum der Lösungen des homogenen lineare Gleichungssystems $(A - \lambda_i\mathbb{I})x = 0$. Dann wissen wir aus unseren allgemeinen Resultaten, dass $\{v_1^1, \dots, v_{n_k}^k\}$ eine Basis $\mathcal{B}$ für $\mathbb{K}^n$ ist. Bezeichnen wir mit $\mathcal{S}$ die Standardbasis, dann ist die Matrix mit Spaltenvektoren $v_1^1, \dots, v_{n_k}^k$ gerade $[\mathrm{id}]_{\mathcal{S}}^{\mathcal{B}}$. Bezeichnen wir mit f die lineare Abbildung $x \mapsto Ax$, dann ist $A = [f]_{\mathcal{S}}$, und nach Korollar 4.17 von [**1**] ist damit $[\mathrm{id}]_{\mathcal{B}}^{\mathcal{S}} A [\mathrm{id}]_{\mathcal{S}}^{\mathcal{B}} = [f]_{\mathcal{B}}$, also eine Diagonalmatrix. Da $[\mathrm{id}]_{\mathcal{B}}^{\mathcal{S}} = ([\mathrm{id}]_{\mathcal{S}}^{\mathcal{B}})^{-1}$ gilt, erhält man die Matrix T indem man mit Hilfe des Algorithmus aus 3.9 von [**1**] die Matrix mit Spaltenvektoren $v_1^1, \dots, v_{n_k}^k$ invertiert.

Hat man es mit einer linearen Abbildung $f : V \to V$ auf einem beliebigen endlichdimensionalen Vektorraum zu tun, dann geht man analog vor. Zunächst wählt man eine beliebige Basis $\mathcal{B}$ von V und bestimmt die Matrixdarstellung $A := [f]_{\mathcal{B}}$. Wie oben kann man dann aus A das charakteristische Polynom $p_A = p_f$, sowie die Eigenwerte und ihre algebraischen und geometrischen Vielfachheiten bestimmen. Die Lösungen von $(A - \lambda_i \mathbb{I})x = 0$ sind dann gerade die Koordinatendarstellungen von Eigenvektoren bezüglich der Basis $\mathcal{B}$, und damit kann man dann eine Basis $\mathcal{B}'$ von V angeben, die aus Eigenvektoren für f besteht.

Beispiel 7.11. (1) Betrachten wir die Matrix $A = \begin{pmatrix} 3 & -1 & -1 \\ 2 & 1 & -2 \\ 0 & -1 & 2 \end{pmatrix} \in M_3(\mathbb{R})$. Nach der Regel von Sarrus erhält man für das charakteristische Polynom

$$p_A = (3-t)(1-t)(2-t) + 2 - 2(3-t) + 2(2-t) = (3-t)(2-t)(1-t).$$

Somit hat A drei verschiedene Eigenwerte, nämlich 1, 2 und 3 und muss daher diagonalisierbar sein. Eigenvektoren zu diesen Eigenwerten kann man leicht durch Lösen von linearen Gleichungssystemen bestimmen. Betrachten wir etwa den Eigenwert 1, dann müssen wir die Gleichung $Bx = 0$ für $B = \begin{pmatrix} 2 & -1 & -1 \\ 2 & 0 & -2 \\ 0 & -1 & 1 \end{pmatrix}$ lösen. Wenden wir darauf den Gauß'schen Algorithmus an, dann erhalten wir

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

Setzt man $x_3 = 1$, so erhält man $x_2 = 1$ und $2x_1 = 2$, also $x_1 = 1$, und damit ist $(1, 1, 1)$ ein Eigenvektor zum Eigenwert 1.

(2) Sei nun $A = \begin{pmatrix} 2 & -2 & 1 \\ 3 & -1 & 1 \\ -1 & 2 & 0 \end{pmatrix} \in M_3(\mathbb{R})$. Mit Hilfe der Regel von Sarrus berechnet man das charakteristische Polynom von A als

$$p_A = (2-t)(-1-t)(-t) + 6 + 2 + (-1-t) - 2(2-t) - 6t = -t^3 + t^2 - 3t + 3.$$

Offensichtlich ist 1 eine Nullstelle dieses Polynoms, und dividiert man p_A durch $(t - 1)$, dann erhält man $-(t^2 + 3)$. Das letztere Polynom hat über $\mathbb{R}$ offensichtlich keine Nullstellen, also kann A über $\mathbb{R}$ nicht diagonalisierbar sein. Über $\mathbb{C}$ hat dieses Polynom natürlich die Nullstellen $\pm i\sqrt{3}$, also ist A über $\mathbb{C}$ diagonalisierbar mit Eigenwerten 1, $i\sqrt{3}$ und $-i\sqrt{3}$. Eigenvektoren kann man wie zuvor durch Lösen von linearen Gleichungssystemen finden.

(3) Ist $A = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} \in M_3(\mathbb{R})$, dann erhalten wir als charakteristisches Polynom $(2-t)^3 - 1 - 1 - (2-t) - (2-t) - (2-t) = -t^3 + 6t^2 - 3t = -t(t-3)^2$. Damit hat A die Eigenwerte 0 und 3 mit algebraischen Vielfachheiten 1 bzw. 2. Offensichtlich ist $(1,1,1)$ ein Eigenvektor zum Eigenwert 0. Für den Eigenwert 3 müssen wir die Gleichung $Bx = 0$ lösen, wobei alle drei Zeilen von B gerade $(-1,-1,-1)$ sind. Das bedeutet aber sofort, dass B den Rang 1 hat, also der Eigenwert 3 auch geometrische Vielfachheit 2 besitzt. Somit ist A diagonalisierbar. Eine Basis des Eigenraumes zum Eigenwert 3 erhält man natürlich, indem man in obigen Gleichungssystem die Lösungen mit $x_2 = 1$ und $x_3 = 0$ bzw. die mit $x_2 = 0$, $x_3 = 1$ berechnet. Das liefert aber gerade $(-1,1,0)$ und $(-1,0,1)$. Betrachten wir also die Basis $\mathcal{B} = \{(1,1,1),(-1,1,0),(-1,0,1)\}$ und bezeichnen wir mit $\mathcal{S}$ die Standardbasis, dann ist $[\mathrm{id}]_{\mathcal{B},\mathcal{S}} = \begin{pmatrix} 1 & -1 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Berechnet man mit Hilfe des Algorithmus aus 3.9 von [**1**] die inverse dieser Matrix, dann erhält man die explizite Diagonalisierung

$$\begin{pmatrix} 1/3 & 1/3 & 1/3 \\ -1/3 & 2/3 & -1/3 \\ -1/3 & -1/3 & 2/3 \end{pmatrix} \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

(4) Betrachte den Raum $\mathbb{R}[x]_n$ der Polynome vom Grad $\leq n$ und den Ableitungsoperator $D : \mathbb{R}[x]_n \to \mathbb{R}[x]_n$. Man kann D einfach algebraisch durch $D(\sum a_j x^j) := \sum j a_j x^{j-1}$ definieren. Betrachten wir die Basis $\mathcal{B} = \{1, x, x^2, \dots, x^n\}$, dann ist $D(x^j) = jx^{j-1}$, also erhalten wir $A := [D]_{\mathcal{B}} = (a_{ij})$, wobei $a_{ij} = 0$ für $j \neq i+1$ und $a_{i,i+1} = i$. Betrachten wir nun $A - t\mathbb{I}$, dann ist das eine obere Dreiecksmatrix, und alle Eintragungen auf der Hauptdiagonale sind gleich $-t$. Nach Korollar 6.5 ist $p_D = \det(A - t\mathbb{I}) = (-1)^n t^n$. Das bedeutet aber, dass 0 der einzige Eigenwert von D ist. Wäre D diagonalisierbar, dann gäbe es eine Basis aus Eigenvektoren zum Eigenwert 0, also wäre D die Nullabbildung. Tatsächlich liegt hier ein extremer Fall vor: Die Matrix A hat ja Zeilenstufenform, und daraus sieht man sofort, dass $\mathrm{rg}(A) = \mathrm{rg}(D) = n - 1$ gilt. Damit ist aber die Dimension des Kerns von D, die ja nach Definition genau die geometrische Vielfachheit des Eigenwertes 0 ist, gleich Eins.

Die Spur

Aus 7.4 wissen wir bereits, dass ähnliche Matrizen das gleiche charakteristische Polynom haben. Insbesondere ist jeder Koeffizient des charakteristischen Polynoms einer beliebigen Matrixdarstellung eine Invariante einer linearen Abbildung. Nach Satz 7.9 ist die Determinante einer dieser Koeffizienten. Wir werden nun einen weiteren dieser sogenannten *charakteristischen Koeffizienten* kennen lernen, der sogar um einiges einfacher ist als die Determinante.

7.12. Sei $A \in M_n(\mathbb{K})$ eine $n \times n$–Matrix mit charakteristischem Polynom p_A. Dann ist es ziemlich einfach, den Koeffizienten von t^{n-1} in p_A berechnen. Setzen wir nämlich $B = A - t\mathbb{I} = b_{ij}$ und betrachten die Leibniz Formel

$$p_A = \det(B) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) b_{\sigma(1)1} \cdots b_{\sigma(n)n}$$

als Produkt von Polynomen. Nach Definition hat für $i \neq j$ das Polynom b_{ij} den Grad Null, während jedes b_{ii} Grad Eins hat. Ist aber $\sigma \neq \mathrm{id}$ eine Permutation, dann gilt $\sigma(i) \neq i$ für mindestens zwei Indizes i, also kann der entsprechende Summand höchstens Grad $n-2$ haben. Damit kommen aber alle Beiträge zum Koeffizienten von t^{n-1} aus dem Summanden $(a_{11}-t)\cdots(a_{nn}-t)$, der $\sigma = \mathrm{id}$ entspricht. Der Koeffizient von t^{n-1} in diesem Produkt ist aber offensichtlich $(-1)^{n-1}(a_{11}+\cdots+a_{nn})$. Das motiviert die folgende Definition.

Definition 7.12. Sei $A = (a_{ij}) \in M_n(\mathbb{K})$. Dann definieren wir die *Spur* (englisch “trace”) $\mathrm{tr}(A)$ von A durch $\mathrm{tr}(A) := a_{11}+\cdots+a_{nn}$, also die Summe der Elemente auf der Hauptdiagonale.

Proposition 7.12. *(1) Die Spurabbildung* $\mathrm{tr} : M_n(\mathbb{K}) \to \mathbb{K}$ *ist linear.*

(2) Ähnliche Matrizen haben die gleiche Spur. Allgemeiner gilt für $A, B \in M_n(\mathbb{K})$ *die Gleichung* $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Beweis. (1) ist aus der Definition offensichtlich und der erste Teil von (2) ist klar, weil die Spur ein Koeffizient des charakteristischen Polynoms ist.

Also müssen wir nur die letzte Behauptung beweisen. Ist $A = (a_{ij})$ und $B = (b_{ij})$, dann sind die Hauptdiagonalelemente von AB gegeben durch $\sum_j a_{ij}b_{ji}$. Damit ist aber $\mathrm{tr}(AB) = \sum_i \sum_j a_{ij}b_{ji}$, und dieser Ausdruck ist offensichtlich unabhängig von der Reihenfolge von A und B. $\square$

Bemerkung 7.12. (1) Die Aussage, dass $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ für alle $A, B \in M_n(\mathbb{K})$ gilt impliziert die Aussage, dass ähnliche Matrizen gleiche Spur haben. Man rechnet einfach $\mathrm{tr}(TAT^{-1}) = \mathrm{tr}(T^{-1}TA) = \mathrm{tr}(A)$.

(2) Für eine 2×2–Matrix A kennen wir nun das vollständige charakteristische Polynom, weil $p_A = t^2 - \mathrm{tr}(A)t + \det(A)$ gilt.

(3) Die Proposition impliziert natürlich, dass man die Spur einer linearen Abbildung als die Spur einer beliebigen Matrixdarstellung definieren kann. Die Spur ist ein ganz simples Kriterium um Ähnlichkeit von Matrizen auszuschließen.

KAPITEL 8

Exkurs: Normalformen

In diesem Kapitel werden wir unsere Beschäftigung mit der Frage, wie möglichst einfache Matrixdarstellungen einer linearen Abbildung von einem Vektorraum $\mathbb{K}$ auf sich selbst aussehen, abschließen. Wir werden diese Frage nicht für allgemeine Körper beantworten können, immerhin aber für $\mathbb{C}$ (und allgemein für algebraisch abgeschlossene Körper) und für $\mathbb{R}$. Auch in diesen Fällen werden wir aber einige Beweise nur skizzieren. Technisch gesehen ist der wichtigste Teil dieses Kapitels die enge Beziehung der Frage von Normalformen zur Theorie der Polynome. Diese Verbindung ist auch der Grund dafür, dass in diesem Bereich die Resultate stark vom betrachteten Körper abhängen, weil sich eben auch Polynome über verschiedenen Körpern ganz verschieden benehmen.

Invariante Teilräume und Triangulierbarkeit

Einer der wesentlichen Schritte in Richtung einfacher Matrixdarstellungen für eine lineare Abbildung $f : V \to V$ ist, den Raum V in Teilräume zu zerlegen, auf denen die Einschränkung von f einfach aussieht. Diese Idee wird uns auch relativ leicht die Antwort auf die Frage liefern, welche linearen Abbildungen durch obere Dreiecksmatrizen dargestellt werden können.

8.1. Invariante Teilräume. Sei V ein $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung. Für einen beliebigen Teilraum W von V kann man zwar f auf W einschränken und somit auch als lineare Abbildung $f : W \to V$ betrachten, aber da dies keine Abbildung von einem Vektorraum auf sich selbst ist, können wir damit nicht viel anfangen. Somit liegt es nahe, Teilräume W von V zu betrachten, sodass $f(W) \subset W$ gilt. Diese Teilräume nennt man *f–invariant* oder einfach *invariant*, wenn klar ist, welche lineare Abbildung gemeint ist. Ist W ein f–invarianter Teilraum, dann können wir die Einschränkung von f auf W wiederum als lineare Abbildung $f : W \to W$ betrachten.

Insbesondere sind Eigenräume von f immer invariante Teilräume. Ist nämlich $v \in V_\lambda^f$, dann ist $f(v) = \lambda v \in V_\lambda^f$, also $f(V_\lambda^f) \subset V_\lambda^f$. Die Einschränkung von f auf V_λ^f ist natürlich gerade $\lambda \operatorname{id}_{V_\lambda^f}$. Ein Eigenraum ist somit ein invarianter Teilraum, auf dem f als Vielfaches der Identität wirkt.

Als nächsten Schritten erinnern wir uns an den Begriff des Quotientenraumes aus Abschnitt 5.1 von [**1**]. Für einen beliebigen Teilraum $W \subset V$ und ein Element $v \in V$ betrachtet man die *Nebenklasse* $v + W := \{v + w : w \in W\}$ von v bezüglich W. Geometrisch gesehen ist das einfach eine durch v verschobene Kopie von W. Anders gesagt ist $v + W$ die Äquivalenzklasse von v bezüglich der Äquivalenzrelation $v \sim v'$ genau dann, wenn $v' - v \in W$. Der *Quotientenraum* V/W ist dann die Menge aller dieser Nebenklassen, also $V/W = \{v+W : v \in V\}$, also die Menge aller zu W parallelen affinen Teilräume. Es gibt eine offensichtlich Abbildung $\pi : V \to V/W$, die durch $\pi(v) = v+W$ gegeben ist, also jedes Element von V auf seine Äquivalenzklasse abbildet.

Man verifiziert leicht, dass man V/W in natürlicher Weise zu einem Vektorraum machen kann, indem man $(v+W)+(v'+W) := (v+v')+W$ und $r(v+W) := rv+W$ setzt. Das ist äquivalent dazu, dass die kanonische Quotientenabbildung $\pi : V \to V/W$ linear ist. Offensichtlich ist π surjektiv und $\mathrm{Ker}(\pi) = W$. Somit ist für endlichdimensionales V auch V/W endlichdimensional und $\dim(V/W) = \dim(V) - \dim(W)$.

Schließlich benötigen wir noch die universelle Eigenschaft des Quotienten. Diese beschreibt, wann man eine lineare Abbildung $\varphi : V \to Z$ in einen beliebigen Vektorraum Z in der Form $\varphi = \tilde{\varphi} \circ \pi$ für eine lineare Abbildung $\tilde{\varphi} : V/W \to Z$ schreiben kann. Nach Proposition 5.2 von [**1**] geht das genau dann, wenn $W \subset \mathrm{Ker}(\varphi)$ gilt, und in diesem Fall ist die lineare Abbildung $\tilde{\varphi}$ eindeutig bestimmt. Explizit ist diese Abbildung durch $\tilde{\varphi}(v + W) = \varphi(v)$ gegeben, und das ist wohldefiniert, weil für $v' \in v + W$ ja $v' - v \in W$ und daher $0 = \varphi(v' - v) = \varphi(v') - \varphi(v)$ gilt.

Ist insbesondere $f : V \to V$ eine lineare Abbildung und W ein f–invarianter Teilraum von V, dann können wir $\pi \circ f : V \to V/W$ betrachten. Für $w \in W$ ist $f(w) \in W$, also $\pi \circ f(w) = 0$, also ist $W \subset \mathrm{Ker}(\pi \circ f)$, und wir finden eine (eindeutige) lineare Abbildung $\underline{f} : V/W \to V/W$, sodass $\pi \circ f = \underline{f} \circ \pi$ gilt. Explizit ist diese Abbildung durch $\underline{f}(v+W) = f(v)+W$ gegeben, und man kann auch leicht direkt verifizieren, dass das wohldefiniert und linear ist, und die gewünschte Eigenschaft hat.

Wir können nun diese Begriffe auch schön in Termen von Matrixdarstellungen charakterisieren. Dazu ist es günstig, folgende Sprechweise einzuführen. Angenommen, wir haben eine Matrix $M = (m_{ij}) \in M_n(\mathbb{K})$, sodass für ein $k < n$ gilt, dass $m_{ij} = 0$ ist, sofern $i > k$ und $j \leq k$ ist, als in den ersten k Spalten Eintragungen ungleich Null nur in den ersten k Zeilen vorkommen. Dann sagen wir einfach, dass M eine Blockform der Form $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ mit $A \in M_k(\mathbb{K})$, $B \in M_{k,n-k}(\mathbb{K})$ und $C \in M_{n-k}(\mathbb{K})$ hat. Beachte, dass die Teilmatrizen A und C wieder quadratisch sind, während B rechteckig ist.

Proposition 8.1. *Sei V ein n–dimensionaler Vektorraum über einem Körper $\mathbb{K}$ und $f : V \to V$ eine lineare Abbildung. Dann gilt: Es gibt genau dann einen k–dimensionalen f–invarianten Teilraum $W \subset V$, wenn bezüglich einer geeigneten Basis $\mathcal{B}$ von V die Matrixdarstellung von f eine Blockform $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ für $A \in M_k(\mathbb{K})$, $B \in M_{k,n-k}(\mathbb{K})$ und $C \in M_{n-k}(\mathbb{K})$ besitzt. Ist das der Fall, dann ist A eine Matrixdarstellung der Einschränkung $f|_W : W \to W$ und C ist eine Matrixdarstellung der induzierten Abbildung $\underline{f} : V/W \to V/W$.*

Beweis. Ist $W \subset V$ ein k–dimensionaler f–invarianter Teilraum, dann wählen wir eine Basis $\mathcal{B}' := \{v_1, \dots, v_k\}$ für W und ergänzen sie zu einer Basis $\mathcal{B} = \{v_1, \dots, v_n\}$ von V. Da W invariant ist, gilt insbesondere $f(v_i) \in W$ für $i = 1, \dots, k$. Damit kann jedes dieser $f(v_i)$ als Linearkombination von $v_1, \dots, v_k$ geschrieben werden, also haben die ersten k–Spalten $[f(v_1)]_{\mathcal{B}}, \dots, [f(v_k)]_{\mathcal{B}}$ von $[f]_{\mathcal{B}}$ nur in den ersten k–Zeilen Eintragungen ungleich Null. Das bedeutet aber gerade, dass $[f]_{\mathcal{B}}$ die verlangte Blockform besitzt. Außerdem ist nach Konstruktion der Block $A \in M_k(\mathbb{K})$ genau $[f|_W]_{\mathcal{B}'}$.

Die kanonische lineare Quotientenabbildung $\pi : V \to V/W$ ist surjektiv, und ihr Kern ist genau W. Nach dem Beweis des Dimensionssatzes für lineare Abbildungen aus 4.12 von [**1**] ist die Menge $\mathcal{B}'' = \{\pi(v_{k+1}), \dots, \pi(v_n)\}$ eine Basis für V/W. Für $j = 1, \dots, n-k$ gilt aber nach Konstruktion $f(v_{k+j}) = b_{1,j}v_1 + \dots + b_{k,j}v_k + c_{1,j}v_{k+1} + \dots + c_{n-k,j}v_n$, wobei $B = (b_{ij})$ und $C = (c_{ij})$. Damit ist aber

$$\underline{f}(\pi(v_{k+j})) = \pi(f(v_{k+j})) = c_{1,j}\pi(v_{k+1}) + \dots + c_{n-k,j}\pi(v_n),$$

also ist C die Matrixdarstellung $[\tilde{f}]_{\mathcal{B}''}$.

Ist umgekehrt $\mathcal{B} = \{v_1, \dots, v_n\}$ eine Basis von V, sodass die Matrixdarstellung $[f]_{\mathcal{B}}$ die angegebene Blockform hat, dann sei $W := \langle v_1, \dots, v_k \rangle$ der von den ersten k

Basisvektoren erzeugen Teilraum. Wegen der Blockform der Matrix ist $f(v_i) \in W$ für $i = 1, \dots, k$, also $f(W) \subset W$. $\square$

8.2. Charakteristisches Polynom und invariante Teilräume. Ist $f : V \to V$ eine lineare Abbildung auf einem endlichdimensionalen $\mathbb{K}$–Vektorraum und ist $W \subset V$ ein f–invarianter Teilraum, dann erhalten wir die Einschränkung $f|_W : W \to W$ und die induzierte Abbildung $\underline{f} : V/W \to V/W$. Natürlich ist nicht alle Information über f in diesen beiden Abbildungen enthalten. In Termen der Matrixdarstellung aus Satz 8.1 merkt man sich nur die Blöcke A und C und vergisst alle Information, die im Block B enthalten ist. Interessanterweise verliert man aber keine Information über das charakteristische Polynom. Dazu benötigen wir noch ein Resultat:

Proposition 8.2. *Für eine Matrix in Blockform wie in Satz 8.1 gilt* $\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A)\det(C)$.

Beweis. Durch Induktion nach k. Ist $k = 1$, dann ist $A = a_{11}$, B der Rest der ersten Zeile und C gerade die Matrix die entsteht, indem man in der gesamten Matrix die erste Zeile und die erste Spalte streicht. Damit folgt die Behauptung aber sofort durch Entwickeln nach der ersten Spalte, siehe Satz 6.7.

Nehmen wir also an, dass $k \geq 2$ gilt und der Satz für Blöcke der Größe $k-1$ bereits bewiesen ist. Wie in 6.7 bezeichnen wir mit A_{ij} die Matrix, die aus $A = (a_{ij})$ durch Streichen der i–ten Zeile und der j–ten Spalte entsteht. Weiters sei B_j die Matrix die aus B durch Streichen der j–ten Zeile entsteht. Entwickeln wir nun die Determinante nach der ersten Spalte, dann erhalten wir

$$\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \sum_{j=1}^{k} (-1)^{1+j} a_{j1} \det \begin{pmatrix} A_{j1} & B_j \\ 0 & C \end{pmatrix}.$$

Nach Induktionsvoraussetzung ist die letzte Determinante gleich $\det(A_{j1})\det(C)$, und wir erhalten $\left(\sum_{j=1}^{k} (-1)^{1+j} a_{j1} \det(A_{j1})\right) \det(C) = \det(A)\det(C)$. $\square$

Korollar 8.2. *Sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$, $f : V \to V$ eine lineare Abbildung, $W \subset V$ ein f–invarianter Teilraum, $f|_W : W \to W$ die Einschränkung von f und $\underline{f} : V/W \to V/W$ die induzierte Abbildung. Dann gilt für die charakteristischen Polynome $p_f = p_{f|_W} p_{\underline{f}}$.*

Beweis. Wähle eine Basis $\mathcal{B}$ für V, sodass $[f]_{\mathcal{B}}$ Blockform wie in Satz 8.1 hat, dann berechne $p_f = \det([f]_{\mathcal{B}} - t\mathbb{I})$ mit Hilfe von Proposition 8.2. $\square$

8.3. Triangulierung linearer Abbildungen. Mit Hilfe der Resultate über das charakteristische Polynom können wir nun ein nützliches Zwischenresultat beweisen, nämlich welche linearen Abbildungen durch obere Dreiecksmatrizen dargestellt werden können.

Satz 8.3. *Sei V ein n–dimensionaler Vektorraum über einem Körper $\mathbb{K}$. Dann sind für eine lineare Abbildung $f : V \to V$ äquivalent:*

(1) Es gibt f–invariante Teilräume $W_1 \subset W_2 \subset \dots \subset W_{n-1} \subset V$ mit $\dim(W_j) = j$.

(2) Es gibt eine Basis $\mathcal{B}$ für V, sodass $[f]_{\mathcal{B}}$ eine obere Dreiecksmatrix ist (siehe 6.5).

(3) Das charakteristische Polynom von f zerfällt in ein Produkt von Polynomen ersten Grades, d.h. alle Eigenwerte von f liegen in $\mathbb{K}$.

Beweis. (1) $\implies$ (2): Sind $W_1 \subset \cdots \subset W_{n-1} \subset V$ invariante Teilräume mit $\dim(W_j) = j$, dann wählen wir eine Basis $\{v_1\}$ für W_1, erweitern sie zu einer Basis $\{v_1, v_2\}$ für W_2, und so weiter bis wir zu einer Basis $\{v_1, \dots, v_{n-1}\}$ von W_{n-1} gelangen, die wir schließlich zu einer Basis $\mathcal{B} = \{v_1, \dots, v_n\}$ für V erweitern. Ist nun $[f]_{\mathcal{B}} = (a_{ij})$, dann besagt die Tatsache, dass jedes W_i invariant ist gerade, dass $f(v_i)$ als Linearkombination von $v_1, \dots, v_i$ geschrieben werden kann. Damit ist aber $a_{ij} = 0$ falls $i > j$, also $[f]_{\mathcal{B}}$ eine obere Dreiecksmatrix.

(2) $\implies$ (3): Sei $\mathcal{B}$ eine Basis von V, sodass $[f]_{\mathcal{B}} = (a_{ij})$ eine obere Dreiecksmatrix ist. Nach Korollar 6.6 ist dann aber $p_f = \det([f]_{\mathcal{B}} - t\mathbb{I}) = (a_{11} - t) \cdots (a_{nn} - t)$, also zerfällt p_f in ein Produkt von Polynomen ersten Grades.

(3) $\implies$ (1): Durch Induktion nach n. Ist $n = 1$, dann ist nichts zu beweisen. Nehmen wir also an, dass $n \geq 2$ gilt, und die Behauptung für lineare Abbildungen auf Vektorräumen der Dimension $n - 1$ bereits gezeigt ist. Sei $f : V \to V$ eine lineare Abbildung, deren charakteristisches Polynom in ein Produkt von Polynomen ersten Grades zerfällt. Dann hat f mindestens einen Eigenwert λ und zu diesem Eigenwert gibt es einen Eigenvektor $v \neq 0$. Somit ist $W_1 := \{rv : r \in \mathbb{K}\}$ ein eindimensionaler Teilraum von V, der wegen $f(v) = \lambda v$ invariant ist. Betrachte nun den Quotienten V/W_1 und die induzierte lineare Abbildung $\underline{f} : V/W_1 \to V/W_1$. Nach Satz 5.1 von [**1**] ist $\dim(V/W_1) = \dim(V) - \dim(W_1) = n - 1$. Außerdem ist nach Korollar 8.2 $p_f = (\lambda - t)p_{\underline{f}}$, also zerfällt auch $p_{\underline{f}}$ in ein Produkt von Polynomen ersten Grades. Damit gibt es aber nach Induktionsvoraussetzung invariante Teilräume $\tilde{W}_1 \subset \cdots \subset \tilde{W}_{n-2} \subset V/W_1$ mit $\dim(\tilde{W}_j) = j$. Nun definieren wir $W_j := \pi^{-1}(\tilde{W}_{j-1})$ für $j = 2, \dots, n$, wobei $\pi : V \to V/W_1$ die kanonische lineare Quotientenabbildung ist.

Als Urbild eines Teilraumes unter einer linearen Abbildung ist jedes W_j ein Teilraum, und weil $W_1 = \mathrm{Ker}(\pi)$ gilt ist $W_1 \subset W_2 \subset \cdots \subset W_{n-1} \subset V$. Weiters bildet π den Teilraum W_i surjektiv auf $\tilde{W}_{i-1}$ ab und hat Kern W_1, also ist nach dem Dimensionssatz für lineare Abbildungen $\dim(W_i) = \dim(W_1) + \dim(\tilde{W}_{i-1}) = i$. Schließlich folgt aus $v \in W_i$, $i \geq 2$ nach Definition $\pi(v) \in \tilde{W}_{i-1}$ und da dieser Teilraum invariant ist, gilt $\underline{f}(\pi(v)) \subset \tilde{W}_{i-1}$. Nun ist aber $\underline{f}(\pi(v)) = \pi(f(v))$, also gilt $f(v) \in W_i$ und somit ist jedes W_i ein invarianter Teilraum. □

Korollar 8.3. *Sei V ein endlichdimensionaler $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung, deren charakteristisches Polynom in ein Produkt von Polynomen ersten Grades zerfällt. Dann ist $\det(f)$ das Produkt aller Eigenwerte von f und $\mathrm{tr}(f)$ die Summe aller Eigenwerte von f (jeweils mit Vielfachheiten genommen).*

Beweis. Nach Satz 8.3 finden wir eine Basis $\mathcal{B}$ von V, sodass $A = [f]_{\mathcal{B}} = (a_{ij})$ eine obere Dreiecksmatrix ist. Nach Korollar 6.5 ist $p_f = p_A = \det(A - t\mathbb{I})$ gegeben durch $(-1)^n(t - a_{11}) \cdots (t - a_{nn})$, also sind die a_{ii} genau die Eigenwerte von f. Wiederum nach Korollar 6.5 ist aber $\det(A) = \det(f) = a_{11} \cdots a_{nn}$ und nach Definition ist $\mathrm{tr}(A) = \mathrm{tr}(f) = a_{11} + \cdots + a_{nn}$. □

Aus Satz 7.8 wissen wir, dass über dem Körper $\mathbb{C}$ *jedes* Polynom in ein Produkt von Polynomen ersten Grades zerfällt. Insbesondere können also lineare Abbildungen auf endlichdimensionalen komplexen Vektorräumen immer durch obere Dreiecksmatrizen dargestellt werden, und auch der Zusammenhang zwischen Eigenwerten, Determinante und Spur aus Korollar 8.3 ist über $\mathbb{C}$ immer gegeben. Analoges gilt nach Bemerkung 7.8 für jeden algebraisch abgeschlossenen Körper.

8.4. Summenzerlegungen und Projektionen. Wie wir bereits bemerkt haben, verliert man Informationen, wenn man eine lineare Abbildung durch ihre Einschränkung auf einen invarianten Teilraum und die induzierte Abbildung auf dem Quotienten nach diesem Teilraum ersetzt. Deshalb kann man auch mit dieser Methode nicht mehr als die obere Dreiecksgestalt erreichen, die zwar technisch sehr nützlich, aber doch noch recht weit von einer endgültigen Normalform entfernt ist.

Um noch weiter zu kommen, müssen wir Zerlegungen von V in eine direkte Summe von invarianten Teilräumen finden. In der Sprache von Abschnitt 4.9 von [**1**] bedeutet das gerade, dass wir invariante Teilräume finden müssen, die ein invariantes Komplement besitzen. Dort haben wir definiert, dass V die *direkte Summe* von zwei Teilräumen $W_1, W_2 \subset W$ ist und das als $V = W_1 \oplus W_2$ geschrieben, wenn $W_1 + W_2 = V$ und $W_1 \cap W_2 = \{0\}$ gilt. In Proposition 4.9 von [**1**] haben wir gesehen, dass man die Bedingung $W_1 + W_2 = V$ auch durch $\dim(W_1) + \dim(W_2) = \dim(V)$ ersetzen kann. Weiters haben wir bewiesen, dass $V = W_1 \oplus W_2$ genau dann gilt, wenn jedes Element $v \in V$ eindeutig in der Form $v = w_1 + w_2$ mit $w_1 \in W_1$ und $w_2 \in W_2$ geschrieben werden kann. Bezeichnet man diese Elemente mit $p_1(v) := w_1$ und $p_2(v) := w_2$, dann erhält man Abbildungen $p_1, p_2 : V \to V$. Wir können direkte Summenzerlegungen auch über diese Abbildungen charakterisieren, was zur Beschreibung der Invarianz sehr günstig sein wird:

Proposition 8.4. *(1) Sei $V = W_1 \oplus W_2$. Dann sind die Abbildungen $p_1, p_2 : V \to V$ linear, es gilt $p_i \circ p_i = p_i$ und $\operatorname{Im}(p_i) = W_i$ für $i = 1, 2$, $p_1 \circ p_2 = p_2 \circ p_1 = 0$ und $p_1 + p_2 = \mathrm{id}_V$.*

(2) Ist umgekehrt $p_1 : V \to V$ eine lineare Abbildung, die $p_1 \circ p_1 = p_1$ erfüllt, dann gilt $V = \operatorname{Im}(p_1) \oplus \operatorname{Ker}(p_1)$. Setzt man $p_2 = \mathrm{id} - p_1$, dann gilt $p_2 \circ p_2 = p_2$, $p_2 \circ p_1 = p_1 \circ p_2 = 0$ und $\operatorname{Im}(p_2) = \operatorname{Ker}(p_1)$.

Beweis. (1) Ist $v = w_1 + w_2$ und $r \in \mathbb{K}$, dann ist $rv = rw_1 + rw_2$, also $p_i(rv) = rp_i(v)$ für $i = 1, 2$. Ist $v' = w_1' + w_2'$ ein weiteres Element von V, dann ist $v + v' = (w_1 + w_1') + (w_2 + w_2')$, also folgt $p_i(v + v') = p_i(v) + p_i(v')$, also sind p_1 und p_2 linear.

Für $w_1 \in W_1$ ist die eindeutige Darstellung als Summe natürlich durch $w_1 = w_1 + 0$ gegeben, also gilt $p_1(w_1) = w_1$ und $p_2(w_1) = 0$ für alle $w_1 \in W_1$. Wendet man das auf $w_1 = p_1(v)$ an, dann folgt $p_1(p_1(v)) = p_1(v)$, also $p_1 \circ p_1 = p_1$, und $p_2(p_1(v)) = 0$, also $p_2 \circ p_1 = 0$. Analog zeigt man $p_2 \circ p_2 = p_2$ und $p_1 \circ p_2 = 0$. Schließlich gilt $v = p_1(v) + p_2(v)$ nach Konstruktion für alle $v \in V$, also folgt $p_1 + p_2 = \mathrm{id}_V$.

(2) Natürlich sind $\operatorname{Ker}(p_1)$ und $\operatorname{Im}(p_1)$ Teilräume von V. Ist $v \in \operatorname{Ker}(p_1) \cap \operatorname{Im}(p_1)$, dann kann man $v = p_1(v')$ schreiben, und erhält $0 = p_1(v) = p_1(p_1(v')) = p_1(v') = v$, also ist $\operatorname{Ker}(p_1) \cap \operatorname{Im}(p_1) = \{0\}$. Andererseits gilt $\dim(\operatorname{Im}(p_1) = \dim(V) - \dim(\operatorname{Ker}(p_1))$, also $\dim(\operatorname{Ker}(p_1)) + \dim(\operatorname{Im}(p_1)) = \dim(V)$ nach dem Dimensionssatz für lineare Abbildungen (Satz 4.12 von [**1**]). Damit folgt $V = \operatorname{Im}(p_1) \oplus \operatorname{Ker}(p_1)$ aus Proposition 4.9 von [**1**].

Setzt man $p_2(v) = v - p_1(v)$, dann ist sowohl $p_2(p_1(v))$ als auch $p_1(p_2(v))$ gleich $p_1(v) - p_1(p_1(v)) = 0$, also gilt $p_1 \circ p_2 = p_2 \circ p_1 = 0$. Damit ist aber $p_2(p_2(v)) = p_2(v - p_1(v)) = p_2(v) - (p_2 \circ p_1)(v) = p_2(v)$ für alle $v \in V$, also folgt auch $p_2 \circ p_2 = p_2$. Wegen $p_1 \circ p_2 = 0$ folgt nach Definition $\operatorname{Im}(p_2) \subset \operatorname{Ker}(p_1)$. Ist umgekehrt $v \in \operatorname{Ker}(p_1)$, also $p_1(v) = 0$, dann ist $p_2(v) = v - p_1(v) = v$, also $v = p_2(v) \in \operatorname{Im}(p_2)$, also folgt $\operatorname{Ker}(p_1) = \operatorname{Im}(p_2)$. □

Die Abbildungen $p_i : V \to V$ heißen die *Projektionen* zur direkten Summenzerlegung $V = W_1 \oplus W_2$.

Das alles lässt sich relativ einfach auf mehr als zwei Summanden verallgemeinern. Wie im Fall von zwei Teilräumen definiert man die Summe endlich vieler Teilräume als den von der Vereinigung der Teilräume erzeugten Teilraum. Sind $W_1, \dots, W_k$ Teilräume eines Vektorraumes V, dann sagt man, dass V die direkte Summe dieser Teilräume ist, und schreibt $V = W_1 \oplus \dots \oplus W_k$ wenn $V = W_1 + \dots + W_k$ und

$$W_i \cap (W_1 + \dots + W_{i-1} + W_{i+1} + \dots + W_k) = \{0\}$$

für alle $i = 1, \dots, k$ gilt. Es gilt dann wieder, dass $\dim(W_1) + \dots + \dim(W_k) = \dim(V)$ ist, und die Vereinigung von Basen der W_i eine Basis für V bildet. Schließlich kann man jedes Element $v \in V$ eindeutig in der Form $v = w_1 + \dots + w_k$ für $w_i \in W_i$ schreiben, und durch $p_i(v) = w_i$ lineare Abbildungen $p_i : V \to V$ definieren. Diese Abbildungen erfüllen $\mathrm{Im}(p_i) = W_i$ und $p_i \circ p_i = p_i$ für alle i, sowie und $p_i \circ p_j = 0$ für $i \neq j$ und $p_1 + \dots + p_k = \mathrm{id}$.

Gibt man sich umgekehrt lineare Abbildungen p_i mit diesen Eigenschaften vor, dann ist $V = \mathrm{Im}(p_1) \oplus \dots \oplus \mathrm{Im}(p_k)$.

8.5. Invariante Summenzerlegungen. Einer der Vorteile der Charakterisierung von Summenzerlegungen über die zugehörigen Projektionen besteht darin, dass man in dieser Sprache leicht charakterisieren kann, wann alle Summanden invariant unter einer linearen Abbildung $f : V \to V$ sind.

Satz 8.5. *Sei $V = W_1 \oplus W_2$ eine Zerlegung eines n–dimensionalen $\mathbb{K}$–Vektorraumes in eine direkte Summe von Teilräumen mit zugehörigen Projektionen $p_j : V \to V$ für $j = 1, 2$ und sei $f : V \to V$ eine lineare Abbildung. Dann gilt:*

(1) Die Teilräume W_1 und W_2 sind genau dann beide f–invariant, wenn $p_j \circ f = f \circ p_j$ für $j = 1, 2$ gilt.

(2) Die Existenz einer f–invarianten Summenzerlegung $V = W_1 \oplus W_2$ mit $\dim(W_1) = k$, ist äquivalent zur Existenz einer Basis $\mathcal{B}$ für V sodass $[f]_{\mathcal{B}}$ eine Blockgestalt der Form $\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$ ("Blockdiagonalform") mit $A \in M_k(\mathbb{K})$ und $C \in M_{n-k}(\mathbb{K})$ besitzt. In diesem Fall ist A ein Matrixdarstellung von $f|_{W_1}$ und C eine Matrixdarstellung von $f|_{W_2}$.

Beweis. (1) Natürlich ist für $v = w_1 + w_2$ auch $f(v) = f(w_1) + f(w_2)$. Sind W_1 und W_2 beide f–invariant, dann ist $f(w_i) \in W_i$ für $i = 1, 2$, also ist das die eindeutige Zerlegung von $f(v)$. Damit ist aber $p_1(f(v)) = f(w_1) = f(p_1(v))$ und $p_2(f(v)) = f(w_2) = f(p_2(v))$, also folgt $p_i \circ f = f \circ p_i$ für $i = 1, 2$.

Ist umgekehrt $f \circ p_1 = p_1 \circ f$, dann gilt für $w_1 \in W_1$ natürlich $f(w_1) = f(p_1(w_1)) = p_1(f(w_1)) \in W_1$. Analog folgt $f(W_2) \subset W_2$ aus $f \circ p_2 = p_2 \circ f$.

(2) Sie zunächst $V = W_1 \oplus W_2$ eine f–invariante Summenzerlegung mit $\dim(W_1) = k$. Dann wählen wir eine Basis $\mathcal{B}_1 = \{v_1, \dots, v_k\}$ für W_1 und eine Basis $\mathcal{B}_2 = \{v_{k+1}, \dots, v_n\}$ für W_2 und setzen $\mathcal{B} = \{v_1, \dots, v_n\}$. Nach dem Beweis des Dimensionssatzes für Summen (Proposition 4.8 in [**1**]) ist $\mathcal{B}$ eine Basis für V. Da W_1 f–invariant ist, liegt für $i = 1, \dots, k$ das Bild $f(v_i)$ in W_1, und kann daher als Linearkombination von $v_1, \dots, v_k$ geschrieben werden. Daher kann für diese i der Koordinatenvektor $[f(v_i)]_{\mathcal{B}}$ Eintragungen ungleich Null nur in den ersten k Zeilen haben. Analog folgt, dass für $i > k$ der Koordinatenvektor $[f(v_i)]_{\mathcal{B}}$ Eintragungen ungleich Null nur in den letzten $n - k$ Zeilen haben kann, was genau die gewünschte Blockform liefert. Nach Konstruktion ist dann $A = [f|_{W_1}]_{\mathcal{B}_1}$ und $C = [f|_{W_2}]_{\mathcal{B}_2}$.

Ist umgekehrt $\mathcal{B} = \{v_1, \dots, v_n\}$ eine Basis für V, sodass $[f]_{\mathcal{B}}$ die angegebene Blockform hat. Dann bezeichnen wir mit W_1 den von $v_1, \dots, v_k$ aufgespannten Teilraum von

V und mit W_2 den von $v_{k+1}, \dots, v_n$ aufgespannten Teilraum. Die Blockform von $[f]_{\mathcal{B}}$ bedeutet dann genau, dass beide Teilräume f–invariant sind.

Weiters kann offensichtlich jedes $v \in V$ in der Form $v = w_1 + w_2$ für $w_i \in W_i$ geschrieben werden, also ist $V = W_1 + W_2$. Da $\dim(V) = \dim(W_1) + \dim(W_2)$ gilt, folgt aus dem Dimensionssatz für Summen sofort, dass $\dim(W_1 \cap W_2) = 0$ und damit $V = W_1 \oplus W_2$ gilt. □

Der zweite Teil zeigt, dass man im Fall einer Zerlegung in eine direkte Summe von invarianten Teilräumen keine Informationen verliert, wenn man von f auf die Einschränkungen von f auf die Teilräume W_j übergeht. Dies bietet also eine echte Chance, das Problem des Findens schöner Matrixdarstellungen von einem Raum auf einen Teilraum zu reduzieren.

Wiederum verallgemeinern sich diese Überlegungen ohne große Probleme auf mehrere Summanden. Für eine Zerlegung $V = W_1 \oplus \dots \oplus W_k$ mit zugehörigen Projektionen p_i ist genau dann jeder Summand W_i ein f–invarianter Teilraum, wenn $f \circ p_i = p_i \circ f$ für alle $i = 1, \dots, k$ gilt. Im zweiten Teil der Aussage erhält man dann natürlich Blockdiagonalmatrizen mit k Blöcken entlang der Hauptdiagonale.

Beispiel 8.5. Einen Hinweis, wie man Zerlegungen in eine invariante direkte Summe finden könnte, liefert uns das Beispiel einer diagonalisierbaren linearen Abbildung $f : V \to V$. Seien $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von f und für jedes i sei $W_i := V^f_{\lambda_i}$ der Eigenraum zum Eigenwert λ_i. Nach dem Beweis von Satz 7.2 ist die Vereinigung von Basen dieser Eigenräume eine Basis für V und daraus folgt leicht, dass $V = W_1 \oplus \dots \oplus W_k$ gilt. In diesem Fall kann man die Projektionen $p_j : V \to W_j$ relativ einfach erraten:

Betrachten wir die linearen Abbildungen $f - \lambda_i \operatorname{id}$ für $i = 1, \dots, k$. Dann rechnet man sofort nach, dass

$$(f - \lambda_i \operatorname{id}) \circ (f - \lambda_j \operatorname{id}) = f \circ f - (\lambda_i + \lambda_j)f + \lambda_i\lambda_j \operatorname{id} = (f - \lambda_j \operatorname{id}) \circ (f - \lambda_i \operatorname{id})$$

gilt. Wenn wir die Projektion p_i auf W_i konstruieren wollen, dann muss diese natürlich jedes W_j für $j \neq i$ auf Null abbilden. Eine Abbildung, die das erfüllt können wir aber sofort konstruieren, indem wir einfach

$$(f - \lambda_1 \operatorname{id}) \circ \dots \circ (f - \lambda_{i-1} \operatorname{id}) \circ (f - \lambda_{i+1} \operatorname{id}) \circ \dots \circ (f - \lambda_k \operatorname{id})$$

bilden. Als Komposition von linearen Abbildungen ist diese Abbildung natürlich selbst linear. Wenn wir Ihren Wert auf $w_j \in W_j$ bestimmen wollen, dann können wir nach den obigen Überlegungen die Reihenfolge der Komposition so vertauschen, dass wir als erstes $f - \lambda_j \operatorname{id}$ anwenden, was nach Definition w_j auf Null abbildet. Andererseits können wir auch leicht den Wert auf $w_i \in W_i$ bestimmen. Da $f(w_i) = \lambda_i w_i$ gilt ist $(f - \lambda_k \operatorname{id})(w_i) = (\lambda_i - \lambda_k)w_i$, wenden wir darauf $(f - \lambda_{k-1} \operatorname{id})$ an, dann wird dieser Vektor noch mit $(\lambda_i - \lambda_{k-1})$ multipliziert, und so weiter. Insgesamt sehen wir, dass w_i durch unsere Funktion einfach mit dem Faktor $\prod_{j\neq i}(\lambda_i - \lambda_j)$ multipliziert wird, und da die $\lambda_j \neq \lambda_i$ für $j \neq i$ gilt, ist dieser Faktor ungleich Null. Damit folgt aber sofort, dass die lineare Abbildung

$$\frac{1}{\prod_{j\neq i}(\lambda_i - \lambda_j)}(f - \lambda_1 \operatorname{id}) \circ \dots \circ (f - \lambda_{j-1} \operatorname{id}) \circ (f - \lambda_{j+1} \operatorname{id}) \circ \dots \circ (f - \lambda_n \operatorname{id})$$

eine Summe $w_1 + \dots + w_k$ auf w_i abbildet und damit mit der Projektion p_i übereinstimmt. Löst man diese Komposition auf, dann erhält man natürlich eine Linearkombination von Termen der Form $f \circ \dots \circ f$, also kann man die Projektionen aus diesen Termen aufbauen.

Polynome von linearen Abbildungen und Matrizen

Man kann Ausdrücke der Form wie sie im letzten Beispiel vorgekommen sind, als Polynome in der gegebenen linearen Abbildung f interpretieren. Damit können wir allgemein versuchen, Projektionen für invariante direkte Summenzerlegungen als Polynome in f zu konstruieren. Es zeigt sich, dass das mit Hilfe einiger algebraischer Resultate über Polynome sehr gut funktioniert. Genauer gesagt, werden wir eine Zerlegung von V in eine f–invariante direkte Summe finden, die einer Zerlegung von p_f in einfache Teile entspricht. Diese Zerlegung ist analog zur Primfaktorzerlegung einer ganzen Zahl. Im nächsten Schritt kann man dann, zumindest in einigen Fällen bestimmen, wie f auf den einzelnen Teilen aussieht. Dieser letzte Schritt ist elementar (d.h. er benötigt keine tiefere Theorie) aber nicht einfach.

8.6. Sei $f : V \to V$ eine lineare Abbildung auf einem endlichdimensionalen $\mathbb{K}$–Vektorraum. Um V in f–invariante Teilräume zu zerlegen, benötigen wir nach Satz 8.5 lineare Abbildungen, die mit f kommutieren. Nun gibt es aber zwei offensichtliche lineare Abbildungen, die diese Eigenschaft haben, nämlich f selbst und id_V. Sind andererseits $g, h : V \to V$ linear mit $g \circ f = f \circ g$ und $h \circ f = f \circ h$ und ist $r \in \mathbb{K}$, dann ist auch $(g + rh) \circ f = f \circ (g + rh)$ und $(h \circ g) \circ f = f \circ (h \circ g)$. Insbesondere können wir $f^2 := f \circ f$, f^3 und allgemein f^k für $k \in \mathbb{N}$ bilden, wobei wir $f^0 = \mathrm{id}_V$ setzen. Dann sehen wir, dass für $a_1, \dots, a_N \in \mathbb{K}$ der Ausdruck $\sum_{i=1}^N a_i f^i$ eine lineare Abbildung definiert, die mit f kommutiert. Das sieht aber gerade so aus, als würden wir f in ein Polynom einsetzten, und man kann es auch tatsächlich so interpretieren.

Definition 8.6. Sei V ein endlichdimensionaler $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung.

(1) Für ein Polynom $p = \sum_{i=0}^N a_i t^i \in \mathbb{K}[t]$ definieren wir $p(f) := \sum_{i=0}^N a_i f^i$. Lassen wir alle Terme mit $a_i = 0$ weg, dann ist das eine Linearkombination von linearen Abbildungen, also ist $p(f) : V \to V$ eine lineare Abbildung.

(2) Für eine $n \times n$–Matrix $A \in M_n(\mathbb{K})$ setzen wir $A^0 := \mathbb{I}_n$ und A^k als die k–te Potenz von A bezüglich der Matrizenmultiplikation. Dann können wir für ein Polynom $p = \sum_{i=0}^N a_i t^i \in \mathbb{K}[t]$ analog das Element $p(A) := \sum_{i=0}^N a_i A^i \in M_n(\mathbb{K})$ bilden.

Die wesentlichen Eigenschaften dieser Operationen sind nun leicht abzuklären:

Satz 8.6. *Sei V ein endlichdimensionaler $\mathbb{K}$–Vektorraum und $f : V \to V$ eine lineare Abbildung. Dann gilt:*

(1) Für $p, q \in \mathbb{K}[t]$ und $\lambda \in \mathbb{K}$ gilt $(p + \lambda q)(f) = p(f) + \lambda q(f)$ und $(pq)(f) = p(f) \circ q(f)$.

(2) Die Menge $I_f := \{p \in \mathbb{K}[t] : p(f) = 0\}$ ein <u>Ideal</u> in $\mathbb{K}[t]$, d.h $I_f \subset \mathbb{K}[t]$ ist ein Teilraum und für $p \in I_f$ und $q \in \mathbb{K}[t]$ ist $pq \in I_f$.

(3) Die Menge $\mathbb{K}[f] := \{p(f) : p \in \mathbb{K}[t]\} \subset L(V, V)$ ist ein Teilraum und abgeschlossen unter der Komposition.

(4) Analoge Resultate gelten, wenn man f durch eine Matrix $A \in M_n(\mathbb{K})$ ersetzt.

Beweis. Die meisten dieser Eigenschaften sind völlig offensichtlich, man muss sie sich nur einmal bewusst machen.

(1) Bezeichnen wir das Maximum der Grade von p und q mit N, dann können wir $p = \sum_{i=0}^N a_i t^i$ und $q = \sum_{i=0}^N b_i t^i$ schreiben, und erhalten $p(f) = \sum_{i=0}^N a_i f^i$ und $q(f) = \sum_{i=0}^N b_i f^i$. Damit ist aber offensichtlich $p(f) + \lambda q(f) = \sum_{i=0}^N (a_i + \lambda b_i) f^i = (p + \lambda q)(f)$.

Nach Definition ist $t^i t^j = t^{i+j}$ in $\mathbb{K}[t]$ und $f^i \circ f^j = f^{i+j}$ in $L(V,V)$. Da beide Multiplikationen distributiv bezüglich der Addition sind, impliziert das sofort $(pq)(f) = p(f) \circ q(f)$.

(2) Für $p, q \in I_f$ und $\lambda \in \mathbb{K}$ gilt nach Teil (1) $(p + \lambda q)(f) = p(f) + \lambda q(f) = 0$. Damit ist $p + \lambda q \in I_f$, also $I_f \subset \mathbb{K}[t]$ ein Teilraum. Ist andererseits $p \in I_f$ und $q \in \mathbb{K}[t]$ beliebig, dann gilt wieder nach Teil (1) $(pq)(f) = p(f) \circ q(f) = 0 \circ q(f) = 0$. Damit ist $pq \in I_f$ und die zweite Behauptung folgt.

(3) Sind $g, h \in K[f] \subset L(V,V)$, dann finden wir nach Definition Polynome $p, q \in \mathbb{K}[t]$, sodass $g = p(f)$ und $h = q(f)$ gilt. Für $\lambda \in \mathbb{K}$ gilt dann nach Teil (1) $g + \lambda h = p(f) + \lambda q(f) = (p + \lambda q)(f)$, sowie $g \circ h = p(f) \circ q(f) = (pq)(f)$.

Die entsprechenden Beweise für eine Matrix A sind völlig analog. □

Bemerkung 8.6. (1) Der Zusammenhang zwischen linearen Abbildungen und Matrizen ist mit dem Anwenden von Polynomen verträglich. Ist nämlich $f : V \to V$ linear, $\mathcal{B}$ eine Basis von V und $A = [f]_{\mathcal{B}}$, dann ist nach Satz 4.16 von [**1**] $A^2 = [f]_{\mathcal{B}}[f]_{\mathcal{B}} = [f^2]_{\mathcal{B}}$ und induktiv erhält man $[f^k]_{\mathcal{B}} = A^k$. Da die Abbildung $f \mapsto [f]_{\mathcal{B}}$ nach Satz 4.15 von [**1**] linear ist, folgt sofort, dass $[p(f)]_{\mathcal{B}} = p(A)$ für alle $p \in \mathbb{K}[t]$ gilt.

(2) Die Elemente von $\mathbb{K}[f]$ sind in mehrfacher Hinsicht nahe mit f verwandt. Sei etwa v ein Eigenvektor von f zum Eigenwert λ. Dann gilt natürlich $f^2(v) = f(f(v)) = f(\lambda v) = \lambda^2 v$ und induktiv folgt $f^k(v) = \lambda^k v$ für alle $k \in \mathbb{N}$. Ist $p = \sum_{i=0}^N a_i t^i \in \mathbb{K}[t]$ ein Polynom, dann ist $p(f)(v) = \sum_{i=0}^n a_i f^i(v) = \sum_{i=0}^n a_i \lambda^i v = p(\lambda)v$. Somit ist v ein Eigenvektor von $p(f)$ zum Eigenwert $p(\lambda)$.

(3) Schließlich ist das Anwenden von Polynomen auf Matrizen gut verträglich mit Ähnlichkeit. Sind nämlich $A, B \in M_n(\mathbb{K})$ ähnlich, dann gibt es eine invertierbare Matrix $T \in M_n(\mathbb{K})$ mit $B = TAT^{-1}$. Dann ist aber $B^2 = TAT^{-1}TAT^{-1} = TA^2T^{-1}$, und induktiv erhält man $B^k = TA^kT^{-1}$. Aus der Distributivität der Matrizenmultiplikation folgt damit aber sofort, dass $p(B) = Tp(A)T^{-1}$ für jedes $p \in \mathbb{K}[t]$ gilt.

(4) Ist A eine Diagonalmatrix mit Eintragungen a_{ii} auf der Hauptdiagonale, dann ist A^k diagonal mit Eintragungen $(a_{ii})^k$ auf der Hauptdiagonale, also $p(A)$ diagonal mit Eintragungen $p(a_{ii})$ auf der Hauptdiagonale. Zusammen mit dem letzten Punkt liefert das auch Informationen über $p(A)$ für eine diagonalisierbare Matrix A.

8.7. Der Satz von Cayley–Hamilton. Für jede Matrix A muss es Polynome $p \in \mathbb{K}[t]$ geben, sodass $p(A) = 0$ gilt. Der Raum $M_n(\mathbb{K})$ hat ja Dimension n^2, also sind die n^2+1 Elemente $\mathbb{I}, A, A^2, \dots, A^{n^2}$ linear abhängig. Daher muss es Skalare $a_0, \dots, a_{n^2} \in \mathbb{K}$ geben, sodass $\sum_{i=0}^{n^2} a_i A^i = 0$ gilt. Das bedeutet aber gerade, dass das Polynom $p = \sum_{i=0}^{n^2} a_i t^i$ die Gleichung $p(A) = 0$ erfüllt. Die große Nützlichkeit der Polynome in der Theorie der linearen Abbildungen basiert aber zu einem guten Teil darauf, dass es einen tieferen Zusammenhang zwischen dem Ideal $I_A = \{p \in \mathbb{K}[t] : p(A) = 0\}$ und den algebraischen Eigenschaften der Matrix A gibt. Der Schlüssel dazu ist der Satz von Cayley–Hamilton, der besagt, dass das charakteristische Polynom p_A von A in I_A liegt.

Satz 8.7 (Cayley–Hamilton). *Ist $\mathbb{K}$ ein Körper und $A \in M_n(\mathbb{K})$ eine $n \times n$–Matrix mit charakteristischem Polynom $p_A \in \mathbb{K}[t]$, dann ist $p_A(A) = 0$. Analog gilt für jede lineare Abbildung $f : V \to V$ mit charakteristischem Polynom p_f die Gleichung $p_f(f) = 0$.*

Beweis. Da für $A = [f]_{\mathcal{B}}$ auch $p_A = p_f$ gilt, und nach Bemerkung (1) von 8.6 dann $p_A(A) = p_f(A) = [p_f(f)]_{\mathcal{B}}$ gilt, genügt es, den Fall von Matrizen zu betrachten.

Weiters können wir $A \in M_n(\mathbb{K})$ auch als Matrix über dem algebraischen Abschluss $\tilde{\mathbb{K}}$ von $\mathbb{K}$ betrachten, und damit ohne Beschränkung der Allgemeinheit annehmen, dass das charakteristische Polynom von A in ein Produkt von Polynomen ersten Grades zerfällt. Damit ist aber A nach Satz 8.3 ähnlich zu einer oberen Dreiecksmatrix B, die nach Satz 7.4 das selbe charakteristische Polynom hat wie A. Nach Bemerkung (3) von 8.6 folgt aus $A = TBT^{-1}$ aber $p_A(A) = Tp_B(B)T^{-1}$, also dürfen wir ohne Beschränkung der Allgemeinheit annehmen, dass $A = (a_{ij})$ selbst eine obere Dreiecksmatrix ist.

Unter dieser Annahme ist aber $p_A = (a_{11} - t) \cdots (a_{nn} - t)$ nach Korollar 6.6. Damit müssen wir zeigen, dass $(a_{11}\mathbb{I} - A) \cdots (a_{nn}\mathbb{I} - A) = 0$ gilt. Dazu zeigen wir mit Induktion, dass $(a_{11}\mathbb{I} - A) \cdots (a_{ii}\mathbb{I} - A)e_j = 0$ für $j = 1, \dots, i$ gilt, wobei $\{e_1, \dots, e_n\}$ die Standardbasis von $\mathbb{K}^n$ bezeichnet. Für $i = 1$ bemerken wir, dass $Ae_1 = a_{11}e_1$ und damit $(a_{11}\mathbb{I} - A)e_1 = 0$ gilt. Nehmen wir induktiv an, dass wir gezeigt haben, dass $(a_{11}\mathbb{I} - A) \cdots (a_{i-1,i-1}\mathbb{I} - A)e_j = 0$ für $j = 1, \dots, i-1$ gilt. Dann ist aber $Ae_i = a_{1i}e_1 + \cdots + a_{ii}e_i$ und damit $(a_{ii}\mathbb{I} - A)e_i$ eine Linearkombination von $e_1, \dots, e_{i-1}$, also ist $(a_{11}\mathbb{I} - A) \cdots (a_{ii}\mathbb{I} - A)e_i$ nach Induktionsvoraussetzung gleich Null. Andererseits ist

$$(a_{11}\mathbb{I} - A) \cdots (a_{i-1,i-1}\mathbb{I} - A)(a_{ii}\mathbb{I} - A) = (a_{ii}\mathbb{I} - A)(a_{11}\mathbb{I} - A) \cdots (a_{i-1,i-1}\mathbb{I} - A),$$

also werden auch die e_j für $j < i$ auf Null abgebildet. Nach Induktion ist somit

$$(a_{11}\mathbb{I} - A) \cdots (a_{nn}\mathbb{I} - A)e_j = 0$$

für alle $j = 1, \dots, n$ und somit ist das Produkt die Nullmatrix. □

Dieser Beweis ist für allgemeine Körper eher heikel, weil er die Existenz des algebraischen Abschlusses voraussetzt, die ein ziemlich schwieriges Resultat darstellt. Es gibt auch andere Beweise, die den algebraischen Abschluss nicht benötigen, dafür aber intensiv Determinanten über kommutativen Ringen mit Eins verwenden. Aus Satz 8.6 folgt nämlich leicht, dass die Teilmenge $K[A] = \{p(A) : p \in \mathbb{K}[t]\} \subset M_n(\mathbb{K})$ einen kommutativen Ring mit Einselement unter der Matrizenmultiplikation bildet. Dann kann man $p_A(A)$ in raffinierter Weise als Determinante einer Matrix mit Eintragungen aus diesem kommutativen Ring interpretieren, und dann nachrechnen, dass diese Determinante verschwinden muss.

Primfaktorzerlegung von Polynomen

Um weitere Informationen über lineare Abbildungen zu erhalten, müssen wir noch ein wenig allgemeine Theorie über Polynome entwickeln. Diese Teile der Theorie sind ganz parallel zu grundlegenden Resultaten über ganze Zahlen. Dieser Zusammenhang ist auch die Grundlage für viele Begriffsbildungen der Algebra (die "Ideale" die wir schon aus Satz 8.6 kennen, waren ursprünglich "ideale Zahlen").

8.8. Der Hauptidealsatz. In Satz 8.6 haben wir die Teilmenge $I_f = \{p \in \mathbb{K}[t] : p(f) = 0\} \subset \mathbb{K}[t]$ betrachtet und gezeigt, dass sie ein Ideal in $\mathbb{K}[t]$ ist. Der Begriff eines Ideals macht allgemein über kommutativen Ring Sinn, und ist eine Verstärkung des offensichtlichen Begriffs eines Teilringes, weil man etwas mehr verlangt als nur die Abgeschlossenheit unter beiden Ringoperationen.

Es gibt eine sehr einfache Möglichkeit, Ideale in $\mathbb{K}[t]$ (und allgemein in beliebigen Ringen) zu konstruieren. Ist nämlich $p \in \mathbb{K}[t]$ ein beliebiges fixes Element, dann betrachten wir die Menge $pK[t] := \{pq : q \in \mathbb{K}[t]\} \subset \mathbb{K}[t]$. Für $q_1, q_2 \in \mathbb{K}[t]$ und $\lambda \in \mathbb{K}$ ist $pq_1 + \lambda pq_2 = p(q_1 + \lambda q_2)$, also ist $pK[t]$ ein Teilraum in $\mathbb{K}[t]$. Andererseits ist natürlich $(pq_1)q_2 = p(q_1q_2)$, also ist $pK[t]$ ein Ideal in $\mathbb{K}[t]$. Mann nennt dieses Ideal das von p erzeugte *Hauptideal* in $\mathbb{K}[t]$.

Als erstes zeigen wir, dass diese einfache Konstruktion im Fall von $\mathbb{K}[t]$ schon *alle* Ideale liefert. Das ist eine einfache Konsequenz des Euklidischen Algorithmus. Erinnern wir uns noch daran, dass wir in 7.5 ein Polynom monisch genannt haben, wenn sein führender Koeffizient (also der Koeffizient der höchsten Potenz, der ungleich Null ist) gleich Eins ist.

SATZ 8.8. *Sei $\mathbb{K}$ ein Körper und $I \subset \mathbb{K}[t]$ ein beliebiges Ideal. Dann gibt es ein eindeutig bestimmtes monisches Polynom $p \in \mathbb{K}[t]$, sodass $I = p\mathbb{K}[t]$ gilt.*

BEWEIS. Falls I ein konstantes Polynom ungleich Null enthält, etwa $\lambda \in I$ für $0 \neq \lambda \in \mathbb{K}$, dann ist für beliebige $q \in \mathbb{K}[t]$ auch $q = \lambda(\lambda^{-1}q) \in I$. Damit ist $I = \mathbb{K}[t] = 1\mathbb{K}[t]$. Ansonsten sei $0 \neq \tilde{p} \in I$ ein Polynom minimalen Grades. Ist a der führende Koeffizient von $\tilde{p}$, dann liegt auch $p = a^{-1}\tilde{p}$ in I, und nach Konstruktion ist p monisch. Da $p \in I$ gilt und I ein Ideal ist, ist offensichtlich $p\mathbb{K}[t] \subset I$. Ist andererseits $q \in I$, dann dividieren wir q mit Rest durch p: Nach Lemma 7.5 finden wir Polynome $\tilde{q}, r \in \mathbb{K}[t]$ mit $r = 0$ oder $\deg(r) < \deg(p)$, sodass $q = p\tilde{q} + r$ gilt. Da $q \in I$ und wegen $p \in I$ auch $p\tilde{q} \in I$ gilt, ist auch $q - p\tilde{q} = r$ in I. Wäre $r \neq 0$, dann wäre $\deg(r) < \deg(p)$, ein Widerspruch zur Definition von p. Damit haben wir $I = p\mathbb{K}[t]$ bewiesen.

Um die Eindeutigkeit zu zeigen, nehmen wir an, dass $p_1, p_2 \in \mathbb{K}[t]$ monische Polynome sind, für die $p_1\mathbb{K}[t] = p_2\mathbb{K}[t]$ gilt. Dann gibt es Polynome $q_1, q_2 \in \mathbb{K}[t]$, sodass $p_2 = p_1q_1$ und $p_1 = p_2q_2$ gilt. Insbesondere folgt daraus $\deg(p_2) \geq \deg(p_1)$ und $\deg(p_1) \geq \deg(p_2)$, also haben p_1 und p_2 gleichen Grad, und q_1, q_2 liegen in $\mathbb{K} \subset \mathbb{K}[t]$. Da aber beide Polynome monisch sind, folgt $q_1 = q_2 = 1$, also $p_1 = p_2$. □

Damit können wir nun elegant einige Grundkonzepte der elementaren Zahlentheorie auf Polynome übertragen, nämlich die Konzepte des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen. Um die Uneindeutigkeit zu vermeiden, die sich durch die Möglichkeit ergibt, Polynome mit Skalaren $\neq 0$ zu multiplizieren, schränkt man sich immer auf monische Polynome ein.

Der Schlüssel zu diesen Ideen ist eigentlich ganz einfach: Ideale in $\mathbb{K}[t]$ sind insbesondere Teilräume, also kann man versuchen, die aus dem letzten Semester bekannten Konstruktionen mit Teilräumen anzuwenden. Wir können also für Ideale $I_1, I_2 \subset \mathbb{K}[t]$ die Teilräume $I_1 \cap I_2$ und $I_1 + I_2$ von $\mathbb{K}[t]$ betrachten, siehe 2.4 und 4.8 von [**1**]. Nun sieht man aber sofort, dass diese beiden Teilräume selbst wieder Ideale sind. Ist nämlich $p \in I_1 \cap I_2$ und $q \in \mathbb{K}[t]$, dann liegt pq in I_1, weil $p \in I_1$ liegt und I_1 ein Ideal ist. Analog folgt $pq \in I_2$, also ist $pq \in I_1 \cap I_2$, und somit $I_1 \cap I_2$ wieder ein Ideal. Andererseits besteht $I_1 + I_2$ genau aus allen Polynomen, die in der Form $p_1 + p_2$ für $p_1 \in I_1$ und $p_2 \in I_2$ geschrieben werden können. Ist $q \in \mathbb{K}[t]$ wieder ein beliebiges Polynom, dann ist $(p_1 + p_2)q = p_1q + p_2q$ und der erste Summand liegt in I_1, weil I_1 ein Ideal ist, während der zweite Summand in I_2 liegt. Damit ist $(p_1 + p_2)q \in I_1 + I_2$, also ist auch die Summe der beiden Ideale ein Ideal.

Sind nun $p_1, p_2 \in \mathbb{K}[t]$ Polynome ungleich Null, dann können wir die entsprechenden Hauptideale $p_1\mathbb{K}[t]$ und $p_2\mathbb{K}[t]$ bilden. Da die Summe dieser beiden Teilräume wieder ein Ideal ist, gibt es nach Satz 8.8 ein eindeutig bestimmtes monisches Polynom $p \in \mathbb{K}[t]$, sodass $p_1\mathbb{K}[t]+p_2\mathbb{K}[t] = p\mathbb{K}[t]$ gilt. Nach Konstruktion liegen p_1 und p_2 in dieser Summe, also gibt es Polynome $q_1, q_2 \in \mathbb{K}[t]$, sodass $p_1 = pq_1$ und $p_2 = pq_2$ gilt. Damit ist p ein Teiler von p_1 und von p_2. Andererseits kann man nach Definition p in der Form $p = p_1r_1 + p_2r_2$ für Polynome $r_1, r_2 \in \mathbb{K}[t]$ schreiben. Ist nun $s \in \mathbb{K}[t]$ ein Polynom, dass sowohl p_1 als auch p_2 teilt, dann gibt es Polynome $\tilde{s}_1$ und $\tilde{s}_2$ sodass $p_1 = s\tilde{s}_1$ und $p_2 = s\tilde{s}_2$ gilt. Setzt man das oben ein, dann erhält man

$$p = p_1r_1 + p_2r_2 = s\tilde{s}_1r_1 + s\tilde{s}_2r_2 = s(\tilde{s}_1r_1 + \tilde{s}_2r_2).$$

Das bedeutet aber gerade, dass das Polynom s auch das Polynom p teilen muss, was die folgende Definition rechtfertigt:

DEFINITION 8.8. (1) Sind $p_1, p_2 \in \mathbb{K}[t]$ Polynome ungleich Null, dann ist der *größte gemeinsame Teiler* von p_1 und p_2 das eindeutig bestimmte monische Polynom p, dass $p\mathbb{K}[t] = p_1\mathbb{K}[t] + p_2\mathbb{K}[t]$ erfüllt. Man schreibt $p = \mathrm{ggT}(p_1, p_2)$.

(2) Zwei Polynome $p_1, p_2 \in \mathbb{K}[t]$ heißen *teilerfremd* oder *relativ prim*, wenn ihr größter gemeinsamer Teiler das konstante Polynom 1 ist, also $\mathrm{ggT}(p_1, p_2) = 1$ gilt.

Insbesondere erhalten wir sofort:

KOROLLAR 8.8. *Sind $p_1, p_2 \in \mathbb{K}[t]$ relativ prim, dann gibt es Polynome $q_1, q_2 \in \mathbb{K}[t]$, sodass $p_1q_1 + p_2q_2 = 1$ gilt.*

BEMERKUNG 8.8. Ganz analog gibt es zu $p_1, p_2 \in \mathbb{K}[t]$ ein eindeutig bestimmtes monische Polynom p, sodass $p\mathbb{K}[t] = (p_1\mathbb{K}[t]) \cap (p_2\mathbb{K}[t])$ gilt. Das bedeutet nach Definition, dass p sowohl in der Form $p = p_1q_1$ als auch in der Form $p = p_2q_2$ geschrieben werden kann, also ein gemeinsames Vielfaches von p_1 und p_2 ist.

Analog wie oben überlegt man (siehe Übungen), dass jedes gemeinsame Vielfache von p_1 und p_2 ein Vielfaches dieses Polynoms p sein muss, also ist p das *kleinste gemeinsame Vielfache* von p_1 und p_2.

8.9. Irreduzible Polynome und die eindeutige Primfaktorzerlegung. Als nächsten Schritt entwickeln wir die Analoga von Primzahlen und der eindeutigen Primfaktorzerlegung für Polynome. Das geht ganz analog wie für ganze Zahlen, man muss nur berücksichtigen, dass alle Elemente von $\mathbb{K} \setminus \{0\}$ (betrachtet als konstante Polynome) invertierbar sind. (Im Gegensatz zu $\mathbb{Z}$, wo nur 1 und -1 invertierbar sind.)

DEFINITION 8.9. Sei $\mathbb{K}$ ein Körper. Ein Polynom $p \in \mathbb{K}[t]$ mit $\deg(p) > 0$ heißt irreduzibel, wenn es nicht als Produkt von zwei Polynomen echt kleineren Grades geschrieben werden kann, d.h. wenn $p = q_1q_2$ nur für $\deg(q_1) = 0$ oder $\deg(q_2) = 0$ möglich ist.

BEISPIEL 8.9. (1) Polynome ersten Grades sind immer automatisch irreduzibel, weil wegen $\deg(q_1q_2) = \deg(q_1) + \deg(q_2)$ ein Produkt nur dann Grad eins haben kann, wenn einer der beiden Faktoren Grad Null hat.

(2) Ist der Körper $\mathbb{K}$ algebraisch abgeschlossen (siehe 7.8), dann zerfällt nach Definition jedes Polynom in ein Produkt von Polynomen ersten Grades. Damit sind aber in diesem Fall die irreduziblen Polynome genau die Polynome vom Grad 1. Insbesondere ist das für $\mathbb{K} = \mathbb{C}$ der Fall.

(3) Das Polynom $p = t^2 + 1 \in \mathbb{R}[t]$ ist irreduzibel. Wäre das nämlich nicht der Fall, dann wäre $p = q_1q_2$ mit $\deg(q_1) = \deg(q_2) = 1$. Weil das Produkt der führenden Koeffizienten von p_1 und p_2 Eins sein muss, dürften wir ohne Beschränkung der Allgemeinheit annehmen, dass $p_i = t - \alpha_i$ für $\alpha_1, \alpha_2 \in \mathbb{R}$ ist. Das würde aber nach Satz 7.5 bedeuten, dass α_1 und α_2 Nullstellen des Polynoms p wären, die es in $\mathbb{R}$ aber nicht geben kann.

Tatsächlich kann man Korollar 7.8 so interpretieren, dass ein Polynom über $\mathbb{R}$ genau dann irreduzibel ist, wenn es entweder Grad eins hat, oder Grad zwei hat, aber keine reelle Nullstelle besitzt.

4) Für allgemeine Körper gibt es irreduzible Polynome höheren Grades. So ist etwa $t^3 - 2 \in \mathbb{Q}[t]$ irreduzibel. Könnte man dieses Polynom nämlich in ein Produkt zerlegen, dann müsste einer der Faktoren Grad eins haben, was analog wie in Beispiel (3) zur Existenz einer Nullstelle des Polynoms in $\mathbb{Q}$ führen würde. Über $\mathbb{R}$ zerfällt dieses Polynom natürlich, und zwar in der Form $t^3 - 2 = (t - 2^{1/3})(t^2 + 2^{1/3}t + 2^{2/3})$.

LEMMA 8.9. *Sei $\mathbb{K}$ ein Körper, $p \in \mathbb{K}[t]$ irreduzibel und $q_1, q_2 \in \mathbb{K}[t]$ beliebig. Dann gilt: Falls p das Produkt $q_1 q_2$ teilt, dann teilt p entweder q_1 oder es teilt q_2.*

BEWEIS. Nehmen wir an, dass p das Produkt $q_1 q_2$, aber nicht den Faktor q_1 teilt. Dann betrachten wir den größten gemeinsamen Teiler $s := \mathrm{ggT}(p, q_1)$. Wäre $\deg(s) = \deg(p)$, dann wäre $s = a^{-1}p$, wobei a der führende Koeffizient von p ist. Nach Konstruktion ist aber s ein Teiler von q_1 und damit wäre auch p ein Teiler von q_1, ein Widerspruch. Also ist $\deg(s) < \deg(p)$ und weil p irreduzibel ist, muss $\deg(s) = 0$, also $s = 1$ folgen.

Damit gibt es nach Korollar 8.8 Polynome $\tilde{p}$ und $\tilde{q}$, sodass $p\tilde{p} + q_1\tilde{q} = 1$ und damit $p\tilde{p}q_2 + \tilde{q}q_1q_2 = q_2$ gilt. Nun ist aber nach Voraussetzung p ein Teiler des Produktes q_1q_2, also gibt es ein Polynom r, sodass $q_1q_2 = pr$ gilt. Damit liefert aber die obige Gleichung $q_2 = p(\tilde{p}q_2 + \tilde{q}r)$, also teilt p den Faktor q_2. □

Induktiv folgt aus diesem Lemma sofort, dass ein irreduzibles Polynom, das ein Produkt von endlich vielen Polynomen teilt, mindestens eines dieser Polynome teilen muss.

Nun haben wir alle Zutaten gesammelt, um die eindeutige Primfaktorzerlegung für Polynome zu beweisen. Das Problem, dass man skalare Faktoren beliebig auf die einzelnen Primfaktoren verteilen kann, löst man dadurch, dass man sich auf monische Primfaktoren beschränkt.

SATZ 8.9. *Sei $\mathbb{K}$ ein Körper, $p \in \mathbb{K}[t]$ ein beliebiges Polynom mit* $\deg(p) > 0$. *Dann gibt es paarweise verschiedene, monische, irreduzible Polynome $p_1, \dots, p_k \in \mathbb{K}[t]$, Elemente $n_1, \dots, n_k \in \mathbb{N} \setminus \{0\}$ und ein Element $c \in \mathbb{K} \setminus \{0\}$, sodass $p = cp_1^{n_1} \cdots p_k^{n_k}$ gilt. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig bestimmt.*

BEWEIS. Zunächst beweisen wir die Existenz der Zerlegung durch Induktion nach $n = \deg(p)$. Ist $n = 1$, dann ist p nach Beispiel (1) von oben irreduzibel. Ist c der führende Koeffizient von p, dann ist $p_1 := c^{-1}p$ irreduzibel und monisch, und $p = cp_1$ ist die gesuchte Zerlegung.

Nehmen wir also an, dass $n \geq 2$ gilt, und die Existenz der Zerlegung für alle Polynome vom Grad $k < n$ schon bewiesen wurde. Ist p irreduzibel, dann liefert wieder $p = c(c^{-1}p)$ die gesuchte Zerlegung, wobei c der führende Koeffizient von p ist. Ist p nicht irreduzibel, dann gibt es Polynome $q_1, q_2 \in \mathbb{K}[t]$ mit $\deg(q_1), \deg(q_2) < \deg(p)$, sodass $p = q_1q_2$ gilt. Nach Induktionsvoraussetzung können wir q_1 und q_2 in der gewünschten Form darstellen, und durch Multiplizieren und Zusammenfassen gemeinsamer Faktoren erhalten wir die gesuchte Darstellung für p.

Zur Eindeutigkeit: Da der Faktor c offensichtlich gerade der führende Koeffizient des Produktes $cp_1^{n_1} \dots p_k^{n_k}$ ist, ist dieser Faktor eindeutig bestimmt. Es genügt also zu zeigen, dass für (nicht notwendigerweise verschiedene) monische irreduzible Polynome $p_1, \dots, p_n, q_1, \dots, q_m$ die Gleichung $p_1 \cdots p_n = q_1 \cdots q_m$ nur dann gelten kann, wenn $n = m$ gilt und sich die Produkte nur durch die Reihenfolge der Faktoren unterscheiden. Wir dürfen ohne Beschränkung der Allgemeinheit $n \leq m$ annehmen und führen den Beweis nun durch Induktion nach n. Für $n = 1$ ist das Resultat offensichtlich, weil alle auftretenden Polynome monisch und irreduzibel, also vom Grad ≥ 1, sind.

Für $n > 1$ sehen wir, dass p_1 das Produkt $q_1 \cdots q_m$ teilt, also gibt es nach dem Lemma ein i, sodass p_1 den Faktor q_i teilt, und weil q_i irreduzibel ist und $\deg(p_1) > 0$ gilt, muss $p_1 = q_i$ gelten. Damit erhalten wir aber

$$p_1(p_2 \cdots p_n - q_1 \cdots q_{i-1}q_{i+1} \cdots q_m) = 0.$$

Das kann aber nur sein, wenn die Klammer verschwindet, also erhalten wir $p_2 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m$ und die Behauptung folgt nach Induktion. $\square$

Die Primärzerlegung

8.10. Das Minimalpolynom. Unsere Motivation zur Betrachtung von Idealen in $\mathbb{K}[t]$ war ja gerade, dass für eine lineare Abbildung $f : V \to V$ auf einem endlichdimensionalen $\mathbb{K}$–Vektorraum V die Teilmenge $I_f := \{p \in \mathbb{K}[t] : p(f) = 0\}$ ein Ideal in $\mathbb{K}[t]$ ist. Nach dem Hauptidealsatz (Satz 8.8) gibt es ein eindeutiges monisches Polynom $m_f \in \mathbb{K}[t]$, sodass $I_f = m_f \mathbb{K}[t]$ gilt. Das bedeutet, dass ein Polynom $p \in \mathbb{K}[t]$ genau dann $p(f) = 0$ erfüllt, wenn es in der Form $p = m_f q$ für ein Polynome $q \in \mathbb{K}[t]$ geschrieben werden kann. Nach dem Beweis von Satz 8.8 ist das Polynom m_f ist das monische Polynom minimalen Grades, das $m_f(f) = 0$ erfüllt. Deshalb heißt m_f das *Minimalpolynom* der linearen Abbildung f. Nach dem Satz von Cayley–Hamilton (Satz 8.7) liegt insbesondere das charakteristische Polynom p_f in I_f, also ist $p_f = m_f q$ für ein Polynom $q \in \mathbb{K}[t]$.

Man kann den Zusammenhang zwischen p_f und m_f in Termen der Primfaktorzerlegung der beiden Polynome genauer beschreiben. Nehmen wir an, dass die Primfaktorzerlegung des Minimalpolynoms durch $m_f = p_1^{m_1} \cdots p_k^{m_k}$ gegeben ist. Dann teilt natürlich jedes p_i das Polynom p_f und man überlegt leicht, dass jedes p_i in der Primfaktorzerlegung von p_f mit einer Potenz $n_i \geq m_i$ auftauchen muss. Umgekehrt kann man zeigen, dass jeder Primfaktor von p_f auch in m_f vorkommen muss, also hat die Primfaktorzerlegung von p_f die Form $p_f = p_1^{n_1} \cdots p_k^{n_k}$, wobei $n_i \geq m_i$ für alle $i = 1, \dots, k$ liegt. Die letzte Tatsache ist etwa im Fall $\mathbb{K} = \mathbb{C}$ leicht zu sehen: Wie wir in Beispiel (2) von 8.9 gesehen haben, hat in diesem Fall jedes irreduzible Polynome Grad 1, also hat die Primfaktorzerlegung von p_f die Form $(t - \lambda_1)^{n_1} \dots (t - \lambda_\ell)^{n_\ell}$, wobei $\lambda_1, \dots, \lambda_\ell$ genau die verschiedenen Eigenwerte von f sind. Nehmen wir an, dass der Primfaktor $(t - \lambda_1)$ nicht in m_f vorkommt, also die Primfaktorzerlegung von m_f die Form $m_f = (t - \lambda_2)^{m_2} \dots (t - \lambda_\ell)^{m_\ell}$ hat. Ist $v \in V$ ein Eigenvektor zum Eigenwert λ_1, dann ist natürlich $(f - \lambda_i \,\mathrm{id})(v) = (\lambda_1 - \lambda_i)v$, also $(f - \lambda_i \,\mathrm{id})^{m_i}(v) = (\lambda_1 - \lambda_i)^{m_i} v$. Damit wäre aber

$$m_f(f)(v) = (\lambda_1 - \lambda_2)^{m_2} \dots (\lambda_1 - \lambda_\ell)^{m_\ell} v \neq 0,$$

ein Widerspruch zu $m_f(f) = 0$.

8.11. Wir können nun die Primfaktorzerlegung des Minimalpolynoms benutzen, um für eine gegebene lineare Abbildung $f : V \to V$ den Raum V ein eine direkte Summe von f–invarianten Teilräumen zu zerlegen. Der Schlüssel dazu ist folgendes Resultat:

Lemma 8.11. *Sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$ und $f : V \to V$ eine lineare Abbildung. Seien $p_1, p_2 \in \mathbb{K}[t]$ Polynome, die relativ prim sind und $(p_1 p_2)(f) = 0$ erfüllen. Setze $W_i := \mathrm{Ker}(p_i(f)) \subset V$ für $i = 1, 2$. Dann sind W_1 und W_2 f–invariante Teilräume von V und $V = W_1 \oplus W_2$.*

Beweis. Da p_1 und p_2 relativ prim sind, finden wir nach Korollar 8.8 Polynome $q_1, q_2 \in \mathbb{K}[t]$, sodass $q_1 p_1 + q_2 p_2 = 1$ gilt. Setzen wir nun $\pi_i = (q_i p_i)(f) \in L(V, V)$ für $i = 1, 2$, dann bedeutet diese Gleichung gerade $\pi_1 + \pi_2 = \mathrm{id}_V$. Außerdem ist

$$\pi_2 \circ \pi_1 = (q_2 p_2)(f) \circ (q_1 p_1)(f) = (q_2 p_2 q_1 p_1)(f) = (q_2 q_1)(f) \circ (p_1 p_2)(f) = 0.$$

Analog folgt $\pi_1 \circ \pi_2 = 0$, und da jedes π_i ein Polynom in f ist folgt $\pi_i \circ f = f \circ \pi_i$ für $i = 1, 2$. Damit ist $V = \mathrm{Im}(\pi_1) \oplus \mathrm{Im}(\pi_2)$ nach Proposition 8.4 und nach Satz 8.5(1) ist das eine Zerlegung in f–invariante Teilräume.

Wegen $p_2(f) \circ \pi_1 = (p_2 q_1 p_1)(f) = 0$ gilt $\mathrm{Im}(\pi_1) \subset W_2 = \mathrm{Ker}(p_2(f))$. Andererseits ist $W_2 = \mathrm{Ker}(p_2(f)) \subset \mathrm{Ker}(q_2(f) \circ p_2(f)) = \mathrm{Ker}(\pi_2)$. Für $v \in W_2$ ist damit aber $v = \pi_1(v) + \pi_2(v) = \pi_1(v)$, also $W_2 \subset \mathrm{Im}(\pi_1)$. Damit gilt aber $W_2 = \mathrm{Im}(\pi_1)$ und analog folgt $W_1 = \mathrm{Im}(\pi_2)$. □

Mit etwas mehr technischem Aufwand (aber ohne zusätzliche Ideen zu benötigen) kann man das analoge Resultat für mehr als zwei Faktoren beweisen. Das kann man dann insbesondere auf die eindeutige Primfaktorzerlegung eines Polynoms anwenden und erhält:

Satz 8.11 (Primärzerlegung). *Sei V ein endlichdimensionaler $\mathbb{K}$–Vektorraum, $f : V \to V$ eine lineare Abbildung und $p \in \mathbb{K}[t]$ ein Polynom, sodass $p(f) = 0$ gilt. Sei $p = cp_1^{n_1} \cdots p_k^{n_k}$ die eindeutige Primfaktorzerlegung von p, und setze $W_i := \mathrm{Ker}(p_i(f)^{n_i})$ für $i = 1, \dots, k$.*

Dann ist jedes W_i ein f–invarianter Teilraum von V und $V = W_1 \oplus \cdots \oplus W_k$.

Bemerkung 8.11. (1) Die offensichtlichen Kandidaten für Polynome, auf die man dieses Resultat anwenden könnte sind natürlich das Minimalpolynom m_f und das charakteristische Polynom p_f. Diese beiden Polynome liefern aber die gleiche Zerlegung (wobei das Minimalpolynom aber zu einer einfacheren Beschreibung der Summanden führt). Aus 8.8 wissen wir ja, dass die Primfaktorzerlegungen der beiden Polynome die Form

$$m_f = p_1^{m_1} \cdots p_k^{m_k} \qquad p_f = p_1^{n_1} \cdots p_k^{n_k}$$

für natürliche Zahlen m_i und n_i, die $1 \leq m_i \leq n_i$ für alle $i = 1, \dots, k$ erfüllen.

Damit hat aber die Primärzerlegung bezüglich m_f die Form $V = W_1 \oplus \cdots \oplus W_k$, wobei $W_i = \mathrm{Ker}(p_i(f)^{m_i})$. Für p_f erhält man eine Primärzerlegung der Form $V = \tilde{W}_1 \oplus \cdots \oplus \tilde{W}_k$, wobei $\tilde{W}_i = \mathrm{Ker}(p_i(f)^{n_i})$. Das bedeutet aber nach Konstruktion, dass $W_i \subset \tilde{W}_i$ für alle $i = 1, \dots, k$ gilt, also jedes W_i ein Teilraum von $\tilde{W}_i$ ist. Wäre eines der $W_i \neq \tilde{W}_i$, dann würde $\dim(\tilde{W}_i) > \dim(W_i)$ gelten. Da aber zusätzlich $\dim(\tilde{W}_j) \geq \dim(W_j)$ gilt, wäre

$$\dim(\tilde{W}_1) + \cdots + \dim(\tilde{W}_k) > \dim(W_1) + \cdots + \dim(W_k).$$

Das kann aber natürlich nicht sein, weil beide Seiten gleich $\dim(V)$ sein müssen. Somit gilt $\tilde{W}_i = W_i$ für alle $i = 1, \dots, n$, und die beiden Zerlegungen sind gleich. Analog zeigt man, dass jedes Polynom $p \in \mathbb{K}[t]$, das $p(f) = 0$ erfüllt, im wesentlichen auf die gleiche Zerlegung führt. Daher spricht man oft einfach von der Primärzerlegung von V bezüglich f.

(2) Betrachten wir den Fall von Primfaktoren vom Grad 1, die also die Form $p_i = (t - \lambda)$ für $\lambda \in \mathbb{K}$ haben. Tritt der entsprechende Primfaktor in m_f in der Form $(t - \lambda)^{m_i}$ auf, dann ist der entsprechende Summand in der Primärzerlegung $W_i := \mathrm{Ker}((f - \lambda)^{m_i})$. Ist $m_i = 1$, dann ist das genau der Eigenraum V_λ^f zum Eigenwert λ aus Definition 7.1.

Im Allgemeinen nennt man $\mathrm{Ker}((f - \lambda)^{m_i})$ den *verallgemeinerten Eigenraum* zum Eigenwert λ und bezeichnet ihn mit $V_{(\lambda)}^f$. Offensichtlich gilt $V_\lambda^f \subset V_{(\lambda)}^f$ aber im Allgemeinen sind die beiden Räume verschieden.

Wir können nun noch Diagonalisierbarkeit einer linearen Abbildung in Termen Ihres Minimalpolynoms charakterisieren:

Korollar 8.11. *Eine lineare Abbildung $f : V \to V$ auf einem endlichdimensionalen $\mathbb{K}$–Vektorraum V ist genau dann diagonalisierbar, wenn ihr Minimalpolynom m_f die Form $(t - \lambda_1) \cdots (t - \lambda_k)$ für paarweise verschiedene Skalare $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ hat.*

Beweis. Hat m_f die angegebene Form, dann sie $V = W_1 \oplus \cdots \oplus W_k$ die Primärzerlegung zu m_f. Nach Definition ist $W_i = \operatorname{Ker}(f - \lambda_i \operatorname{id}) = V^f_{\lambda_i}$ der Eigenraum zum Eigenwert λ_i. Wählt man nun für jedes i eine Basis für W_i, dann ist die Vereinigung dieser Basen eine Basis für V, die aus Eigenvektoren für f besteht, also ist f diagonalisierbar.

Ist umgekehrt f diagonalisierbar, dann seine $\lambda_1, \dots, \lambda_k$ die verschiedenen Eigenwerte von f. Nach Satz 7.12 zerfällt das charakteristische Polynom p_f in ein Produkt von Polynomen ersten Grades, und die Nullstellen von p_f sind genau die λ_i also hat p_f die Form $p_f = (t - \lambda_1)^{n_1} \cdots (t - \lambda_k)^{n_k}$. Betrachten wir nun

$$(f - \lambda_1 \operatorname{id}) \circ \ldots \circ (f - \lambda_k \operatorname{id}),$$

dann kann man die Reihenfolge der Komposition beliebig vertauschen. Damit folgt aber sofort, dass diese Komposition jeden Eigenvektor von f auf Null abbildet. Da f diagonalisierbar ist, gibt es eine Basis für V die aus solchen Eigenvektoren besteht, also ist diese Komposition die Nullabbildung. Damit liegt aber das Polynom $(t - \lambda_1) \cdots (t - \lambda_k)$ in I_f und muss daher nach unseren Überlegungen aus 8.10 das Minimalpolynom m_f sein. □

Die Jordan'sche Normalform

Wir können nun die Frage des Findens einer schönen Matrixdarstellung für eine gegebene lineare Abbildung $f : V \to V$ endgültig beantworten. Durch die Primärzerlegung haben wir V in eine direkte Summe von f–invarianten Teilräumen W_i zerlegt, und erhalten nach 8.5 ein Matrixdarstellung von f in Blockdiagonalform wobei die Blöcke Matrixdarstellungen von $f|_{W_i}$ sind. Damit müssen wir nur noch für diese Einschränkungen schöne Matrixdarstellungen finden.

Betrachten wir zunächst $\mathbb{K} = \mathbb{C}$ (oder allgemein den Fall von algebraisch abgeschlossenen Körpern). Dann wissen wir, dass jeder der Summanden W_i als $\operatorname{Ker}((f - \lambda_i)^{m_i})$ für einen Eigenwert λ_i von f und eine Zahl $m_i \in \mathbb{N}$ geschrieben werden kann. Setzen wir $g := f|_{W_i}$ dann sagt das gerade, dass $(g - \lambda_i \operatorname{id}_{W_i})^{m_i} = 0$ gilt. Lineare Abbildungen, für die eine gewisse Potenz verschwindet kann man aber (über beliebigen Körpern) gut verstehen, was unsere nächste Aufgabe ist.

8.12. Nilpotente lineare Abbildungen. Zunächst benötigen wir noch einige Definitionen.

Definition 8.12. (1) Sei V ein Vektorraum über einem Körper $\mathbb{K}$. Eine lineare Abbildung $f : V \to V$ heißt *nilpotent*, wenn es eine Zahl $k \in \mathbb{N}$ gibt, sodass $f^k = 0$ ist. Das bedeutet also, dass $(f \circ \ldots \circ f)(v) = 0$ für alle $v \in V$ gilt, wobei k Kopien von f komponiert werden.

(2) Ist $f : V \to V$ nilpotent, so heißt das kleinste k, sodass $f^k = 0$ gilt, der *Nilpotenzindex* von f. Der Nilpotenzindex von f ist also genau dann k, wenn $f^k(v) = 0$ für alle $v \in V$ gilt, es aber ein $v_0 \in V$ mit $f^{k-1}(v_0) \neq 0$ gibt.

(3) Für $\lambda \in \mathbb{K}$ und $m \in \mathbb{N}$, $m \geq 1$ definieren wir den *Jordan–Block* $J_m(\lambda) \in M_m(\mathbb{K})$ der Größe m mit Eigenwert λ als die $m \times m$–Matrix (a_{ij}) mit $a_{ii} = \lambda$ für alle $i = 1, \dots, m$, $a_{i,i+1} = 1$ für $i = 1, \dots, m-1$ und $a_{ij} = 0$ für alle anderen i und j. Die Matrix $J_m(\lambda)$ hat also auf der Hauptdiagonale lauter λ's, direkt über der Hauptdiagonale lauter Einsen und sonst lauter Nullen als Eintragungen.

Da $J_m(\lambda) - t\mathbb{I}$ eine obere Dreiecksmatrix ist, können wir sofort ablesen, dass das charakteristische Polynom von $J_m(\lambda)$ durch $(-1)^m (t - \lambda)^m$ gegeben ist, also ist λ der einzige Eigenwert von $J_m(\lambda)$. Betrachten wir andererseits $J_m(0) = J_m(\lambda) - \lambda\mathbb{I}$. In Termen der Standardbasis $\{e_1,\dots,e_m\}$ von $\mathbb{K}_m$ gilt einfach $J_m(0)e_i = e_{i-1}$ für $i = 2,\dots,m$ und $J_m(0)e_1 = 0$. Insbesondere ist $(J_m(0))^{m-1}e_m = e_1 \neq 0$ aber offensichtlich $(J_m(0))^m = 0$, also ist $J_m(0)$ nilpotent mit Nilpotenzindex m. Somit ist auch das Minimalpolynom von $J_m(\lambda)$ durch $(t-\lambda)^m$ gegeben. Die Jordan Blöcke sind somit die einfachsten Matrizen, deren Minimalpolynom eine gegebene Potenz eines Polynoms ersten Grades ist.

Betrachten wir nun wieder einen endlichdimensionalen Vektorraum V über einem Körper $\mathbb{K}$ und eine lineare Abbildung $f : V \to V$. Dann können wir für jedes $k \geq 0$ die Potenz $f^k : V \to V$ betrachten. Insbesondere haben wir für jedes k den Teilraum $\mathrm{Im}(f^k) \subset V$. Für $k = 0$ ist $\mathrm{Im}(f^0) = V$, weil $f^0 = \mathrm{id}$ gilt. Ist allgemein $v \in \mathrm{Im}(f^k)$, dann gibt es ein Element $w \in V$ mit $f^k(w) = v$. Damit ist aber $v = f^k(w) = f^{k-1}(f(w))$, also $v \in \mathrm{Im}(f^{k-1})$, und wir erhalten $\mathrm{Im}(f^k) \subset \mathrm{Im}(f^{k-1})$. Ist f nilpotent mit Nilpotenzindex ℓ, dann ist $\mathrm{Im}(f^\ell) = 0$ und somit $\mathrm{Im}(f^{\ell-1}) \subset \mathrm{Ker}(f)$.

Der wesentliche Schritt zum Verständnis nilpotenter Abbildungen ist nun:

Lemma 8.12. *Sei V ein Vektorraum über einem Körper $\mathbb{K}$, $f : V \to V$ eine lineare Abbildung und $k \in \mathbb{N}$. Angenommen, wir finden eine lineare unabhängige Teilmenge $\{\tilde{v}_1,\dots,\tilde{v}_m\} \subset \mathrm{Im}(f^k) \cap \mathrm{Ker}(f)$, dann gilt:*

Sind $v_1,\dots,v_m \in V$, so dass $f^k(v_i) = \tilde{v}_i$ für $i = 1,\dots,m$ gilt, dann ist die Teilmenge $\mathcal{B} := \{f^i(v_j) : 0 \leq i \leq k, 1 \leq j \leq m\} \subset V$ linear unabhängig und spannt einen f–invarianten Teilraum W von V auf.

Für eine geeignete Anordnung der Basis $\mathcal{B}$ ist die Matrixdarstellung der Einschränkung von f auf W bezüglich $\mathcal{B}$ gegeben durch eine Blockdiagonalmatrix mit m Jordan–Blöcken $J_{k+1}(0)$ entlang der Hauptdiagonale und ansonsten lauter Nullen.

Beweis. Seien $a_j^i \in \mathbb{K}$ so, dass $\sum_{i,j} a_j^i f^i(v_j) = 0$ gilt. Wenden wir auf diese Gleichung f^k an, dann gilt $f^k(f^i(v_j)) = f^{k+i}(v_j) = f^i(f^k(v_j)) = f^i(\tilde{v}_j)$, und das ist $\tilde{v}_j$ für $i = 0$ und 0 für $i > 0$, weil nach Voraussetzung $\tilde{v}_j \in \mathrm{Ker}(f)$ gilt. Damit erhalten wir aber $0 = \sum_{j=1}^m a_j^0 \tilde{v}_j$, was wegen der linearen Unabhängigkeit der $\tilde{v}_j$ schon $a_j^0 = 0$ für alle $j = 1,\dots,m$ impliziert.

Nehmen wir nun induktiv an, dass wir $a_j^i = 0$ für alle $i < \ell$ und alle $j = 1,\dots,m$ bereits gezeigt haben. Dann hat unsere Gleichung die Form $\sum_{i=\ell}^k \sum_{j=1}^m a_j^i f^i(v_j) = 0$. Wenden wir auf diese Gleichung $f^{k-\ell}$ an, dann verschwinden wieder alle Terme mit $i > \ell$, und wir erhalten $\sum_{j=1}^n a_j^\ell \tilde{v}_j = 0$. Wegen der linearen Unabhängigkeit der $\tilde{v}_j$ impliziert das wieder $a_j^\ell = 0$ für alle $j = 1,\dots,m$. Nach Induktion folgt nun $a_j^i = 0$ für alle i und j, also ist die Menge $\mathcal{B}$ linear unabhängig.

Ist W der von dieser Menge erzeugte Teilraum, dann ist $f(f^i(v_j)) = f^{i+1}(v_j) \in W$ für $i < k$ und $f(f^k(v_j)) = f(\tilde{v}_j) = 0 \in W$. Da die Elemente $f^i(v_j)$ eine Basis für W bilden, folgt damit $f(W) \subset W$, also ist W ein f–invarianter Teilraum.

Natürlich können wir W aber noch feiner zerlegen. Für $i = 1,\dots,m$ setze $\mathcal{B}_i = \{f^k(v_i), f^{k-1}(v_i),\dots,f(v_i),v_i\}$. Als Teilmenge der linear unabhängigen Menge $\mathcal{B}$ ist das linear unabhängig, und f bildet das erste Element von $\mathcal{B}_i$ auf 0 und jedes weitere Element auf das vorhergehende Element von $\mathcal{B}_i$ ab. Damit erzeugt jedes $\mathcal{B}_i$ einen f–invarianten Teilraum $W_i \subset W$ und die Matrixdarstellung der Einschränkung von f bezüglich $\mathcal{B}_i$ ist $J_{k+1}(0)$. Da die Vereinigung der $\mathcal{B}_i$ die Basis $\mathcal{B}$ von W ist, folgt die letzte Behauptung des Satzes aus 8.4 und 8.5. □

Korollar 8.12. *Sei V ein Vektorraum über einem Körper $\mathbb{K}$ und $f : V \to V$ eine nilpotente lineare Abbildung. Dann ist der Nilpotenzindex von f höchstens gleich $\dim(V)$.*

Beweis. Hat f Nilpotenzindex k, dann gibt es nach Definition ein Element $v_0 \in V$, sodass $f^{k-1}(v_0) =: \tilde{v}$ ungleich Null ist, während $f(\tilde{v}) = f^k(v_0) = 0$ gilt. Damit können wir aber das Lemma auf die linear unabhängige Menge $\{\tilde{v}\}$ anwenden, und sehen, dass die k–elementige Teilmenge $\{v_0, f(v_0), \dots, f^{k-1}(v_0)\} \subset V$ linear unabhängig ist. Damit kann die Menge höchsten $\dim(V)$ viele Elemente enthalten, also ist $k \leq \dim(V)$. □

Aus Lemma 8.12 kann man mit einem elementaren aber eher unangenehmen Induktionsargument eine Normalform für nilpotente lineare Abbildungen beweisen:

Satz 8.12. *Sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$ und $f : V \to V$ eine nilpotente lineare Abbildung. Dann gibt es eine Basis $\mathcal{B}$ von V, bezüglich derer die Matrixdarstellung von f Blockdiagonalform hat, wobei entlang der Hauptdiagonale nur Jordan–Blöcke mit Eigenwert* 0 *auftreten.*

Beweisidee. Sei n der Nilpotenzindex von f und betrachte $\operatorname{Im}(f^{n-1})$.Da $f^n = 0$ gilt, ist $\operatorname{Im}(f^{n-1}) \subset \operatorname{Ker}(f)$ und damit kann man Lemma 8.12 auf eine Basis von $\operatorname{Im}(f^{n-1})$ anwenden. Das liefert einen f–invarianten Teilraum $W \subset V$ sodass $f|_W$ eine Matrixdarstellung in Blockdiagonalform mit Jordan–Blöcken der Form $J_n(0)$ besitzt. Ist $W = V$, dann sind wir fertig. Falls nicht, dann gilt nach Konstruktion $f^{n-1}(W) = \operatorname{Im}(f^{n-1}) = f^{n-1}(V)$. Also gibt es einen größten Index k, sodass $f^k(W) \neq \operatorname{Im}(f^k)$ aber $f^{k+1}(W) = \operatorname{Im}(f^{k+1})$ gilt. Dann überlegt man, dass es eine linear unabhängige Teilmenge in $\operatorname{Ker}(f) \cap \operatorname{Im}(f^k)$ gibt, die gemeinsam mit $f^k(W)$ den Teilraum $\operatorname{Im}(f^k)$ erzeugt. Auf diese Teilmenge wendet man dann wieder Lemma 8.12 an, was einen f–invarianten Teilraum Teilraum $U \subset V$ liefert, auf dem f eine Matrixdarstellung der verlangten Form besitzt. Dann beweist man, dass $U \cap W = \{0\}$ gilt und damit ist der Teilraum $U \oplus W \subset V$ invariant mit einer geeigneten Matrixdarstellung für f. Das setzt man dann induktiv fort, bis man im letzten Schritt nur noch eine linear unabhängige Teilmenge von $\operatorname{Ker}(f)$ erhält, die die vorhandene Basis für eine Teilraum zu einer Basis für V ergänzt, bezüglich derer f eine Matrixdarstellung der verlangten Form hat. □

8.13. Die Jordan'sche Normalform über $\mathbb{C}$. Durch unsere bisherigen Überlegungen erhalten wir aus der Normalform für nilpotente lineare Abbildungen sofort eine Normalform für lineare Abbildungen, deren charakteristisches Polynom in ein Produkt von Polynomen ersten Grades zerfällt. Insbesondere gilt das immer über algebraisch abgeschlossenen Körpern und damit speziell über $\mathbb{C}$.

Satz 8.13. *Sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$ und sei $f : V \to V$ eine lineare Abbildung, deren charakteristisches Polynom in ein Produkt von Polynomen ersten Grades zerfällt. Seien $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ die verschiedenen Eigenwerte von f und für jedes i sei n_i die algebraische Vielfachheit von λ_i, und m_i die Potenz, mit der $(t - \lambda_i)$ im Minimalpolynom m_f von f auftritt. Dann gibt es eine Basis für V, bezüglich derer die Matrixdarstellung A von f folgende Form hat:*

A ist eine Blockdiagonalmatrix wie in Satz 8.5. Jeder der Blöcke auf der Hauptdiagonale ist ein Jordan Block der Form $J_{m_{ij}}(\lambda_i)$ für einen der Eigenwerte λ_i. Die Blockgrößen erfüllen $m_{ij} \leq m_i$, für mindestens ein j gilt $m_{ij} = m_i$ und $\sum_j m_{ij} = n_i$. Die Matrixdarstellung dieser Form ist bis auf die Reihenfolge der Jordan Blöcke eindeutig bestimmt.

Analog ist jede quadratische Matrix B über $\mathbb{K}$, deren Eigenwerte alle in $\mathbb{K}$ liegen, ähnlich zu einer Matrix der obigen Form. Diese Matrix heißt die Jordan'sche Normalform von B und ist bis auf die Reihenfolge der Blöcke eindeutig bestimmt. Schließlich sind zwei quadratische Matrizen über $\mathbb{K}$ deren charakteristische Polynome in ein Produkt von

Polynomen ersten Grades zerfallen genau dann ähnlich, wenn sich ihre Jordan'schen Normalformen nur durch die Reihenfolge der Blöcke unterscheiden.

Beweisskizze. Man zerlegt zuerst V in die direkte Summe der verallgemeinerten Eigenräume $V^f_{(\lambda_i)}$, siehe 8.11. Das liefert eine Matrixdarstellung in Blockdiagonalform sodass die Blöcke Matrixdarstellungen der Einschränkung von f auf den jeweiligen verallgemeinerten Eigenraum ist, also genügt es, diese Einschränkung zu betrachten.

Auf $V^f_{(\lambda_i)}$ ist $f - \lambda_i \operatorname{id}$ nilpotent, also erhalten wir nach Satz 8.12 eine Matrixdarstellung von $f - \lambda_i \operatorname{id}$ aus Jordan–Blöcken mit Eigenwert 0 und damit einer Darstellung von f aus Jordan–Blöcken mit Eigenwert λ_i. Nach unserer Beweisskizze für diesen Satz ist klar, dass die Größe dieser Blöcke höchsten gleich dem Nilpotenzindex der Einschränkung von $f - \lambda_i \operatorname{id}$ ist, und das mindestens einer der Blöcke auch tatsächlich diese Größe haben muss. Betrachtet man die resultierende Matrixdarstellung, dann liest man leicht ab, dass sich als charakteristisches Polynom gerade $(t - \lambda_i)^{\sum m_{ij}}$ und als Minimalpolynom $(t - \lambda_i)^{\max m_{ij}}$ ergibt, also folgen die Aussagen über die m_{ij}.

Hat man so eine Matrixdarstellung, dann kann man (durch geeignete Permutation der Basisvektoren) natürlich die Blöcke vertauschen. Um zu sehen, dass das die einzige Freiheit ist, muss man anhand eines vollen Beweises von Satz 8.12 überlegen, dass man die Blockgrößen für die einzelnen Eigenwerte aus Invarianten der Einschränkung von f auf den entsprechenden verallgemeinerten Eigenraum (wie etwa $\dim(\operatorname{Im}(f^k) \cap \operatorname{Ker}(f^\ell))$) ablesen kann. Die entsprechenden Aussagen über Matrizen folgen dann sofort. □

Beispiel 8.13. (1) Für diagonalisierbare Matrizen A ist natürlich die Diagonalform die Jordan'sche Normalform und in diesem Fall habe alle Jordan Blöcke die Größe Eins.

(2) Für 2×2–Matrizen A, für die beide Eigenwerte in $\mathbb{K}$ liegen, gibt es nur drei mögliche Jordan'sche Normalformen. Ist $p_A = (t - \lambda_1)(t - \lambda_2)$, dann muss A nach 7.2 diagonalisierbar sein, und die Diagonalform ist die Jordan'sche Normalform mit Blöcken $J_1(\lambda_1)$ und $J_1(\lambda_2)$.

Ist $p_A = (t-\lambda)^2$, dann gibt es zwei Möglichkeiten: Hat λ geometrische Vielfachheit 2, bzw. äquivalent ist $m_A = (t-\lambda)$, dann ist $A = \lambda \operatorname{id}$ und ist damit schon in Jordan'scher Normalform mit zwei Blöcken $J_1(\lambda)$. Ist andererseits $m_A = (t - \lambda)^2$, dann muss in der Jordan'schen Normalform ein Block $J_2(\lambda) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ vorkommen, also muss das schon die Jordan'sche Normalform sein.

(3) Für 3×3–Matrizen ist die Situation ähnlich einfach. Hat A drei verschiedene Eigenwerte, so muss A diagonalisierbar sein. Gibt es zwei verschieden Eigenwerte, λ und μ, der erste mit algebraischer Vielfachheit zwei, der zweite mit algebraischer Vielfachheit eines, dann erhalten wir einen Block der Form $J_1(\mu)$, und für den Rest die möglichen Jordan'schen Normalformen von 2×2–Matrizen mit charakteristischem Polynom $(t-\lambda)^2$. Somit ist nur der Fall $p_A = -(t - \lambda)^3$ interessant, und hier können wir wieder die verschiedenen Möglichkeiten für m_A untersuchen. Ist $m_A = (t - \lambda)$, dann ist $A = \lambda \operatorname{id}$, also diagonalisierbar. Für $m_A = (t - \lambda)^2$ müssen wir einen Block $J_2(\lambda)$ erhalten, dürfen aber keine größeren Blöcke haben. Somit kommt für die Jordan'sche Normalform nur ein Block $J_2(\lambda)$ und ein Block $J_1(\lambda)$ in Frage. Ist schließlich $m_A = (t - \lambda)^3$, dann muss ein Block $J_3(\lambda)$ auftauchen, also muss das schon die Jordan'sche Normalform sein.

(4) Betrachten wir 4×4–Matrizen A mit $p_A = (t - \lambda)^4$. (Der Fall verschiedener Eigenwerte kann wieder leicht auf die vorherigen Beispiele zurückgeführt werden). Dies ist der erste Fall, indem das Minimalpolynom alleine nicht mehr ausreicht, um die verschiedenen möglichen Jordan'schen Normalformen zu unterscheiden. Für $m_A = (t -$

λ) ist $A = \lambda \operatorname{id}$, für $m_A = (t-\lambda)^4$ ist die Jordan'sche Normalform $J_4(\lambda)$, und für $m_A = (t-\lambda)^3$ muss ein Block $J_3(\lambda)$ auftauchen, also bleibt nur noch ein Block $J_1(\lambda)$ übrig.

Im Fall $m_A = (t-\lambda)^2$ gibt es aber zwei Möglichkeiten für die Jordan'sche Normalform nämlich entweder zwei Blöcke $J_2(\lambda)$, oder ein Block $J_2(\lambda)$ und zwei Blöcke $J_1(\lambda)$. Um diese Möglichkeiten zu unterscheiden muss man nur bemerken, dass im ersten Fall $\dim(\operatorname{Im}(A - \lambda\mathbb{I})) = 2$ gilt, während im zweiten Fall diese Dimension gleich Eins ist.

Bemerkung 8.13. Im Prinzip sehen wir aus den letzten beiden Abschnitten auch, wie man die Jordan'sche Normalform einer Matrix A (bzw. einer linearen Abbildung f), deren Eigenwerte alle in $\mathbb{K}$ liegen, konkret bestimmen kann, sofern man die Eigenwerte und ihre algebraischen Vielfachheiten kennt (also die Nullstellen des charakteristischen Polynoms bestimmt hat). Man sieht im Prinzip auch, wie man eine Basis finden kann, für die die Matrixdarstellung Jordan'sche Normalform hat. Dazu muss man immer nur lineare Gleichungssysteme lösen.

8.14. Die Jordan'sche Normalform über $\mathbb{R}$. Im Bild der Matrizen kann man die Ergebnisse über die Jordan'sche Normalform über $\mathbb{C}$ direkt benutzen, um Ergebnisse für reelle Matrizen abzuleiten. Man kann ja eine reelle Matrix einfach auch als komplexe Matrix betrachten. Für allgemeine Vektorräume und lineare Abbildungen gibt es eine analoge Konstruktion, die sogenannte *Komplexifizierung*.

Sei dazu V ein reeller Vektorraum. Dann definiert man $V^{\mathbb{C}} := V \times V$ und definiert eine Skalarmultiplikation $\mathbb{C} \times V^{\mathbb{C}} \to V^{\mathbb{C}}$ durch $(a+ib)\cdot(v_1,v_2) = (av_1 - bv_2, bv_1 + av_2)$. Dann verifiziert man leicht, dass diese Skalarmultiplikation $V^{\mathbb{C}}$ mit der komponentenweisen Addition zu einem komplexen Vektorraum macht. Wir können V als Teilraum von $V^{\mathbb{C}}$ betrachten, indem wir $v \in V$ mit $(v,0) \in V^{\mathbb{C}}$ identifizieren. Dann folgt sofort, dass $(v_1,v_2) = (v_1,0)+(0,v_2) = v_1+i\cdot v_2$ ist. Man verifiziert auch leicht, dass eine Basis für den $\mathbb{R}$–Vektorraum V zugleich eine Basis für den $\mathbb{C}$–Vektorraum $V^{\mathbb{C}}$ bildet. Für eine lineare Abbildung $f : V \to V$ definiert man $\tilde{f} : V^{\mathbb{C}} \to V^{\mathbb{C}}$ durch $\tilde{f}(v_1,v_2) := (f(v_1), f(v_2))$. Dann verifiziert man leicht, dass $\tilde{f}$ eine komplex lineare Abbildung ist, die bezüglich einer Basis wie zuvor durch die gleiche Matrix dargestellt wird wie f. Wir können aber im weiteren problemlos im Bild der Matrizen bleiben.

Um die Jordan'sche Normalform über $\mathbb{R}$ zu beschreiben, erinnern wir uns zunächst an die Primfaktorzerlegung von reellen Polynomen aus 7.9. Hier treten einerseits Primfaktoren ersten Grades auf, die also die Form $(t-\lambda)$ für $\lambda \in \mathbb{R}$ haben. Die entsprechenden Summanden in der Primärzerlegung sind einfach verallgemeinerte Eigenräume zu reellen Eigenwerten. Auf diesen kann man dann wir im komplexen Fall vorgehen und erhält Jordan–Blöcke der Form $J_m(\lambda)$ für $\lambda \in \mathbb{R}$.

Andererseits erhält man Primfaktoren zweiten Grades, die keine reellen Nullstellen besitzen, also die Form $q = (t-\lambda)(t-\bar{\lambda})$ für $\lambda \in \mathbb{C} \setminus \mathbb{R}$ haben. Dafür kann man auch ein Analogon von Jordan–Blöcken definieren:

Definition 8.14. Für $\lambda = \alpha + i\beta \in \mathbb{C} \setminus \mathbb{R}$ und $m \in \mathbb{N}$, $m \geq 1$ definieren wir den reellen Jordan Block $\tilde{J}_{2m}(\lambda) \in M_{2m}(\mathbb{R})$ als (a_{jk}) wobei $a_{jj} = \alpha$ für alle $j = 1,\dots,2m$, $a_{2j-1,2j} = \beta$ und $a_{2j,2j-1} = -\beta$ für $j = 1,\dots,m$ und $a_{j,j+2} = 1$ für $j = 1,\dots,2m-2$. Der Block $\tilde{J}_{2m}(\lambda)$ sieht also ähnlich aus wie der komplexe Jordan Block $J_m(\lambda)$ wobei aber alle Eintragungen durch 2×2–Blöcke ersetzt werden, nämlich die Elemente λ auf der Hauptdiagonale durch $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ und die Einsen über der Hauptdiagonale durch $\mathbb{I}_2$.

Setzen wir weiterhin $\lambda = \alpha + i\beta$ und betrachten wir das reelle Polynom

$$q = (t - \lambda)(t - \bar{\lambda}) = t^2 - 2\alpha t + (\alpha^2 + \beta^2).$$

Das ist gerade das charakteristische Polynom der Matrix $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$. Mit Hilfe von Proposition 8.2 folgt daraus leicht induktiv, dass das charakteristische Polynom von $\tilde{J}_{2m}(\lambda)$ gleich q^m ist. Eine direkte Rechnung zeigt, dass auch das Minimalpolynom von $\tilde{J}_{2m}(\lambda)$ gleich q^m ist. Mit Hilfe der komplexen Jordan–Zerlegung zeigt man dann:

SATZ 8.14. *Sei V ein endlichdimensionaler reeller Vektorraum und $f : V \to V$ eine lineare Abbildung. Sei $p_f = (-1)^n(t - a_1)^{n_1} \cdots (t - a_k)^{n_k} q_1^{n'_1} \cdots q_\ell^{n'_\ell}$ die eindeutige Primfaktorzerlegung des charakteristischen Polynoms von f, wobei $a_1, \dots, a_k \in \mathbb{R}$ und jedes q_i ein Polynom vom Grad 2 ohne reelle Nullstellen ist. Für jedes $j = 1, \dots, \ell$ sei $\lambda_j \in \mathbb{C}$ die Nullstelle von q_j mit positivem Imaginärteil. Seien m_j und m'_j die Potenzen der irreduziblen Komponenten im Minimalpolynom m_f. Dann gilt:*

Es gibt eine Basis von V bezüglich derer die Matrixdarstellung von f Blockdiagonalform mit endlich vielen Jordan Blöcken $J_{m_{jr}}(a_j)$ und $\tilde{J}_{2m'_{jr}}(\lambda_j)$ besitzt. Hierbei ist $m_{jr} \leq m_j$ und $m'_{jr} \leq m'_j$ für alle r und für mindestens ein r gilt Gleichheit. Außerdem ist $\sum_r m_{jr} = n_j$ und $\sum_r m'_{jr} = n'_j$ für alle j. Bezüglich der Eindeutigkeit dieser Darstellung und für quadratische Matrizen gelten analoge Aussagen wie in Satz 8.13.

KAPITEL 9

Normen und innere Produkte

Mit diesem Kapitel verlassen wir endgültig die allgemeinen Körper und schränken uns ganz auf die Fälle $\mathbb{K} = \mathbb{R}$ und $\mathbb{K} = \mathbb{C}$ ein. Dafür kehren wir zu Themen zurück, die im Ansatz schon aus der Schule bekannt sind, nämlich zu inneren Produkten und den damit verbundenen Konzepten der Länge von Vektoren und des Winkels zwischen zwei Vektoren. Der Längenbegriff kann tatsächlich allgemeiner mit Hilfe des Begriffs der Norm formuliert werden, was auch Bezüge zur Analysis liefert.

Normierte Räume

Zunächst beschäftigen wir uns mit dem Begriff der Norm, der es erlaubt, jedem Vektor eine Länge zuzuordnen. Das liefert eine Distanzfunktion, mit deren Hilfe Konvergenz und Stetigkeit definiert werden können. Der Normbegriff ist einerseits als Ausblick auf unendlichdimensionalen Räumen wichtig. Im Endlichdimensionalen ist insbesondere der Fall von Räumen der Form $L(V, V)$ interessant, wo man mit Hilfe des Normbegriffs gewisse stetige Funktionen auf lineare Abbildungen bzw. Matrizen anwenden kann. Wir werden uns in diesem Abschnitt eher kurz fassen und Grundkenntnisse aus der Analysis voraussetzen.

9.1. Normen. Die allgemeine Definition einer Norm ist intuitiv ziemlich einsichtig:

Definition 9.1. (1) Sei V ein Vektorraum über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$. Eine *Norm* auf V ist eine Funktion $\| \ \| : V \to \mathbb{R}$ mit folgenden Eigenschaften:
(N1) $\|v\| \geq 0$ für alle $v \in V$ und $\|v\| = 0 \iff v = 0$.
(N2) Für $v \in V$ und $\lambda \in \mathbb{K}$ ist $\|\lambda v\| = |\lambda| \cdot \|v\|$.
(N3) Für $v, w \in V$ ist $\|v + w\| \leq \|v\| + \|w\|$.

(2) Ein *normierter Vektorraum* über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$ ist ein $\mathbb{K}$–Vektorraum V zusammen mit einer Norm auf V.

Die Bedingung (N1) wird üblicherweise als "Nichtnegativität" bezeichnet, Bedingung (N2) als "positive Homogenität". Denkt man an die geometrische Interpretation der Vektoraddition, dann sagt (N3) gerade, dass die Länge einer Seite eines Dreiecks höchsten so groß sein kein, wie die Summe der Längen der beiden anderen Seiten, weshalb diese Bedingung als *Dreiecksungleichung* bezeichnet wird.

Beispiel 9.1. (1) Das wichtigste Beispiel einer Norm auf einem endlichdimensionalen Vektorraum ist die aus der Schule und der Grundvorlesung Analysis bekannte *euklidische Norm* $\| \ \|_2$ auf $\mathbb{R}^n$ und $\mathbb{C}^n$. Diese Norm ist definiert durch $\|(x_1, \dots, x_n)\|_2 := \sqrt{\sum_{j=1}^n |x_j|^2}$, wobei man für $\mathbb{K} = \mathbb{R}$ natürlich den Betrag auf der rechten Seite weglassen darf. Die Eigenschaften (N1) und (N2) sind dann offensichtlich erfüllt. Für (N3) benutzt man zunächst die Dreiecksungleichung für den Absolutbetrag auf $\mathbb{R}$, siehe Proposition 6.4.12 von [**2**]. Daraus folgt sofort

$$\textstyle\sum_i |x_i + y_i|^2 \leq \sum_i (|x_i|^2 + 2|x_i||y_i| + |y_i|^2) \leq (\|x\|_2)^2 + 2\|x\|_2\|y\|_2 + (\|y\|_2)^2,$$

und damit (N3) durch Ziehen der Wurzel.

(2) Betrachten wir wieder $\mathbb{R}^n$ oder $\mathbb{C}^n$ und die Funktion $\| \|_1$, die definiert ist durch $\|(x_1,\dots,x_n)\|_1 = \sum_{j=1}^n |x_j|$. Hier sind wieder (N1) und (N2) offensichtlich, und (N3) folgt sofort aus der Dreiecksungleichung für den Absolutbetrag.

Analog definiert $\|(x_1,\dots,x_n)\|_\infty = \max\{|x_1|,\dots,|x_n|\}$ eine Norm auf $\mathbb{K}^n$. Auch dafür sind (N1) und (N2) offensichtlich. Für (N3) bemerkt man, dass für jedes $j = 1,\dots,n$ die Ungleichung $|x_j + y_j| \leq |x_j| + |y_j|$ gilt. Geht man auf der rechten Seite zu den Maxima über, dann bleibt die Ungleichung richtig, also ist $|x_j+y_j| \leq \|x\|_\infty + \|y\|_\infty$, und da das für alle j gilt, folgt (N3).

(3) Die Beispiele (1) und (2) sind tatsächlich Spezialfälle einer Familie $\| \|_p$ von Normen für $p \in (1,\infty) \subset \mathbb{R}$, wobei $\|(x_1,\dots,x_n)\|_p = \left(\sum_{j=1}^n |x_j|^p\right)^{1/p}$. Hier sind immer noch (N1) und (N2) offensichtlich, (N3) ist allgemein schwieriger zu beweisen. Alle diese Normen besitzen Verallgemeinerungen auf geeignete (unendlichdimensionale) Räume von Folgen. Insbesondere macht jede dieser Normen auf dem Raum aller endlichen Folgen in $\mathbb{K}$ Sinn.

(4) In der Analysis und in der Funktionalanalysis spielen verschiedene Normen auf Funktionenräumen eine wichtige Rolle. Wir bemerken hier nur zum Beispiel, dass auf dem Raum $C([a,b],\mathbb{R})$ aller stetigen Funktionen auf einem abgeschlossenen Intervall $[a,b] \subset \mathbb{R}$ sowohl $\sup_{x\in[a,b]} |f(x)|$ als auch $\int_a^b |f(x)|dx$ eine Norm definiert.

Hat man eine Norm $\| \|$ auf V, dann kann man eine zugehörige Distanzfunktion $d : V \times V \to \mathbb{R}$ definieren, indem man $d(v,w) := \|w - v\|$ setzt. Es ist leicht zu zeigen, dass diese Distanzfunktion die aus der Analysis bekannten Eigenschaften erfüllt:

Proposition 9.1. *Sei V ein Vektorraum über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$, sei $\| \|$ eine Norm auf V und sei $d : V\times V \to \mathbb{R}$ die zugehörige Distanzfunktion. Dann ist (V,d) ein metrischer Raum (im Sinne der Analysis), d.h. es für alle $u,v,w \in V$ gilt:*

(D1) *$d(v,w) \geq 0$ und $d(v,w) = 0$ gilt genau dann, wenn $v = w$ gilt.*
(D2) *$d(v,w) = d(w,v)$ (Symmetrie)*
(D3) *$d(u,w) \leq d(u,v) + d(v,w)$ (Dreiecksungleichung)*

Beweis. Nach (N1) ist $d(v,w) = \|w-v\| \geq 0$, und Gleichheit gilt nur für $0 = w-v$, also für $v = w$, und (D1) ist gezeigt. Für (D2) bemerken wir, dass $v - w = (-1)(w - v)$ gilt, also nach (N2) $\|v - w\| = |-1|\|w - v\|$ gilt. Wegen $w - u = (w - v) + (v - u)$ folgt auch (D3) sofort aus (N3). □

Damit kann man nun einige Grundkonzepte aus der Analysis in der bekannten Art definieren:

- Eine Folge $(v_n)_{n\in\mathbb{N}}$ mit $v_n \in V$ *konvergiert* gegen ein Element $v \in V$, wenn es zu jedem $\varepsilon > 0$ einen Index $N \in \mathbb{N}$ gibt, sodass $d(v_n,v) < \varepsilon$ für alle $n \geq N$ gilt.
- Eine Folge $(v_n)_{n\in\mathbb{N}}$ mit $v_n \in V$ heißt *Cauchy–Folge*, wenn es zu jedem $\varepsilon > 0$ einen Index $N \in \mathbb{N}$ gibt, sodass $d(v_n,v_m) < \varepsilon$ für alle $m,n \geq N$ gilt.
- Eine Funktion $f : V \to V$ heißt stetig ein einem Punkt $v_0 \in V$, wenn es zu jedem $\varepsilon > 0$ ein $\delta > 0$ gibt, sodass aus $d(v_0,v) < \varepsilon$ immer $d(f(v_0),f(v)) < \varepsilon$ folgt.

Es stellt sich heraus, dass man im Fall $V = \mathbb{R}^n$ oder $\mathbb{C}^n$ für jede Wahl einer Norm die gleichen Begriffe erhält ("alle Normen sind äquivalent"). Für einen allgemeinen endlichdimensionalen Vektorraum V kann man einen linearen Isomorphismus mit $\mathbb{R}^n$

($n = \dim(V)$) wählen, und man zeigt, dass so ein Isomorphismus mit den oben definierten Begriffen verträglich ist. Damit sind auch auf V alle Normen äquivalent. Insbesondere folgt aus den aus der Analysis bekannten Resultaten, dass in jedem endlichdimensionalen normierten Vektorraum V eine Folge genau dann konvergiert, wenn sie eine Cauchy–Folge ist ("V ist vollständig").

In unendlichdimensionalen Räumen ist das ganz anders. In diesem Fall ist die Vollständigkeit eines Raumes eine höchst nicht–triviale und sehr wichtige Eigenschaft, vollständige normierte Räume nennt man *Banachräume*. Weiters führen verschiedene Normen im unendlichdimensionalen oft zu verschiedenen Topologien, also zu verschiedenen Begriffen von Konvergenz, Stetigkeit und Cauchy–Folgen. Betrachten wir etwa den im obigen Beispiel erwähnten Raum aller endlichen Folgen auf $\mathbb{R}$ mit den Normen $\| \ \|_p$ für $p \in \mathbb{R} \cup \{\infty\}$, dann erhält man für verschiedene p verschiedene Topologien und nie einen vollständigen Raum.

9.2. Die Operatornorm. Wir erwähnen hier nur kurz einen wichtigen Spezialfall einer Norm. Sei $(V, \| \ \|)$ ein endlichdimensionaler normierter Vektorraum über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$, und $f : V \to V$ eine lineare Abbildung. Dann zeigt man, dass es eine Konstante $C \in \mathbb{R}$ gibt, sodass $\|f(v)\| \leq C\|v\|$ gibt ("f ist beschränkt"). Die kleinste Konstante für die das gilt, heißt die *Operatornorm* von f und wird mit $\|f\|$ bezeichnet. Nach Definition gilt also $\|f(v)\| \leq \|f\|\|v\|$. Daraus folgt aber sofort die wichtigste Eigenschaft der Operatornorm. Ist nämlich $g : V \to V$ noch eine lineare Abbildung, dann ist auch $g \circ f : V \to V$ linear und nach Definition gilt für jedes Element $v \in V$ die Ungleichung

$$\|(g \circ f)(v)\| = \|g(f(v))\| \leq \|g\|\|f(v)\| \leq \|g\|\|f\|\|v\|.$$

Damit folgt aber aus der Definition der Operatornorm sofort, dass $\|g \circ f\| \leq \|g\|\|f\|$. Bilden wir insbesondere $f^2 = f \circ f$, dann gilt $\|f\|^2 \leq \|f\|^2$, und induktiv folgt $\|f^k\| \leq \|f\|^k$ für alle $k \in \mathbb{N}$. Natürlich kann man das insbesondere auf den Raum $\mathbb{R}^n$ mit der euklidischen Norm anwenden um eine Operatornorm auf dem Raum $M_n(\mathbb{R})$ der $n \times n$–Matrizen zu erhalten, die $\|A^k\| \leq \|A\|^k$ erfüllt, wobei A^k die k–te Potenz bezüglich der Matrizenmultiplikation bezeichnet.

Damit kann man nun die Idee, Polynome auf lineare Abbildungen und Matrizen anzuwenden (siehe 8.6) auf konvergente Potenzreihen erweitern. Ein wichtiger Spezialfall ist die Exponentialfunktion. Wie aus der Analysis bekannt, konvergiert die Reihe $\sum_{k=0}^{\infty} \frac{1}{k!}x^k$ für jedes $x \in \mathbb{R}$ gegen $e^x \in \mathbb{R}$. Betrachtet man nun eine Matrix $A \in M_n(\mathbb{R})$, dann kann man für jeden Wert $n \in \mathbb{N}$ natürlich $B_n := \sum_{k=0}^{n} \frac{1}{k!}A^k \in M_n(\mathbb{R})$ bilden, und dann die Folge $(B_n)_{n\in\mathbb{N}}$ betrachten. Für $\varepsilon > 0$ folgt nun aus der Konvergenz der reellen Exponentialreihe für $x = \|A\| \in \mathbb{R}$, dass es einen Index $N \in \mathbb{N}$ gibt, sodass $\sum_{k=n}^{m} \frac{1}{k!}\|A\|^k < \varepsilon$ für alle $m \geq n \geq N$ gilt. Dann gilt aber auch

$$\|B_m - B_n\| = \|\sum_{k=n}^{m} \tfrac{1}{k!}A^k\| \leq \sum_{k=n}^{m} \tfrac{1}{k!}\|A^k\| \leq \sum_{k=n}^{m} \tfrac{1}{k!}\|A\|^k < \varepsilon.$$

Das bedeutet aber gerade, dass $(B_n)_{n\in\mathbb{N}}$ ein Cauchy–Folge in $M_n(\mathbb{R})$ (bezüglich der Operatornorm) ist. Damit konvergiert diese Folge in $M_n(\mathbb{R})$ gegen eine Matrix, die man sinnvollerweise mit e^A bezeichnet. Aus unseren Überlegungen folgt sofort, dass $\|e^A\| \leq e^{\|A\|}$ gilt. Somit kann man die Exponentialfunktion allgemein für Matrizen (und ganz analog für lineare Abbildungen auf beliebigen endlichdimensionalen Vektorräumen) definieren.

Analog zu oben kann man aus der Stetigkeit der reellen Exponentialfunktion leicht schließen, dass das Matrizenexponential stetig als Funktion $M_n(\mathbb{R}) \to M_n(\mathbb{R})$ ist. Auch andere schöne Eigenschaften der reellen Exponentialfunktion lassen sich leicht auf das Matrizenexponential übertragen. Interessant sind hier insbesondere Exponentialkurven $t \mapsto e^{tA}$ für $t \in \mathbb{R}$ und eine fixe Matrix $A \in M_n(\mathbb{R})$, die man als Funktion $\mathbb{R} \to M_n(\mathbb{R})$ betrachten kann. Da $M_n(\mathbb{R})$ ja mit $\mathbb{R}^{n^2}$ identifiziert werden kann, können die aus der Analysis bekannten Konzepten von Differenzierbarkeit problemlos auf diese Kurven angewandt werden. Man zeigt, dass für jede Matrix A die Kurve $c(t) := e^{tA}$ differenzierbar ist, und für die Ableitung gilt $c'(t) = A \cdot c(t)$, wobei der Punkt das Matrizenprodukt bezeichnet. Daraus folgt dann sofort, dass die Kurve $c(t)$ beliebig oft differenzierbar ist. Aus der Definition folgt sofort, dass $c(0) = \mathbb{I}_n$ gilt.

Betrachten wir nun einen Vektor $v \in \mathbb{R}^n$, dann können wir natürlich für jedes $t \in \mathbb{R}$ die Matrix e^{tA} auf den Vektor v anwenden. Bezeichnen wir den resultierenden Vektor mit $v(t)$, dann definiert das eine Kurve $t \mapsto v(t)$ in $\mathbb{R}^n$. Man schließt sofort, dass diese Kurve stetig und sogar beliebig oft differenzierbar ist, wobei die Ableitung durch $v'(t) = A(v(t))$ gegeben ist. Außerdem gilt natürlich $v(0) = \mathbb{I}_n v = v$. Das bedeutet aber gerade, dass die Kurve $v(t) = e^{tA}(v)$ eine Lösung der Differentialgleichung $v'(t) = A(v(t))$ mit Anfangsbedingung $v(0) = v$ ist. Aus grundlegenden Resultaten der Analysis folgt, dass eine Lösung dieser Gleichung durch ihren Wert in einem Punkt eindeutig bestimmt ist. Damit liefert das Matrizenexponential alle Lösungen von linearen gewöhnlichen Differentialgleichungen in $\mathbb{R}^n$ mit konstanten Koeffizienten.

Um das Matrizenexponential konkret auszurechnen kann man Ideen benutzen, die uns von Polynomen von Matrizen bereits vertraut sind. Nach Definition erhält man e^{tA} als Limes einer Folge $(B_n)_{n\in\mathbb{N}}$ in $M_n(\mathbb{R})$, wobei $B_n = \sum_{k=0}^n \frac{t^k}{k!}A^k$. Für eine invertierbare Matrix $T \in M_n(\mathbb{R})$ ist nun $(TAT^{-1})^k = TA^kT^{-1}$ und allgemeiner $p(TAT^{-1}) = Tp(a)T^{-1}$ für jedes Polynom $p \in \mathbb{R}[x]$, siehe Bemerkung 8.6. Nun ist jedes der Folgenglieder B_n als ein Polynom in A gegeben. Berechnet man also $e^{tTAT^{-1}}$, dann muss man nur die B_n durch TB_nT^{-1} ersetzen. Nun sieht man sofort, dass die Abbildung $B \mapsto TBT^{-1}$ stetig ist, also ist

$$e^{tTAT^{-1}} = \lim_n TB_nT^{-1} = T(\lim_n B_n)T^{-1} = T(e^{tA})T^{-1}.$$

Ist etwa A diagonalisierbar, dann finden wir eine invertierbare Matrix T, sodass TAT^{-1} eine Diagonalmatrix D ist. Man rechnet aber sofort nach, dass für eine Diagonalmatrix D mit Eintragungen $\lambda_1, \dots, \lambda_n$ auch e^{tD} diagonal mit Eintragungen $e^{t\lambda_1}, \dots, e^{t\lambda_n}$ ist. Damit kann man aber auch $e^{tA} = T^{-1}(e^{tD})T$ sofort berechnen. Analog kann man die Berechnung beliebiger Matrizenexponentiale über die Jordan'sche Normalform (siehe 8.13 und 8.14) auf die Berechnung von Matrixexponentialen von Jordan–Blöcken zurückführen, die nicht so schwierig ist.

Innere Produkte

Eine Norm auf einem Vektorraum liefert den Begriff der Länge eines Vektors. Spezielle Normen, etwa die euklidische Norm $\| \ \|_2$ auf $\mathbb{R}^n$ erlauben es aber, auch den Winkel zwischen zwei Vektoren zu definieren. Diese speziellen Normen kommen von inneren Produkten, die dann eine Vielzahl an zusätzlichen Strukturen auf einem Vektorraum liefern.

9.3. Grundlegende Definitionen. Sei V ein reeller Vektorraum. Eine *Bilinearform* auf V ist eine Abbildung $b : V \times V \to \mathbb{R}$, $(v, w) \mapsto b(v, w)$, sodass $b(v + \lambda v', w) = b(v, w) + \lambda b(v', w)$ und $b(v, w + \lambda w') = b(v, w) + \lambda b(v, w')$ für alle $v, v', w, w' \in V$ und $\lambda \in \mathbb{K}$ gelten. Diese Bedingungen sagen gerade, dass für fixes $v \in V$ die Funktionen $w \mapsto b(v, w)$ und $w \mapsto b(w, v)$ lineare Abbildungen $V \to \mathbb{R}$ sind.

Sei $b : V \times V \to \mathbb{R}$ eine Bilinearform.

(1) b heißt *symmetrisch* falls $b(w, v) = b(v, w)$ für alle $v, w \in V$ gilt
(2) Ist b symmetrisch, dann heißt b *positiv semidefinit* falls $b(v, v) \geq 0$ für alle $v \in V$ gilt, und *positiv definit*, falls zusätzlich $b(v, v) = 0$ nur für $v = 0$ gilt.
(3) Ein *inneres Produkt* ist eine positiv definite symmetrische Bilinearform.
(4) Ein *euklidischer Vektorraum* ist ein reeller Vektorraum V zusammen mit einem inneren Produkt auf V.

Bemerkung 9.3. (1) Ist $b : V \times V \to \mathbb{R}$ eine Bilinearform, dann folgt aus der Linearität in der ersten Variable sofort, dass $b(0, v) = 0$ für alle $v \in V$ gilt. Ist $0 \in V$ der einzige Vektor, für den das vorkommt, dann nennt man die Form b *nicht ausgeartet* oder *nicht degeneriert*. Innere Produkte sind natürlich nicht ausgeartet, weil in diesem Fall schon $b(v, v) = 0$ nur für $v = 0$ möglich ist.

Sei $b : V \times V \to \mathbb{R}$ nicht ausgeartet und seien $v, v' \in V$ zwei Vektoren, sodass $b(v, w) = b(v', w)$ für alle $w \in V$ gilt. Dann folgt aus der Linearität in der ersten Variable sofort, dass $0 = b(v - v', w)$ für alle $w \in V$ gilt, was nach Voraussetzung $v - v' = 0$, also $v = v'$ impliziert.

(2) Innere Produkte werden üblicherweise mit $(v, w) \mapsto \langle v, w\rangle$ bezeichnet.

Beispiel 9.3. (1) Das wichtigst Beispiel eines inneren Produktes ist das *Standard innere Produkt* auf $\mathbb{R}^n$, das durch

$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n)\rangle := x_1y_1 + \cdots + x_ny_n.$$

definiert ist. Man sieht sofort, dass dieser Ausdruck bilinear und symmetrisch ist. Außerdem ist $\langle x, x\rangle = x_1^2 + \cdots + x_n^2$, also folgt sofort, dass $\langle\ ,\ \rangle$ tatsächlich ein inneres Produkt definiert.

(2) Ähnlich wie bei Normen sind auch innere Produkte auf unendlichdimensionalen Räumen sehr interessant. Wir erwähnen hier nur ein Beispiel, nämlich den Raum $C([a, b], \mathbb{R})$ aller stetigen, reellwertigen Funktionen auf einem abgeschlossenen Intervall $[a, b] \subset \mathbb{R}$. Aus den aus der Analysis bekannten Eigenschaften des Integrals kann man leicht schließen, dass

$$\langle f, g\rangle := \int_a^b f(t)g(t)dt$$

ein inneres Produkt auf diesem Raum definiert.

9.4. Sesquilinearformen. Natürlich kann ganz analog zu Bilinearformen $V \times V \to \mathbb{R}$ auf einem reellen Vektorraum V auch $\mathbb{C}$–wertige komplexe Bilinearformen auf komplexen Vektorräumen betrachten, und alle Begriffe aus 9.5 mach auch über $\mathbb{C}$ Sinn. Es gibt allerdings ein gravierendes Problem, nämlich dass komplexe Bilinearformen niemals positiv definit sein können. Für $v \in V$ und $b : V \times V \to \mathbb{C}$ komplex bilinear gilt nämlich $b(iv, iv) = i^2b(v, v) = -b(v, v)$. Daher benötigen wir einen etwas anderen Begriff um ein gutes Analogon reeller innerer Produkte zu erhalten, nämlich den Begriff der *Sesquilinearform*.

Definition 9.4. Sei V ein Vektorraum über $\mathbb{C}$. Eine Sesquilinearform auf V ist eine Funktion $s : V \times V \to \mathbb{C}$, die $s(v + \lambda v', w) = s(v, w) + \lambda s(v', w)$, sowie $s(w, v) = \overline{s(v, w)}$ für alle $v, v', w \in V$ und alle $\lambda \in \mathbb{C}$ erfüllt.

Aus den beiden Bedingungen in der Definition folgt sofort, dass $s(v, w + \lambda w') = s(v, w) + \bar{\lambda} s(v, w')$ gilt. Man sagt, eine Sesquilinearform ist *konjugiert linear* in der zweiten Variable. Andererseits gilt natürlich $s(v, v) = \overline{s(v, v)}$, also $s(v, v) \in \mathbb{R} \subset \mathbb{C}$

für alle $v \in V$. Man sagt nun eine Sesquilinearform s ist *positiv semidefinit*, wenn $s(v,v) \geq 0$ für alle $v \in V$ gilt und s heißt *positiv definit*, wenn zusätzlich $s(v,v) = 0$ nur für $v = 0$ gilt. Der Begriff "nicht degeneriert" macht natürlich für Sesquilinearformen in genau der selben Form Sinn, wie für Bilinearformen, und wieder sind positiv definite Sesquilinearformen automatisch nicht degeneriert.

Positiv definite Sesquilinearformen werden *hermitische innere Produkte* genannt und meist mit $\langle\ ,\ \rangle$ bezeichnet. Ein *unitärer Vektorraum* ist ein komplexer Vektorraum V zusammen mit einem hermitischen inneren Produkt auf V.

Formal kann man symmetrische Bilinearformen und Sesquilinearformen gleichzeitig behandeln, indem man einfach immer mit Sesquilinearformen arbeitet und im reellen Fall die Konjugation als Identität definiert.

Beispiel 9.4. Betrachte $V = \mathbb{C}^n$, und definiere $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ durch $\langle z, w\rangle = z_1\bar{w}_1 + \cdots + z_n\bar{w}_n$. Offensichtlich ist das eine Sesquilinearform und wegen $\langle z, z\rangle = \sum z_j\bar{z}_j = \sum |z_j|^2$ ist diese Form positiv definit. Das ist das *Standard hermitische innere Produkt* auf $\mathbb{C}^n$.

9.5. Vom inneren Produkt zur Norm. Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum. Dann ist $\langle v, v\rangle \geq 0$ für jedes $v \in V$, also können wir $\|v\| := \sqrt{\langle v, v\rangle}$ bilden. Wir wollen zeigen, dass dies eine Norm auf V definiert. Dazu brauchen wir ein Resultat, das noch öfters sehr nützlich sein wird, nämlich die sogenannte *Cauchy–Schwarz–Ungleichung.*

Lemma 9.5 (Cauchy–Schwarz–Ungleichung). *Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum. Dann ist $|\langle v, w\rangle|^2 \leq \langle v, v\rangle\langle w, w\rangle$. Gleichheit gilt genau dann, wenn v und w linear abhängig sind.*

Beweis. Für $w = 0$ sind offensichtlich beide Seiten gleich Null, also nehmen wir $w \neq 0$ an. Für jedes $\lambda \in \mathbb{K} = \mathbb{R}$ bzw. $\mathbb{C}$ gilt

$$0 \leq \langle v - \lambda w, v - \lambda w\rangle = \langle v, v\rangle - \lambda\langle v, w\rangle - \bar{\lambda}\langle w, v\rangle + \lambda\bar{\lambda}\langle w, w\rangle.$$

Setzt man $\lambda = \langle v, w\rangle/\langle w, w\rangle$, so erhält man $0 \leq \langle v, v\rangle - \frac{|\langle v,w\rangle|^2}{\langle w,w\rangle}$, und die Ungleichung folgt durch Multiplizieren mit der positiven reellen Zahl $\langle w, w\rangle$. In der obigen Ungleichung gilt außerdem genau dann Gleichheit, wenn $v - \lambda w = 0$ gilt, also v und w linear abhängig sind. □

Satz 9.5. *Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum. Dann definiert $\|v\| := \sqrt{\langle v, v\rangle}$ eine Norm auf V. Diese Norm erfüllt die Parallelogrammidentität*

$$\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2).$$

Weiters gelten die Polarisierungsformeln:

(1) für $(V, \langle\ ,\ \rangle)$ euklidisch: $\langle v, w\rangle = \frac{1}{4}(\|v + w\|^2 - \|v - w\|^2)$.

(2) für $(V, \langle\ ,\ \rangle)$ unitär: $\langle v, w\rangle = \frac{1}{4}(\|v + w\|^2 - \|v - w\|^2 + i\|v + iw\|^2 - i\|v - iw\|^2)$.

Beweis. Nach Konstruktion ist $\|v\| \geq 0$ und $\|v\| = 0$ impliziert $\langle v, v\rangle = 0$ und damit $v = 0$, also ist (N1) erfüllt. Für $\lambda \in \mathbb{K}$ ist $\langle \lambda v, \lambda v\rangle = \lambda\bar{\lambda}\langle v, v\rangle$, also folgt $\|\lambda v\| = |\lambda| \cdot \|v\|$ wegen $\lambda\bar{\lambda} = |\lambda|^2$. Wiederum wegen der Bilinearität gilt

$$(*) \qquad \langle v \pm w, v \pm w\rangle = \langle v, v\rangle \pm \langle v, w\rangle \pm \langle w, v\rangle + \langle w, w\rangle.$$

Für positives Vorzeichen liefert diese Gleichung $\|v + w\|^2 = \|v\|^2 + 2\,\mathrm{Re}(\langle v, w\rangle) + \|w\|^2$. Natürlich ist $\mathrm{Re}(\langle v, w\rangle) \leq |\langle v, w\rangle|$ und nach der Cauchy–Schwarz Ungleichung ist $|\langle v, w\rangle| \leq \|v\| \cdot \|w\|$, also erhalten wir $\|v + w\|^2 \leq \|v\|^2 + 2\|v\| \cdot \|w\| + \|w\|^2$, und das impliziert natürlich die Dreiecksungleichung für $\| \ \|$. Addiert man die Gleichungen $(*)$ für positives und negatives Vorzeichen, dann erhält man direkt die Parallelogrammidentität.

Die Differenz der beiden Gleichungen $(*)$ für positives und negatives Vorzeichen liefert $\|v+w\|^2 - \|v-w\|^2 = 2\langle v,w\rangle + 2\langle w,v\rangle$. Im reellen Fall liefert das sofort die Polarisierungsformel. Im komplexen Fall muss man nur noch bemerken, dass das auch $\|v+iw\|^2 - \|v-iw\|^2 = -2i\langle v,w\rangle + 2i\langle w,v\rangle$ impliziert. Multipliziert man diese Gleichung mit i und addiert sie zur obigen, dann erhält man die komplexe Polarisierungsformel. □

Definition 9.5. Ein reeller bzw. komplexer *Hilbertraum* ist ein euklidischer bzw. unitärer Vektorraum $(V, \langle\ ,\ \rangle)$, der bezüglich der Norm $\|v\| = \sqrt{\langle v,v\rangle}$ vollständig ist.

Bemerkung 9.5. Ein inneres Produkt liefert also eine Norm auf V und wegen der Polarisierungsformel ist das innere Produkt durch diese Norm vollständig bestimmt. Es zeigt sich, dass die Parallelogrammidentität charakteristisch für Normen ist, die von inneren Produkten kommen. Man kann leicht elementar-geometrisch zeigen, dass diese Identität äquivalent zum Satz von Pythagoras ist. Sie hat aber den Vorteil, dass man den Begriff des rechten Winkels (bzw. der Orthogonalität) in der Formulierung nicht benötigt. Man kann allgemein beweisen, dass für eine Norm, die die Parallelogrammidentität erfüllt, durch die Polarisierungsformel ein inneres Produkt auf V definiert wird, das gerade die gegebene Norm liefert.

Beispiel 9.5. (1) Das Standard innere Produkt $\langle x,y\rangle = \sum x_i y_i$ auf $\mathbb{R}^n$ liefert als zugehörige Norm die euklidische Norm $\|x\|_2 = \sqrt{\sum x_i^2}$ (daher auch der Name "euklidische Norm"). Analog liefert das Standard hermitische innere Produkt $\langle z,w\rangle = \sum z_j \bar{w}_j$ die euklidische Norm auf $\mathbb{C}^n = \mathbb{R}^{2n}$. Wie wir bereits in 9.1 bemerkt haben, sind endlichdimensionale normierte Räume immer vollständig, also erhalten wir hier jeweils einen Hilbertraum.

(2) Für $p \neq 2$ und $n > 1$ kommt keine der Normen $\| \ \|_p$ auf $\mathbb{R}^n$ aus Beispiel (3) von 9.1 von einem inneren Produkt. Betrachten wir nämlich die Standardbasis $\{e_1, \dots, e_n\}$, dann ist $\|e_i\|_p = 1$ für alle i und p. Andererseits ist $\|e_1 \pm e_2\|_p = (1^p + 1^p)^{1/p} = 2^{1/p}$, also $\|e_1+e_2\|^2 + \|e_1-e_2\|^2 = 2^{1+2/p}$. Damit die Parallelogrammidentität erfüllt ist, muss das gleich 4, also $2/p = 1$ sein. Für $p = \infty$ ist $\|e_1 \pm e_2\|_\infty = 1$ und damit liefert eine Seite der Parallelogrammidentität zwei, die andere vier.

(3) Das Standardbeispiel eines unendlichdimensionalen Hilbertraumes ist der Raum ℓ^2 aller komplexen Folgen $(a_n)_{n\in\mathbb{N}}$, für die $\sum_{n\in\mathbb{N}} |a_n|^2 < \infty$ gilt. Man kann direkt verifizieren, dass diese Folgen einen Teilraum des Raumes aller komplexwertigen Folgen bilden. Weiters zeigt man, dass für zwei Folgen $(a_n), (b_n) \in \ell^2$ die Summe $\sum_{n\in\mathbb{N}} a_n \bar{b}_n$ immer konvergiert. Damit kann man

$$\langle (a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \rangle := \sum_{n\in\mathbb{N}} a_n \bar{b}_n$$

definieren, und man zeigt, dass das ein inneres Produkt auf ℓ^2 ist. Dieses innere Produkt liefert dann die Norm $\|(a_n)\| = \sqrt{\sum_{n\in\mathbb{N}} |a_n|^2}$ und man verifiziert, dass ℓ^2 mit dieser Norm ein vollständiger Raum ist.

Orthogonalität und Orthonormalbasen

Innere Produkte liefern den Begriff der Orthogonalität (der allgemeiner auch für nicht entartete Bilinear– bzw. Sesquilinearformen Sinn macht), der zum Begriff des Winkels zwischen zwei Vektoren verfeinert werden kann.

9.6. Orthogonalität. Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum. Dann nennen wir zwei Elemente $v, w \in V$ *orthogonal* und schreiben $v \perp w$, wenn $\langle v, w\rangle = 0$ gilt. Ist $A \subset V$ eine beliebige Teilmenge, dann definieren wir den *Orthogonalraum* $A^\perp$ von A durch $A^\perp := \{v \in V : \langle v, a\rangle = 0 \quad \forall a \in A\}$. Offensichtlich ist das ein Teilraum von V (auch wenn A selbst kein Teilraum ist).

Ein *Orthogonalsystem* in V ist eine Teilmenge $\{v_i : i \in I\} \subset V$, sodass $v_i \neq 0$ für alle $i \in I$ und $\langle v_i, v_j\rangle = 0$ für $i \neq j$ gilt. Gilt zusätzlich $\langle v_i, v_i\rangle = 1$ (also $\|v_i\| = 1$) für alle $i \in I$, dann spricht man von einem *Orthonormalsystem* in V. Eine *Orthonormalbasis* ist ein Orthonormalsystem in V, das eine Basis von V ist.

Proposition 9.6. *Sei $(V, \langle\ ,\ \rangle)$ ein Euklidischer oder unitärer Vektorraum und $\mathcal{B} = \{v_1, \dots, v_n\}$ eine Orthonormalbasis für V. Dann gilt:*

(1) Jedes Orthogonalsystem in V ist eine linear unabhängige Teilmenge.

(2) Für Skalare $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{K}$ gilt $\langle \sum x_j v_j, \sum y_k v_k\rangle = \sum_{j=1}^n x_j \bar{y}_j$.

(3) Für $x \in V$ ist die eindeutige Darstellung als Linearkombination der Elemente von $\mathcal{B}$ gegeben durch $x = \sum_{j=1}^n \langle x, v_j\rangle v_j$.

(4) Ist $(W, \langle\ ,\ \rangle_W)$ ein weiterer Vektorraum der gleichen Art, $\mathcal{C} = \{w_1, \dots, w_m\}$ eine Orthonormalbasis und $f : V \to W$ eine lineare Abbildung, dann ist die Matrixdarstellung $[f]^{\mathcal{B}}_{\mathcal{C}} = (a_{ij})$ gegeben durch $a_{ij} = \langle f(v_j), w_i\rangle_W$.

Beweis. (1) Sei $A \subset V$ ein Orthogonalsystem, $a_1, \dots, a_n \in A$ und $\lambda_1, \dots, \lambda_n \in \mathbb{K}$, sodass $\sum \lambda_j a_j = 0$ gilt. Dann gilt für jedes $k = 1, \dots, n$ die Gleichung

$$0 = \langle \textstyle\sum_j \lambda_j a_j, a_k\rangle = \sum_j \lambda_j \langle a_j, a_k\rangle = \lambda_k \langle a_k, a_k\rangle.$$

Nach Definition ist $a_k \neq 0$, also $\langle a_k, a_k\rangle \neq 0$. Damit muss aber $\lambda_k = 0$ für alle $k = 1, \dots, n$ gelten, also ist A linear unabhängig.

(2) Wegen der Sesquilinearität von $\langle\ ,\ \rangle$ ist

$$\langle \textstyle\sum_j x_j v_j, \sum_k y_k v_k\rangle = \sum_j x_j \langle v_j, \sum_k y_k v_k\rangle = \sum_{j,k} x_j \bar{y}_k \langle v_j, v_k\rangle,$$

und nach Definition ist $\langle v_j, v_k\rangle$ gleich Null für $j \neq k$ und gleich Eins für $j = k$.

(3) Da $\{v_1, \dots, v_n\}$ eine Basis für V ist, können wir den Vektor $x \in V$ eindeutig in der Form $x = \sum_{i=1}^n x_i v_i$ schreiben. Damit rechnen wir

$$\langle x, v_j\rangle = \langle \textstyle\sum_{i=1}^n x_i v_i, v_j\rangle = \sum_{i=1}^n x_i \langle v_i, v_j\rangle = x_j.$$

(4) Die j–te Spalte der Matrix $[f]^{\mathcal{B}}_{\mathcal{C}}$ ist der Koordinatenvektor $[f(v_j)]_{\mathcal{C}}$, siehe Proposition 4.15 von [**1**]. Nach Teil (3) ist aber $f(v_j) = \sum_i \langle f(v_j), w_i\rangle_W w_i$ und die Behauptung folgt. □

Ein zentrales Resultat über euklidische und unitäre Vektorräume ist nun, dass linear unabhängige Teilmengen eindeutig Orthonormalsysteme liefern. Der Beweis besteht in einer expliziten Prozedur, dem sogenannten *Gram–Schmidt Orthonormalisierungsverfahren.*

Satz 9.6. *Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum und sei $A := \{a_1, \dots, a_n\} \subset V$ linear unabhängig. Dann gibt es ein eindeutiges Orthonormalsystem $\{v_1, \dots, v_n\} \subset V$, das folgende Bedingung erfüllt: Für jedes $j = 1, \dots, k$ kann a_j als Linearkombination von $v_1, \dots, v_j$ geschrieben werden, wobei der Koeffizient von v_j reell und positiv ist.*

Beweis. Zunächst beweisen wir die Existenz durch eine induktive Konstruktion. Da A linear unabhängig ist, ist $a_1 \neq 0$, also $\|a_1\| \neq 0$, und wir setzen $v_1 := \frac{1}{\|a_1\|}a_1$. Dann ist $\langle v_1, v_1\rangle = \frac{1}{\|a_1\|^2}\langle a_1, a_1\rangle = 1$, also $\{v_1\}$ ein Orthonormalsystem, und $a_1 = \|a_1\|v_1$.

Nehmen wir induktiv an, dass $k \geq 2$ gilt, und wir $\{v_1, \dots, v_{k-1}\}$ bereits konstruiert haben. Setze nun $\tilde{v}_k := a_k - \sum_{j=1}^{k-1}\langle a_k, v_j\rangle v_j$. Für $\ell < k$ ist dann

$$\langle \tilde{v}_k, v_\ell\rangle = \langle a_k, v_\ell\rangle - \sum_{j=1}^{k-1}\langle a_k, v_j\rangle\langle v_j, v_\ell\rangle.$$

Nach Induktionsvoraussetzung ist $\{v_1, \dots, v_{k-1}\}$ ein Orthonormalsystem, also $\langle \tilde{v}_k, v_\ell\rangle = 0$ für alle $\ell < k$.

Wäre $\tilde{v}_k = 0$, dann könnte man a_k als Linearkombination von $v_1, \dots, v_{k-1}$ schreiben. Das diese $k-1$ Elemente ein Orthogonalsystem bilden, erzeugen sie nach Teil (3) der Proposition einen $k-1$–dimensionalen Teilraum, in dem a_k liegen würde. Aber ebenfalls nach Induktionsvoraussetzung liegt $\{a_1, \dots, a_{k-1}\}$ in diesem Teilraum und ist linear unabhängig, also eine Basis. Somit könnte man a_k als Linearkombination der a_j für $j < k$ schreiben, ein Widerspruch zur linearen Unabhängigkeit von A.

Somit ist $\tilde{v}_k \neq 0$, also können wir $v_k := \frac{1}{\|\tilde{v}_k\|}\tilde{v}_k$ setzen. Dann gilt natürlich immer noch $\langle v_k, v_j\rangle = 0$ für $j < k$ und außerdem $\langle v_k, v_k\rangle = 1$, also ist $\{v_1, \dots, v_k\}$ ein Orthonormalsystem. Außerdem ist wiederum nach Konstruktion $a_k = \|\tilde{v}_k\|v_k + \sum_{j=1}^{k-1}\langle a_k, v_j\rangle v_j$, also ist die letzte Bedingung verifiziert.

Zur Eindeutigkeit: Es muss $a_1 = av_1$ für $a \in \mathbb{R}$, $a > 0$ und $\|v_1\| = 1$ gelten. Daraus folgt aber $a = \|a_1\|$ und damit $v_1 = \frac{a_1}{\|a_1\|}$. Haben wir gezeigt, dass $v_1, \dots, v_{k-1}$ eindeutig bestimmt sind, dann muss nach Teil (2) der Proposition $a_k = \langle a_k, v_k\rangle v_k + \sum_{j=1}^{k-1}\langle a_k, v_j\rangle v_j$ und damit ist v_k bis auf Vielfache eindeutig bestimmt. Nun soll aber auch noch $\langle a_k, v_k\rangle$ reell und positiv sein, was v_k bis auf einen positiven reellen Faktor bestimmt, der durch $\|v_k\| = 1$ dann eindeutig festgelegt wird. □

Korollar 9.6. *Sei $(V, \langle\ ,\ \rangle)$ ein endlichdimensionaler euklidischer oder unitärer Vektorraum. Dann gilt:*

(1) V besitzt eine Orthonormalbasis.

(2) Jedes Orthonormalsystem in V kann zu einer Orthonormalbasis erweitert werden.

(3) Ist $W \subset V$ ein Teilraum mit Orthogonalraum $W^\perp$, dann ist $V = W \oplus W^\perp$.

Beweis. (1) Nach Korollar 4.4 von [**1**] besitzt V eine Basis $\mathcal{B} = \{a_1, \dots, a_n\}$. Wenden wir darauf das Orthonormalisierungsverfahren aus Satz 9.6 an, dann erhalten wir ein Orthonormalsystem $\{v_1, \dots, v_n\}$ mit $\dim(V)$ vielen Elementen. Nach Teil (1) von Proposition 9.6 ist das eine linear unabhängige Teilmenge in V, also eine Basis nach Korollar 4.5 von [**1**].

(2) Ist A ein Orthonormalsystem in V, dann ist A nach Teil (1) von Proposition 9.6 linear unabhängig, kann also nach Korollar 4.5 von [**1**] zu einer Basis von V erweitert werden. Wendet man auf diese Basis das Orthonormalisierungsverfahren an, dann passiert in den ersten Schritten (bei den Elementen von A) nichts, also erhält man ein Orthonormalsystem mit $\dim(V)$ Elementen, das A enthält, und dieses muss wie zuvor eine Orthonormalbasis für V sein.

(3) Wählt man eine Basis von W und orthonormalisiert diese, dann erhält man eine Orthonormalbasis $\{w_1, \dots, w_k\}$ für W. Nach (2) kann man diese zu einer Orthonormalbasis für V erweitern. Seien $v_1, \dots, v_\ell$ die hinzugekommenen Elemente. Für

$i = 1, \dots, \ell$ ist nach Konstruktion ist $\langle v_i, w_j\rangle = 0$ für alle $j = 1, \dots, k$. Da jedes $w \in W$ als Linearkombination der w_j geschrieben werden kann, folgt $\langle v_i, w\rangle = 0$ für alle $w \in W$, also $v_i \in W^\perp$ für $i = 1, \dots, \ell$. Weiters ist $W \cap W^\perp = \{0\}$, weil für $w \in W \cap W^\perp$ insbesondere $\langle w, w\rangle = 0$ gelten muss. Nach der Dimensionsformel für Summen ist $\dim(W^\perp) \leq \dim(V) - \dim(W) = \ell$, also muss Gleichheit gelten. Damit folgt $V = W \oplus W^\perp$ aus Proposition 4.9 von [**1**]. □

Bemerkung 9.6. (1) Nach dem Korollar kann man in einem endlichdimensionalen euklidischen oder unitären Vektorraum immer in Orthonormalbasen arbeiten. In einer Orthonormalbasis sieht aber das innere Produkt auf V nach Teil (3) von Proposition 9.6 genau so aus wie das Standard innere Produkt auf $\mathbb{K}^n = \mathbb{R}^n$ bzw. $\mathbb{C}^n$. Man kann das auch so ausdrücken, dass der lineare Isomorphismus $V \to \mathbb{K}^n$, $v \mapsto [v]_{\mathcal{B}}$, der durch eine Orthonormalbasis induziert wird, verträglich mit den inneren Produkten ist. (Wir werden solche lineare Isomorphismen später "orthogonal" bzw. "unitär" nennen.) Man kann also die Untersuchung von euklidischen (unitären) Vektorräumen immer auf $\mathbb{R}^n$ ($\mathbb{C}^n$) mit den Standard inneren Produkten zurückführen. Für unendlichdimensionale Hilberträume gelten ähnliche Resultate, hier gibt es bis auf Isomorphie auch jeweils nur einen Hilbertraum für jede Kardinalzahl.

(2) Unsere Resultate liefern uns auch eine schöne geometrische Interpretation des inneren Produktes in einem euklidischen Vektorraum. Sind nämlich $v, w \in V$ linear unabhängig, dann erzeugen die beiden Vektoren eine Ebene, und wir können (etwa durch Orthonormalisieren von $\{v, w\}$) einen Vektor $\tilde{v} \neq 0$ in dieser Ebene finden der orthogonal auf v steht. Dann können wir aber w eindeutig als $av + b\tilde{v}$ für $a, b \in \mathbb{R}$ schreiben, und av kann als die Projektion von w auf v interpretiert werden. Nach Teil (2) von Proposition 9.6 ist aber $a = \frac{\langle v,w\rangle}{\langle v,v\rangle}$ und damit ist $|\langle v, w\rangle| = |a| \cdot \|v\|^2 = \|av\| \cdot \|v\|$, und wir können den Betrag des inneren Produktes als das Produkt der Länge von v und der Länge der Projektion von w auf v interpretieren.

(3) Der letzte Teil des Korollars sagt, dass für jeden Teilraum $W \subset V$ der Orthogonalraum $W^\perp$ ein Komplement zu W ist. Deshalb bezeichnet man $W^\perp$ oft auch als das *orthogonale Komplement* von W.

(4) Da man in einem euklidischen bzw. unitären Vektorraum zu jedem Teilraum W automatische ein Komplement (nämlich $W^\perp$) erhält, gibt es natürlich auch die zugehörigen Projektionen, π_W und $\pi_{W^\perp}$, siehe 8.4. Die Projektion π_W heißt die *Orthogonalprojektion* auf W. Wir werden in Kürze eine geometrische Charakterisierung dieser Projektion besprechen.

(5) Mit kleinen Änderungen machen die Konzepte dieses Abschnitts auch allgemeiner für eine nicht entartete symmetrische Bilinearform bzw. Sesquilinearform $b : V \times V \to \mathbb{K}$ Sinn. Man muss dann nur Orthogonalsysteme durch $b(v_i, v_j) = 0$ und $b(v_i, v_i) \neq 0$ definieren und für ein Orthonormalsystem zusätzlich $b(v_i, v_i) = \pm 1$ verlangen. Dann gelten auch fast alle Resultate dieses Abschnitts mit kleinen Modifikationen weiter. Der wesentliche Unterschied ist, dass für allgemeine Teilräume $W \subset V$ nicht mehr $W \cap W^\perp = \{0\}$ gilt. Es gilt aber immer $\dim(W^\perp) = \dim(V) - \dim(W)$, also ist in diesen Fällen $W + W^\perp$ ein echter Teilraum von V. Der Unterschied stammt daher, dass die Einschränkung einer nicht degenerierten symmetrischen Bilinearform auf einen Teilraum degeneriert sein kann. Damit gibt es für allgemeine Teilräume keine Orthonormalbasen mehr.

9.7. Der Winkel. Wie schon angekündigt kann man in euklidischen Vektorräumen den Winkel zwischen zwei Vektoren definieren. Grundlage dafür ist die Cauchy–Schwarz

Ungleichung: Für einen euklidischen Raum V und $v, w \in V$ mit $v, w \neq 0$ impliziert diese, dass $-\|v\| \cdot \|w\| \leq \langle v, w \rangle \leq \|v\| \cdot \|w\|$ gilt. Somit ist $\frac{\langle v,w \rangle}{\|v\| \cdot \|w\|}$ eine reelle Zahl die zwischen 1 und -1 liegt. Weiters wissen wir, dass diese Zahl nur dann 1 (bzw. -1) sein kann, wenn w ein positives (bzw. negatives) Vielfaches von v ist, sowie dass sie genau dann gleich Null ist, wenn $v \perp w$ gilt. Wie aus der Analysis bekannt ist, gibt es einen eindeutigen Winkel $\alpha \in [0, \pi]$, sodass $\frac{\langle v,w \rangle}{\|v\| \cdot \|w\|} = \cos(\alpha)$ gilt, und wir definieren dieses α als den Winkel zwischen den Vektoren v und w.

Diese Definition entspricht genau der intuitiven Vorstellung des Winkels, und stimmt in $\mathbb{R}^n$ mit dem Standard inneren Produkt mit dem üblichen Begriff des Winkels überein. Insbesondere ist der Winkel zwischen v und w genau dann 0, wenn w ein positives Vielfaches von v ist, er ist genau dann gleich π, wenn w ein negatives Vielfaches von v ist, und er ist genau dann $\frac{\pi}{2}$, wenn $v \perp w$ gilt.

Die Definition des Winkels α zwischen zwei Vektoren $v, w \in V$ mit $v, w \neq 0$ kann man nun auch als $\langle v, w \rangle = \|v\| \cdot \|w\| \cdot \cos(\alpha)$ schreiben. Die Gleichung

$$\langle v + w, v + w \rangle = \langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle$$

liefert nun den *Cosinussatz* $\|v + w\|^2 = \|v\|^2 + \|w\|^2 + 2\cos(\alpha)\|v\| \cdot \|w\|$ der euklidischen Geometrie. Für $v \perp w$ erhalten wir insbesondere den *Satz von Pythagoras* $\|v+w\|^2 = \|v\|^2 + \|w\|^2$, der natürlich (mit genau dem selben Beweis) auch in unitären Vektorräumen gilt.

Der Satz von Pythagoras liefert auch die angekündigte geometrische Interpretation der Orthogonalprojektion $\pi = \pi_W$ auf einen Teilraum W eines euklidischen oder unitären Vektorraumes V. Sei nämlich $v \in V$ und betrachte $\pi(v) \in W$, sowie ein beliebiges weiteres Element $w \in W$. Wegen $w - v = (w - \pi(v)) + (\pi(v) - v)$ erhalten wir für das Quadrat der Distanz von v nach w, die Formel

$$\|w - v\|^2 = \|(w - \pi(v)) + (\pi(v) - v)\|^2 = \|w - \pi(v)\|^2 + \|\pi(v) - v\|^2,$$

wobei wir benutzt haben, dass $\pi(v) - v = \pi_{W^\perp}(v) \in W^\perp$, und $w - \pi(v) \in W$ gilt, und wir damit den Satz von Pythagoras anwenden können. Da $\|w - \pi(v)\|^2 \geq 0$ gilt und Gleichheit nur für $w = \pi(v)$ vorkommen kann, sehen wir, dass es einen eindeutigen Punkt in W gibt, der minimalen Abstand zu v hat, nämlich $\pi(v)$.

Dualraum und adjungierte Abbildung

Als nächsten Schritt zeigen wir, dass ein inneres Produkt auf einem Vektorraum V eine Identifikation von V mit seinem Dualraum liefert. Damit kann man für lineare Abbildungen $f : V \to V$ die duale Abbildung ebenfalls als Abbildung von V nach V betrachten, die in diesem Bild die adjungierte Abbildung zu f heißt. Wir werden dieses Konzept aber ohne die Benutzung von Resultaten über Dualräume herleiten.

9.8. Identifikation mit dem Dualraum. Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum. Nach Definition ist für jeden Vektor $v \in V$ die Zuordnung $w \mapsto \langle w, v \rangle$ eine lineare Abbildung $\varphi_v : V \to \mathbb{K}$, also ein Element des Dualraumes $V^* = L(V, \mathbb{K})$ von V.

Proposition 9.8. *Sei $(V, \langle\ ,\ \rangle)$ ein (endlichdimensionaler) euklidischer bzw. unitärer Vektorraum über $\mathbb{K} = \mathbb{R}$ bzw. $\mathbb{C}$ und $\varphi : V \to \mathbb{K}$ ein lineares Funktional. Dann gibt es ein eindeutiges Element $v_0 \in V$, sodass $\varphi(v) = \langle v, v_0 \rangle$ für alle $v \in V$ gilt.*

Beweis. Betrachte zunächst den Fall eines euklidischen Vektorraumes. Für $v \in V$ setze $\varphi_v : V \to \mathbb{R}$, $\varphi_v(w) = \langle w, v\rangle$ und betrachte $v \mapsto \varphi_v$ als Funktion $V \to L(V, \mathbb{R})$. Nach Definition gilt für $v_1, v_2 \in V$, $r \in \mathbb{R}$ und alle $w \in V$

$$\varphi_{v_1+rv_2}(w) = \langle w, v_1 + rv_2\rangle = \langle w, v_1\rangle + r\langle w, v_2\rangle = \varphi_{v_1}(w) + r\varphi_{v_2}(w) = (\varphi_{v_1} + r\varphi_{v_2})(w).$$

Damit ist aber $\varphi_{v_1+rv_2} = \varphi_{v_1} + r\varphi_{v_2}$, also ist $v \mapsto \varphi_v$ eine lineare Abbildung zwischen den $\mathbb{R}$–Vektorräumen V und $L(V, \mathbb{R})$. Außerdem gilt $\varphi_v = 0$ genau dann, wenn $0 = \varphi_v(w) = \langle w, v\rangle$ für alle $w \in V$ gilt, und das gilt nur für $v = 0$. Damit ist $v \mapsto \varphi_v$ injektiv und da $\dim(V) = \dim(L(V, \mathbb{R}))$ ist ist die Abbildung sogar bijektiv und die Behauptung folgt.

Im Fall unitärer Vektorräume ist die resultierende Abbildung $V \to L(V, \mathbb{C})$ nicht linear sondern konjugiert linear, die Argumentationsweise funktioniert aber auch für solche Abbildungen. □

Identifiziert man in dieser Weise den Vektorraum V mit seinem Dualraum V^*, dann können wir zu einer Teilmenge $A \subset V$ den Annihilator A° (siehe Abschnitt 5.4 von [**1**]) bilden, und diesen als Teilraum von V betrachten. Nach Definition liegt ein Element $v \in V$ genau dann in diesem Teilraum, wenn $0 = \varphi_v(a) = \langle a, v\rangle$ für alle $a \in A$ gilt, man erhält also genau den Orthogonalraum $A^\perp$ aus 9.6. Damit kann man alle Resultate über Annihilatoren aus 5.4 von [**1**] auf Orthogonalräume übertragen. Man kann die entsprechenden Aussagen aber auch leicht direkt beweisen:

Satz 9.8. *Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer oder unitärer Vektorraum, $A, A' \subset V$ Teilmengen und $W, W' \subset V$ Teilräume. Dann gilt:*
(1) $A \subset A' \implies (A')^\perp \subset A^\perp$.
(2) $\dim(W^\perp) = \dim(V) - \dim(W)$.
(3) $(A^\perp)^\perp$ *ist der von A erzeugte Teilraum von V. Insbesondere ist* $(W^\perp)^\perp = W$.
(4) $(W + W')^\perp = W^\perp \cap (W')^\perp$.
(5) $(W \cap W')^\perp = W^\perp + (W')^\perp$.

Beweis. (1) ist offensichtlich und (2) haben wir schon in 9.6 bewiesen. Für (3) bemerken wir zunächst, dass $(A^\perp)^\perp$ ein Teilraum von V ist, der A enthält, weil für $a \in A$ und $v \in A^\perp$ natürlich $\langle a, v\rangle = 0$ gilt. Ist W der von A erzeugte Teilraum, dann kann jedes Element von W als Linearkombination von Elementen von A geschrieben werden. Damit folgt aber, dass jedes Element $v \in A^\perp$ auch schon in $W^\perp$ liegt, und mittels (1) erhalten wir $A^\perp = W^\perp$ und damit $(A^\perp)^\perp = (W^\perp)^\perp$. Von vorher wissen wir, dass $W \subset (W^\perp)^\perp$ gilt und nach (2) haben die beiden Teilräume gleiche Dimension, also folgt $W = (W^\perp)^\perp$.

(4) Da $W \subset W + W'$ gilt, folgt $(W + W')^\perp \subset W^\perp$ nach (1). Analog gilt das für W' und damit folgt $(W + W')^\perp \subset W^\perp \cap (W')^\perp$. Liegt umgekehrt ein Vektor $v \in V$ sowohl in $W^\perp$ als auch in $(W')^\perp$, dann liegt v offensichtlich in $(W \cup W')^\perp$ und von oben wissen wir, dass das mit $(W + W')^\perp$ übereinstimmt.

(5) Nach (4) und (3) wissen wir, dass $(W^\perp + (W')^\perp)^\perp = W \cap W'$ gilt. Daraus folgt die Behauptung, indem man auf beiden Seiten den Orthogonalraum bildet. □

9.9. Anwendungen. Wie wollen hier zwei geometrische Anwendungen der Identifikation von V mit V^* durch ein inneres Produkt geben, nämlich einerseits die Hessesche Normalform für affine Hyperebenen und andererseits die Konstruktion des Normalvektors in $\mathbb{R}^2$ und des Kreuzprodukts in $\mathbb{R}^3$.

(1) Betrachte $\mathbb{R}^n$ mit dem Standard inneren Produkt $\langle\ ,\ \rangle$. Ist $x \in \mathbb{R}^n$ mit $x \neq 0$ beliebig, dann der von x erzeugt Teilraum gerade $\mathbb{R}x = \{\lambda x : \lambda \in \mathbb{R}\}$ und nach Teil

(2) des Satzes ist das orthogonale Komplement $\{x\}^\perp = \{y \in \mathbb{R}^n : \langle y, x\rangle = 0\}$ ein Teilraum der Dimension $n-1$, eine sogenannte Hyperebene. Ist umgekehrt $W \subset \mathbb{R}^n$ eine Hyperebene, dann ist $W^\perp$ ein eindimensionaler Teilraum von V und ist x ein Element darin, das ungleich Null ist, dann ist $W = \{x\}^\perp$. Man bemerke, dass das Element x bis auf Vielfache (ungleich Null) eindeutig bestimmt ist. Nimmt man zusätzlich $\|x\| = 1$ an, dann ist x bis auf das Vorzeichen eindeutig bestimmt. Man kann also jede Hyperebene in der Form $\{x\}^\perp$ darstellen. Insbesondere ist in $\mathbb{R}^2$ jede Gerade durch Null und in $\mathbb{R}^3$ jede Ebene durch Null von dieser Form.

Betrachten wir nun eine verschobene Kopie eine Hyperebene (eine *“affine Hyperebene”*) $A \subset \mathbb{R}^n$. Dann gibt es einen Punkt $y \in A$ und eine Hyperebene $W \subset \mathbb{R}^n$, sodass $A = y + W = \{y + w : w \in W\}$ gilt. Ist $x \in W^\perp$ mit $\|x\| = 1$, dann ist $\langle x, w\rangle = 0$, also $\langle x, y + w\rangle = \langle x, y\rangle$ für alle $w \in W$. Damit gilt $\langle x, a\rangle = \langle x, y\rangle$ für alle $a \in A$. Ist umgekehrt $z \in \mathbb{R}^n$ so, dass $\langle x, z\rangle = \langle x, y\rangle$ gilt, dann ist $\langle x, z - y\rangle = 0$, also $z - y \in W$ und damit $z \in A$. Das bedeutet aber gerade, dass man A als $\{v \in \mathbb{R}^n : \langle x, v\rangle = d\}$ für einen Einheitsnormalvektor $x \in \mathbb{R}^n$ zu W ein geeignetes $d \in \mathbb{R}$ beschreiben kann.

Wir können aber auch dieses d leicht beschreiben: Nach Teil (3) von Korollar 9.6 ist $\mathbb{R}^n = W \oplus W^\perp$, also kann man jedes Element $a \in A$ eindeutig als $w + \lambda x$ für $w \in W$ und $\lambda \in \mathbb{R}$ schreiben. Da $a + w \in A$ für alle $a \in A$ und $w \in W$ gilt hat $A \cap W^\perp$ genau ein Element, also gibt es ein eindeutiges $\lambda \in \mathbb{R}$, sodass $\lambda x \in A$ gilt, und wegen $\|x\| = 1$ erhalten wir sofort $\lambda = d$. Wählen wir x so, dass $d \geq 0$ gilt, dann ist d genau der *Normalabstand* der affinen Hyperebene A vom Nullpunkt.

(2) Betrachten wir wieder $\mathbb{R}^n$ mit dem Standard inneren Produkt $\langle\ ,\ \rangle$ und sei $\det : (\mathbb{R}^n)^n \to \mathbb{R}$ die Determinante. Fixieren wir beliebige Vektoren $v_1, \dots, v_{n-1} \in \mathbb{R}^n$, dann ist $y \mapsto \det(v_1, \dots, v_{n-1}, y)$ eine lineare Abbildung, also gibt es einen eindeutigen Vektor $x \in \mathbb{R}^n$, sodass $\langle x, y\rangle = \det(v_1, \dots, v_{n-1}, y)$ für alle $y \in \mathbb{R}^n$ gilt.

Im Fall $n = 2$ bedeutet das, dass wir für einen fix gewählten Vektor $v \in \mathbb{R}^2$ einen eindeutigen Vektor $x \in \mathbb{R}^2$ finden, der $\langle x, y\rangle = \det(v, y)$ für alle $y \in \mathbb{R}^n$ erfüllt. Insbesondere ist $\langle x, v\rangle = \det(v, v) = 0$, also x ein Normalvektor zu v. Ist $v = (v_1, v_2)$ und $x = (x_1, x_2)$, dann ist $x_1 = \langle x, e_1\rangle = \det(v, e_1) = -v_2$ und $x_2 = \langle x, e_2\rangle = \det(v, e_2) = v_1$, also ist $x = (-v_2, v_1)$. Insbesondere ist $\|x\| = \|v\|$. Nun ist $|\langle x, y\rangle|$ das Produkt der Länge der von x mit der Länge der Projektion von y auf x. Da $x \perp v$ gilt, ist die Länge dieser Projektion genau die Höhe des von y und v aufgespannten Parallelogramms, also ist $|\det(v, y)| = |\langle x, y\rangle|$ genau die Fläche des von v und y aufgespannten Parallelogramms. Man zeigt leicht (siehe Übungen), dass $|\det(v, y)| = \|v\| \cdot \|y\| \sin(\alpha)$ gilt, wobei α der Winkel zwischen v und y ist.

Im Fall $n = 3$ erhalten wir zu zwei Vektoren $v, w \in \mathbb{R}^3$ einen eindeutigen Vektor $v \times w \in \mathbb{R}^3$, der $\langle v \times w, y\rangle = \det(v, w, y)$ für alle $y \in \mathbb{R}^3$ erfüllt. Das definiert also ein Produkt $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, das sogenannte Kreuzprodukt. Aus der Linearität der Determinante in jeder Eintragung folgt sofort, dass $(v + \lambda v') \times w = v \times w + \lambda(v' \times w)$ und $v \times (w + \lambda w') = v \times w + \lambda(v' \times w)$ gelten. Da die Determinante alternierend ist, erhalten wir $w \times v = -v \times w$ und $\langle v \times w, v\rangle = \langle v \times w, w\rangle = 0$.

Sind v und w linear abhängig, dann ist $\det(v, w, x) = 0$ für alle x, also $v \times w = 0$. Ist andererseits $\{v, w\}$ linear unabhängig, dann finden wir ein $y \in \mathbb{R}^3$, sodass $\{v, w, y\}$ eine Basis, und damit $\det(v, w, y) = \langle v \times w, y\rangle \neq 0$ gilt. Somit gilt $v \times w = 0$ genau dann, wenn v und w linear abhängig sind.

Schließlich ist nach Konstruktion $\det(v, w, v \times w) = \|v \times w\|^2$. Ist also $\{v, w\}$ linear unabhängig, dann ist $\{v, w, v \times w\}$ eine Basis für $\mathbb{R}^3$. Eine explizite Formel für $v \times w$ erhält man, indem man benutzt, dass die i–te Komponente von $v \times w$ gerade als $\langle v \times w, e_i\rangle = \det(v, w, e_i)$ berechnet werden kann. Entwickelt man diese Determinante jeweils nach der letzten Spalte, dann erhält man

$$(v_1, v_2, v_3) \times (w_1, w_2, w_3) = (v_2w_3 - v_3w_2, -v_1w_3 + v_3w_1, v_1w_2 - v_2w_1).$$

Aus dieser Formel verifiziert man direkt, dass $\|v \times w\|^2 = \|v\|^2 \cdot \|w\|^2 - \langle v, w\rangle^2$ gilt. Sind v und w linear unabhängig, dann wählen wir wie in Bemerkung (2) von 9.6 einen Vektor $\tilde{v} \neq 0$ in der von v und w erzeugten Ebene mit $\langle v, \tilde{v}\rangle = 0$, und schrieben $w = av + b\tilde{v}$. Dann wissen wir, dass $\langle v, w\rangle^2 = \|v\|^2 \cdot \|av\|^2$ gilt, also erhalten wir $\|v \times w\|^2 = \|v^2\|(\|w\|^2 - \|av\|^2)$. Nach dem Satz von Pythagoras liefert die Klammer $\|b\tilde{v}\|^2$, also erhalten wir $\|v \times w\| = \|v\| \cdot \|b\tilde{v}\|$, und das kann man offensichtlich als die Fläche des von v und w aufgespannten Parallelogramms interpretieren. Nun ist $|\langle v \times w, y\rangle|$ gerade das Produkt der Länge von $v \times w$ mit der Länge der Projektion von y auf $v \times w$. Da $v \times w$ normal auf die von v und w erzeugte Ebene steht, ist die Länge dieser Projektion genau die Höhe des von v, w und y erzeugten Parallelepipeds. Somit sehen wir, dass $|\det(v, w, y)| = |\langle v \times w, y\rangle|$ genau das Volumen des von v, w und y erzeugten Parallelepipeds ist.

9.10. Die adjungierte Abbildung. Wir kommen jetzt zu der Interpretation der dualen Abbildung, die durch die Identifikation eines euklidischen oder unitären Vektorraumes mit seinem Dualraum ermöglicht wird. Wir werden allerdings wieder nicht auf Resultate über duale Abbildungen aufbauen, sondern direkte Beweise geben. Für ein tieferes Verständnis ist aber sehr hilfreich, sich die Zusammenhänge bewusst zu machen.

SATZ 9.10. *Seien $(V, \langle\ ,\ \rangle_V)$, $(W, \langle\ ,\ \rangle_W)$ und $(Z, \langle\ ,\ \rangle_Z)$ endlichdimensionale euklidische bzw. unitäre Vektorräume über $\mathbb{K} = \mathbb{R}$ bzw. $\mathbb{C}$. Dann gilt:*

(1) Zu einer linearen Abbildung $f : V \to W$ gibt es eine eindeutige lineare Abbildung $f^* : W \to V$, sodass $\langle f(v), w\rangle_W = \langle v, f^*(w)\rangle_V$ für alle $v \in V$ und $w \in W$ gilt.

(2) Die adjungierte Abbildung $(f^*)^* : V \to W$ zu $f^* : W \to V$ ist durch $(f^*)^* = f$ gegeben.

(3) $\operatorname{Ker}(f^*) = \operatorname{Im}(f)^\perp \subset W$ *und* $\operatorname{Im}(f^*) = \operatorname{Ker}(f)^\perp \subset V$.

(4) Sind $\mathcal{B} \subset V$ und $\mathcal{C} \subset W$ Orthonormalbasen, und ist $[f]^{\mathcal{B}}_{\mathcal{C}} = (a_{ij})$ die Matrixdarstellung von f bezüglich dieser Basen, dann ist die Matrixdarstellung $[f^*]^{\mathcal{C}}_{\mathcal{B}} = (b_{ij})$ charakterisiert durch $b_{ij} = \bar{a}_{ji}$.

(5) Ist $\tilde{f} : V \to W$ eine weitere lineare Abbildung und $\lambda \in \mathbb{K}$, dann gilt $(f + \lambda\tilde{f})^* = f^* + \bar{\lambda}\tilde{f}^*$.

(6) Ist $g : W \to Z$ eine weitere lineare Abbildung, dann ist $(g \circ f)^* = f^* \circ g^*$.

BEWEIS. (1) Fixieren wir zunächst ein Element $w_0 \in W$ und betrachten die Funktion $V \to \mathbb{K}$, die durch $\langle f(v), w_0\rangle_W$ gegeben ist. Aus der Linearität von f folgt sofort, dass auch diese Abbildung linear ist. Somit gibt es nach Proposition 9.8 ein eindeutig bestimmtes Element in V, dass wir mit $f^*(w_0)$ bezeichnen, sodass $\langle f(v), w_0\rangle_W = \langle v, f^*(w_0)\rangle_V$. Damit haben wir eine Vorschrift gefunden, die jedem Vektor $w \in W$ einen Vektor $f^*(w) \in V$ zuordnet, sodass die gewünschte Gleichung gilt, und damit eine Funktion $f^* : W \to V$ definiert.

Es bleibt also nur noch zu zeigen, dass f^* linear ist: Seien dazu $w_1, w_2 \in W$ und $\lambda \in \mathbb{K}$. Dann rechnen wir für beliebiges $v \in V$

$$\begin{aligned}\langle v, f^*(w_1) + \lambda f^*(w_2)\rangle_V &= \langle v, f^*(w_1)\rangle_V + \bar{\lambda}\langle v, f^*(w_2)\rangle_V \\ &= \langle f(v), w_1\rangle_W + \bar{\lambda}\langle f(v), w_2\rangle_W = \langle f(v), w_1 + \lambda w_2\rangle_W = \langle v, f^*(w_1 + \lambda w_2)\rangle_V,\end{aligned}$$

und da $\langle\ ,\ \rangle_V$ nicht entartet ist, folgt $f^*(w_1 + \lambda w_2) = f^*(w_1) + \lambda f^*(w_2)$.

(2) Für $v \in V$ und $w \in W$ rechnen wir einfach

$$\langle w, f(v)\rangle_W = \overline{\langle f(v), w\rangle_W} = \overline{\langle v, f^*(w)\rangle_W} = \langle f^*(w), v\rangle_W = \langle w, (f^*)^*(v)\rangle_W.$$

Da das für alle $w \in W$ gilt, folgt $f(v) = (f^*)^*(v)$ für alle $v \in V$, also $f = (f^*)^*$.

(3) Da $\langle\ ,\ \rangle_V$ nicht entartet ist, ist $f^*(w) = 0$ äquivalent zu $0 = \langle v, f^*(w)\rangle_V = \langle f(v), w\rangle_V$ für alle $v \in V$, also zu $w \in \operatorname{Im}(f)^\perp$.

Ist andererseits $v \in \operatorname{Ker}(f)$, dann gilt $0 = \langle f(v), w\rangle_W = \langle v, f^*(w)\rangle_V$, also gilt $f^*(w) \in \operatorname{Ker}(f)^\perp$. Das gilt aber für alle $w \in W$, also folgt $\operatorname{Im}(f^*) \subset \operatorname{Ker}(f)^\perp$. Nach Satz 9.8 ist $\dim(\operatorname{Ker}(f)^\perp) = \dim(V) - \dim(\operatorname{Ker}(f)) = \dim(\operatorname{Im}(f))$. Nach dem Dimensionssatz für lineare Abbildungen ist $\dim(\operatorname{Im}(f^*)) = \dim(W) - \dim(\operatorname{Ker}(f^*)) = \dim(W) - \dim(\operatorname{Im}(f)^\perp) = \dim(\operatorname{Im}(f))$. Damit hat der Teilraum $\operatorname{Im}(f^*) \subset \operatorname{Ker}(f)^\perp$ die gleiche Dimension wie der ganze Raum, also folgt Gleichheit.

(4) Ist $\mathcal{B} = \{v_1, \dots, v_n\}$ und $\mathcal{C} = \{w_1, \dots, w_m\}$, dann wissen wir aus Proposition 9.6, dass $a_{ij} = \langle f(v_j), w_i\rangle_W$ gilt. Analog ist

$$b_{ij} = \langle f^*(w_j), v_i\rangle_V = \overline{\langle v_i, f^*(w_j)\rangle_V} = \overline{\langle f(v_i), w_j\rangle_V} = \bar{a}_{ji}.$$

(5) Für beliebige Elemente $v \in V$ und $w \in W$ rechnen wir

$$\begin{aligned}\langle v, f^*(w) + \bar{\lambda}\tilde{f}^*(w)\rangle_V &= \langle v, f^*(w)\rangle_V + \lambda\langle v, \tilde{f}^*(w)\rangle_V \\ &= \langle f(v), w\rangle_W + \langle\lambda\tilde{f}(v), w\rangle_W = \langle(f + \lambda\tilde{f})(v), w\rangle_W = \langle v, (f + \lambda\tilde{f})^*(w)\rangle_V,\end{aligned}$$

und die Behauptung folgt analog wie in (2).

(6) Für $v \in V$ und $z \in Z$ rechnen wir

$$\begin{aligned}\langle v, f^*(g^*(z))\rangle_V &= \langle f(v), g^*(z)\rangle_W = \langle g(f(v)), z\rangle_Z \\ &= \langle(g \circ f)(v), z\rangle_Z = \langle v, (g \circ f)^*(z)\rangle_V,\end{aligned}$$

und die Behauptung folgt wie in (2). □

Definition 9.10. (1) Für eine lineare Abbildung $f : V \to W$ zwischen zwei euklidischen bzw. unitären Vektorräumen heißt die lineare Abbildung $f^* : W \to V$ aus Teil (1) des Satzes die *zu f adjungierte Abbildung.*

(2) Für eine Matrix $A = (a_{ij}) \in M_n(\mathbb{C})$ nennt man die Matrix $(b_{ij}) \in M_n(\mathbb{C})$ die gegeben ist durch $b_{ij} = \overline{a_{ji}}$ die *adjungierte Matrix* zu A und bezeichnet sie mit A^*.

Bemerkung 9.10. (1) Im Fall euklidischer Vektorräume erhält man in Teil (4) des Satzes als Matrixdarstellung für f^* einfach die Transponierte der Matrixdarstellung von f, siehe Abschnitt 5.3 von [**1**]. Deshalb spricht man in diesem Fall oft auch von der *Transponierten* der linearen Abbildung f und schreibt dafür auch f^t statt f^*. Die Tatsache, dass im Komplexen nicht einfach die transponierte Matrix auftritt hängt damit zusammen, dass die Identifikation mit dem Dualraum in diesem Fall konjugiert linear ist.

(2) Man kann die Ergebnisse des Satzes natürlich insbesondere auf Abbildungen $f : V \to V$ von einem euklidischen oder unitären Vektorraum auf sich selbst anwenden. In diesem Fall ist dann auch f^* eine lineare Abbildung von V auf sich selbst. Wählt man eine Orthonormalbasis $\mathcal{B}$ für V und setzt $A = [f]_\mathcal{B}$, dann gilt $[f^*]_\mathcal{B} = A^*$ (im komplexen Fall) bzw. $[f^*]_\mathcal{B} = A^t$ im reellen Fall.

Betrachtet man insbesondere den Fall $V = \mathbb{K}^n$ für $\mathbb{K} = \mathbb{R}$ bzw. $\mathbb{C}$, dann ist die Standardbasis $\{e_1, \dots, e_n\}$ orthonormal bezüglich des Standard inneren Produkts. Damit ist die Adjungierte Abbildung zu $x \mapsto Ax$ (bezüglich des Standard inneren Produkts) einfach durch $x \mapsto A^*x$ bzw. $x \mapsto A^tx$ gegeben.

Orthogonale und unitäre Abbildungen

Als letztes Thema der Vorlesung behandeln wir spezielle Klassen von linearen Abbildungen auf euklidischen und unitären Vektorräumen. Wir beginnen mit dem offensichtlichen Verträglichkeitsbegriff zwischen einer linearen Abbildung und einem inneren Produkt. Das liefert auch den richtigen Isomorphiebegriff für euklidische und unitäre Vektorräume.

9.11. Definitionen und grundlegende Eigenschaften. Der Begriff der orthogonalen bzw. unitären Abbildung ist ganz naheliegend:

Definition 9.11. Seien $(V, \langle\ ,\ \rangle_V)$ und $(W, \langle\ ,\ \rangle_W)$ zwei euklidische (bzw. unitäre) Vektorräume.

(1) Eine lineare Abbildung $f : V \to W$ heißt *orthogonal* (bzw. *unitär*), wenn $\langle f(v_1), f(v_2)\rangle_W = \langle v_1, v_2\rangle_V$ für alle $v_1, v_2 \in V$ gilt.

(2) $f : V \to W$ heißt ein *euklidischer (bzw. unitärer) Isomorphismus*, falls f orthogonal (bzw. unitär) ist, und es eine orthogonale (bzw. unitäre) lineare Abbildung $g : W \to V$ gibt, sodass $g \circ f = \mathrm{id}_V$ und $f \circ g = \mathrm{id}_W$ gilt.

(3) Eine Matrix $A \in M_n(\mathbb{R})$ heißt *orthogonal*, wenn die lineare Abbildung $\mathbb{R}^n \to \mathbb{R}^n$, $x \mapsto Ax$ orthogonal bezüglich des Standard inneren Produktes ist.

(4) Eine Matrix $A \in M_n(\mathbb{C})$ heißt *unitär*, wenn die lineare Abbildung $\mathbb{C}^n \to \mathbb{C}^n$, $z \mapsto Az$ unitär bezüglich des Standard hermitischen inneren Produktes ist.

Eine invertierbare euklidische (unitäre) lineare Abbildung $f : V \to W$ ist automatisch ein euklidischer (unitärer) Isomorphismus. Ist nämlich $f^{-1} : W \to V$ die inverse lineare Abbildung zu f, dann gilt

$$\langle f^{-1}(w_1), f^{-1}(w_2)\rangle_V = \langle f(f^{-1}(w_1)), f(f^{-1}(w_2))\rangle_W = \langle w_1, w_2\rangle_W.$$

Allgemein können wir orthogonale (unitäre) lineare Abbildungen wie folgt charakterisieren:

Satz 9.11. *Seien $(V, \langle\ ,\ \rangle_V)$ und $(W, \langle\ ,\ \rangle_W)$ zwei endlichdimensionale euklidische (bzw. unitäre) Vektorräume. Dann sind für eine lineare Abbildung $f : V \to W$ mit adjungierter Abbildung $f^* : W \to V$ äquivalent:*

(1) f ist orthogonal (unitär).

(2) $\|f(v)\| = \|v\|$ für alle $v \in V$.

(3) Es gibt eine Orthonormalbasis $\{v_1, \dots, v_n\}$ für V, sodass $\{f(v_1), \dots, f(v_n)\} \subset W$ ein Orthonormalsystem ist.

(4) Für jedes Orthonormalsystem $\{v_1, \dots, v_k\} \subset V$ ist $\{f(v_1), \dots, f(v_k)\} \subset W$ ein Orthonormalsystem.

(5) $f^* \circ f = \mathrm{id}_V$.

Beweis. (1) $\implies$ (2) ist klar wegen $\|v\| = \sqrt{\langle v, v\rangle}$ und (2) $\implies$ (1) folgt sofort aus den Polarisierungsformeln aus Satz 9.5. (1) $\implies$ (4) ist klar nach Definition eines Orthonormalsystems, und (4) $\implies$ (3) ist offensichtlich.

(3) $\implies$ (1): Nach Korollar 9.6 können wir $\{f(v_1), \dots, f(v_n)\}$ zu einer Orthonormalbasis für W erweitern. Sind $x = x_1v_1 + \dots + x_nv_n$ und $y = y_1v_1 + \dots + y_nv_n$ beliebige Elemente von V, dann ist nach Proposition 9.6 $\langle x, y\rangle_V = x_1\bar{y}_1 + \dots + x_n\bar{y}_n$. Andererseits ist $f(x) = x_1f(v_1) + \dots + x_nf(v_n)$ und analog für y und damit wiederum nach Proposition 9.8(2) $\langle f(x), f(y)\rangle_V = x_1\bar{y}_1 + \dots + x_n\bar{y}_n$.

(1) $\iff$ (5) Nach Definition ist $\langle v_1, f^*(f(v_2))\rangle_V = \langle f(v_1), f(v_2)\rangle_W$. Da das innere Produkt nicht entartet ist, ist $f^*(f(v_2)) = v_2$ äquivalent zu $\langle v_1, f^*(f(v_2))\rangle_V = \langle v_1, v_2\rangle_V$ für alle $v_1 \in V$, und damit folgt die Behauptung. □

KOROLLAR 9.11. *(1) Orthogonale und unitäre lineare Abbildungen sind automatisch injektiv, also bei gleicher Dimension automatisch euklidische bzw. unitäre Isomorphismen.*

(2) Jeder n–dimensionale euklidische (unitäre) Vektorraum ist orthogonal (unitär) isomorph zu $\mathbb{R}^n$ ($\mathbb{C}^n$) mit dem Standard (hermitischen) inneren Produkt.

(3) $f : V \to V$ ist genau dann orthogonal (unitär) wenn $f^* = f^{-1}$ gilt.

(4) Ist $f : V \to V$ orthogonal (unitär) und $\lambda \in \mathbb{K}$ ein Eigenwert von f, dann ist $|\lambda| = 1$.

(5) Ist $f : V \to V$ orthogonal (unitär), dann ist $|\det(f)| = 1$.

(6) Für eine Matrix $A \in M_n(\mathbb{R})$ ($M_n(\mathbb{C})$) sind äquivalent:

(a) *A ist orthogonal (unitär)*
(b) *die Spaltenvektoren von A bilden eine Orthonormalbasis von $\mathbb{R}^n$ ($\mathbb{C}^n$).*
(c) *$A^t = A^{-1}$ ($A^* = A^{-1}$).*

BEWEIS. (1) Nach Teil (2) des Satzes folgt aus $f(v) = 0$ schon $\|v\| = 0$, also $v = 0$, also ist $\mathrm{Ker}(f) = \{0\}$, also f injektiv.

(2) Nach Korollar 9.6 findet man immer eine Orthonormalbasis. Die eindeutige lineare Abbildung nach $\mathbb{K}^n$, die diese Orthonormalbasis auf die Standardbasis abbildet ist nach Teil (4) des Satzes ein orthogonaler (unitärer) Isomorphismus.

(3) Ist f orthogonal, dann ist f nach (1) invertierbar und nach Teil (5) des Satzes ist $f^* \circ f = \mathrm{id}$. Komponiert man diese Gleichung von rechts mit f^{-1}, so erhält man $f^* = f^{-1}$.

(4) folgt sofort aus $\|f(v)\| = \|v\|$.

(5) Ist $\mathcal{B}$ eine Orthonormalbasis für V und $A = [f]_{\mathcal{B}}$, dann ist nach Satz 9.10 $[f^*]_{\mathcal{B}} = A^*$ (bzw. A^t). Nach Satz 6.7 ist $\det(A^t) = \det(A)$ und daraus folgt natürlich $\det(A^*) = \overline{\det(A)}$. Damit erhalten wir aus $f^* \circ f = \mathrm{id}$ im reellen Fall $\det(A)^2 = 1$ und im komplexen Fall $\det(A)\overline{\det(A)} = 1$, also in beiden Fällen $|\det(A)| = 1$.

(6) Die Äquivalenz der ersten beiden Bedingungen ist die Matrizenversion von Teil (4) des Satzes, die Äquivalenz zur letzten die Matrizenversion von (3). □

9.12. Die QR–Zerlegung. Eine Matrix A ist also genau dann orthogonal bzw. unitär, wenn die Spaltenvektoren eine Orthonormalbasis bilden. Damit können wir aber das Gram–Schmidt Orthonormalisierungsverfahren aus 9.8 auch in Termen von Matrizen formulieren. Das liefert eine Zerlegung für beliebige invertierbare Matrizen, die theoretisch unter dem Namen *Iwasawa–Zerlegung* ziemlich bedeutsam ist, aber auch in der angewandten Mathematik (unter dem Name *QR–Zerlegung*) eine wichtige Rolle spielt.

SATZ 9.12. *Sei A eine invertierbare $n \times n$–Matrix über $\mathbb{R}$ (bzw. $\mathbb{C}$). Dann gibt es eine orthogonale (bzw. unitäre) Matrix Q und eine obere Dreiecksmatrix R mit reellen positiven Eintragungen auf der Hauptdiagonale, sodass $A = QR$ gilt. Die Matrizen Q und R sind eindeutig bestimmt.*

BEWEIS. Sind $v_1, \dots, v_n$ die Spaltenvektoren von A, dann bilden diese Vektoren eine Basis, weil A invertierbar ist. Wenden wir darauf das Gram–Schmidt Orthonormalisierungsverfahren an, dann erhalten wir eine Orthonormalbasis $\{w_1, \dots, w_n\}$, sodass jedes w_j als $b_{1j}v_1 + \dots + b_{jj}v_j$ mit b_{jj} reell und positiv dargestellt werden kann. Ist Q die

Matrix, die die w_j als Spaltenvektoren hat, dann ist Q nach Korollar 9.11 orthogonal (bzw. unitär).

Nach Definition der Matrizenmultiplikation ist $A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1v_1 + \dots + x_nv_n$. Bilden wir also die Matrix $B := (b_{ij})$ (wobei man für $i > j$ $b_{ij} = 0$ setzt), dann erhält man die Spaltenvektoren von AB indem man A auf die Spaltenvektoren von B anwendet, also ergibt sich $AB = Q$. Offensichtlich ist B eine obere Dreiecksmatrix mit reellen positiven Eintragungen auf der Hauptdiagonale. Insbesondere ist $\det(B)$ das Produkt der Hauptdiagonalelemente, also $\det(B) \neq 0$, also B invertierbar und damit $A = QB^{-1}$. Sei B_{ij} die Matrix, die man erhält, wenn man in B die i–te Zeile und die j–te Spalte streicht. Dann ist jedes B_{ij} eine obere Dreiecksmatrix und für $j > i$ ist mindestens eines der Hauptdiagonalelemente gleich 0, also $\det(B_{ij}) = 0$ falls $j > i$. Ist $R := B^{-1} = (r_{ij})$, dann ist nach Satz 6.9 $r_{ij} = (-1)^{i+j}\det(B_{ji})/\det(B)$. Daraus überlegt man leicht direkt, dass $r_{ij} = 0$ für $i > j$ gilt, und $r_{jj} = b_{jj}^{-1}$ reell und positiv ist. Damit folgt die Existenz der Zerlegung.

Zur Eindeutigkeit: Sind Q_1, Q_2 orthogonal und R_1, R_2 obere Dreiecksmatrizen mit positiven reellen Eintragungen auf der Hauptdiagonale, sodass $Q_1R_1 = Q_2R_2$ gilt, dann ist $Q_2^{-1}Q_1 = R_2R_1^{-1}$. Einerseits ist aber $Q_2^{-1}Q_1$ unitär, andererseits ist $R_2R_1^{-1}$ eine obere Dreiecksmatrix mit positiven reellen Eintragungen auf der Hauptdiagonale. Damit sind aber die Hauptdiagonalelemente Eigenwerte einer orthogonalen (unitären) linearen Abbildung, haben also nach Teil (4) von Korollar 9.11 Betrag Eins, also sind alle Hauptdiagonalelemente gleich Eins, weil sie reell und positiv sein müssen. Da die Spaltenvektoren von eine orthogonalen (unitären) Matrix ein Orthonormalsystem bilden, folgt sofort $R_2R_1^{-1} = \mathbb{I}$ und damit $R_1 = R_2$, also auch $Q_1 = Q_2$. □

9.13. Spiegelungen. Das einfachste Beispiel einer nichttrivialen orthogonalen (unitären) Abbildung ist die Spiegelung an einer Hyperebene. Nach 9.9 kann man jede Hyperebene W in einem euklidischen oder unitären Vektorraum V als $W = \{a\}^\perp$ für einen Einheitsvektor $a \in V$ schreiben. Definieren wir nun für $a \in V$ mit $\|a\| = 1$ die *Spiegelung* $s_a : V \to V$ an $\{a\}^\perp$ durch $s_a(v) := v - 2\langle v, a\rangle a$.

Lemma 9.13. *Für jedes $a \in V$ mit $\|a\| = 1$ ist die Spiegelung s_a an $\{a\}^\perp$ eine orthogonale (unitäre) lineare Abbildung mit $(s_a)^{-1} = s_a$ und $\det(s_a) = -1$. Die Spiegelung ist charakterisiert durch $s_a(a) = -a$ und $s_a(v) = v$ falls $\langle v, a\rangle = 0$.*

Für $v \neq w \in V$ gibt es genau dann einen Einheitsvektor $a \in V$ mit $s_a(v) = w$, wenn $\|v\| = \|w\|$ sowie $\langle v, w\rangle \in \mathbb{R}$ gilt.

Beweis. Die Abbildung s_a ist offensichtlich linear, und nach Definition gilt $s_a(a) = a - 2\langle a, a\rangle a = -a$ und $s_a(v) = v$ falls $\langle v, a\rangle = 0$. Nach Korollar 9.6 ist $V = \mathbb{K}\cdot a \oplus \{a\}^\perp$, also kann man jedes $v \in V$ eindeutig als $\lambda a + w$ mit $\langle w, a\rangle = 0$ schreiben. Damit ist aber $s_a(v) = -\lambda a + w$, also ist s_a durch die obigen Eigenschaften eindeutig bestimmt. Nach dem Satz von Pythagoras liefert diese Zerlegung $\|v\|^2 = |\lambda|^2 + \|w\|^2 = \|s_a(v)\|^2$, also ist s_a orthogonal nach Satz 9.11. Erweitern wir das Orthonormalsystem $\{a\} \subset V$ zu einer Orthonormalbasis $\mathcal{B} = \{a, v_2, \dots, v_n\}$, dann ist $\langle v_i, a\rangle = 0$ für alle $i = 2, \dots, n$, also ist $[s_a]_{\mathcal{B}}$ eine Diagonalmatrix mit einer -1 und sonst lauter Einsen auf der Hauptdiagonale, also ist $s_a \circ s_a = \mathrm{id}$ und $\det(s_a) = -1$.

Das s_a orthogonal bzw. unitär ist, ist $\|s_a(v)\| = \|v\|$. Außerdem ist nach Definition $\langle v, s_a(v)\rangle = \langle v, v\rangle - 2\overline{\langle v, a\rangle}\langle v, a\rangle \in \mathbb{R}$. Damit bleibt nur noch zu zeigen, dass es für $v \neq w \in V$ mit $\|v\| = \|w\|$ und $\langle v, w\rangle \in \mathbb{R}$ einen Einheitsvektor $a \in V$ gibt, sodass

$s_a(v) = w$ gilt. Geometrisch bedeuten die Bedingungen $\|v\| = \|w\|$ und $\langle v, w\rangle \in \mathbb{R}$ genau, dass $(v + w) \perp (v - w)$ gilt. Es ist nämlich

$$\langle v + w, v - w\rangle = (\|v\|^2 - \|w\|^2) - (\langle v, w\rangle - \overline{\langle v, w\rangle}),$$

und die letzte Klammer liefert genau den $2i$ mal dem Imaginärteil von $\langle v, w\rangle$. Nach Voraussetzung ist $v - w \neq 0$, also können wir $a := \frac{1}{\|v-w\|}(v - w)$ setzen. Dann ist

$$s_a(v) = v - 2\langle v, a\rangle a = v - 2\tfrac{\langle v,v-w\rangle}{\langle v-w,v-w\rangle}(v - w).$$

Aus $\langle v+w, v-w\rangle = 0$ folgt aber sofort $\langle w, v-w\rangle = -\langle v, v-w\rangle$, und damit $\frac{\langle v,v-w\rangle}{\langle v-w,v-w\rangle} = \frac{1}{2}$, also $s_a(v) = w$. □

Daraus erhalten wir sofort eine schöne geometrische Charakterisierung von orthogonalen Abbildungen:

Satz 9.13. *Sei $(V, \langle\ ,\ \rangle)$ ein n–dimensionaler euklidischer Vektorraum und $f : V \to V$ eine orthogonale lineare Abbildung. Dann gibt es eine Zahl $k \leq n$ und Einheitsvektoren $a_1, \dots, a_k \in V$, sodass $f = s_{a_1} \circ \dots \circ s_{a_k}$ gilt. Insbesondere ist* $\det(f) = (-1)^k$.

Beweis. Fixieren wir eine Orthonormalbasis $\{v_1, \dots, v_n\}$ von V. Nach Teil (4) von Satz 9.11 ist $\{f(v_1), \dots, f(v_n)\}$ ebenfalls eine Orthonormalbasis für V. Sei j der kleinste Index, sodass $f(v_j) \neq v_j$ gilt. Wegen $\|f(v_j)\| = \|v_j\| = 1$ (und weil wir über $\mathbb{R}$ arbeiten) ist nach dem Lemma $s_{a_1}(f(v_j)) = v_j$, wobei $a_1 = \frac{f(v_j)-v_j}{\|f(v_j)-v_j\|}$.

Für $i < j$ ist $v_i \perp v_j$ und $v_i = f(v_i) \perp f(v_j)$, also auch $v_i = f(v_i) \perp a_1$, also $s_{a_1}(f(v_i)) = f(v_i) = v_i$. Damit gilt aber $(s_{a_1} \circ f)(v_i) = v_i$ für alle $i \leq j$ und $s_{a_1} \circ f$ ist wiederum orthogonal. Induktiv finden wir Einheitsvektoren $a_1, \dots, a_k$, sodass $(s_{a_k} \circ \dots \circ s_{a_1} \circ f)(v_i) = v_i$ für alle $i = 1, \dots, n$. Damit ist diese Komposition aber die Identitätsabbildung, und wegen $(s_{a_j})^{-1} = s_{a_j}$ liefert das $f = s_{a_1} \circ \dots \circ s_{a_k}$. Wegen $\det(s_{a_j}) = -1$ für alle j folgt $\det(f) = (-1)^k$ sofort. □

9.14. Orthogonale Abbildungen in Dimension 2 und 3. Als nächstes wollen wir orthogonale Abbildungen in $\mathbb{R}^2$ und $\mathbb{R}^3$ (jeweils mit dem Standard inneren Produkt) beschreiben. Nach Korollar 9.11 liefert das auch die Beschreibung für beliebige euklidische Vektorräume der Dimensionen zwei und drei.

Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ orthogonal. Dann ist nach Satz 9.13 entweder f eine Spiegelung, oder f ist eine Komposition von zwei Spiegelungen und $\det(f) = 1$. Ein Einheitsvektor in $\mathbb{R}^2$ hat die Form (x, y) mit $x^2 + y^2 = 1$. Damit gibt es aber einen eindeutigen Winkel $\varphi \in [0, 2\pi)$, sodass $x = \cos(\varphi)$ und $y = \sin(\varphi)$ gilt. Die zwei möglichen Einheitsnormalvektoren zu (x, y) sind nach 9.9 durch $(-y, x)$ und $(y, -x)$ gegeben. Ist nun f orthogonal mit $\det(f) = 1$ und ist $f(e_1) = a = (\cos(\varphi), \sin(\varphi))$, dann muss $f(e_2)$ ein Normalvektor zu $f(e_1)$ sein, der außerdem noch $\det(f(e_1), f(e_2)) = 1$ erfüllt. Damit entspricht f aber der Matrix $\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$, also ist f genau die Drehung um den Winkel φ.

Um andererseits eine Matrixdarstellung für die Spiegelung s_a für $a = (\cos(\varphi), \sin(\varphi))$ zu erhalten, betrachten wir die Rotation f um den Winkel φ. Diese bildet e_1 auf a und e_2 auf ein Element von $a^\perp$ ab. Damit folgt aber sofort, dass $f^{-1} \circ s_a \circ f$ den Basisvektor e_1 auf $-e_1$ und e_2 auf sich selbst abbildet. Damit ist aber die Matrix zu s_a gegeben durch

$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} = \begin{pmatrix} -\cos(2\varphi) & -\sin(2\varphi) \\ -\sin(2\varphi) & \cos(2\varphi) \end{pmatrix}.$$

In drei Dimensionen ist die Situation ähnlich einfach. Eine orthogonale lineare Abbildung $f : \mathbb{R}^3 \to \mathbb{R}^3$ ist entweder eine Spiegelung, oder eine Komposition von zwei Spiegelungen und erfüllt $\det(f) = 1$, oder eine Komposition von drei Spiegelungen. Die wesentliche Beobachtung hier ist aber, dass f mindestens einen reellen Eigenwert besitzen muss, weil jedes Polynom dritten Grades mindestens eine reelle Nullstelle hat. Nach Korollar 9.11 muss dieser Eigenwert gleich 1 oder -1 sein.

Ist v ein Eigenvektor dazu, dann betrachten wir den Teilraum $W = \{v\}^\perp \subset \mathbb{R}^3$. Für $w \in W$ ist $\langle v, f(w)\rangle = \pm\langle f(v), f(w)\rangle = \pm\langle v, w\rangle = 0$, also ist $f(w) \in W$, also W ein f–invarianter Teilraum. Wir können das innere Produkt auf W einschränken und natürlich ist die Einschränkung von f auf W orthogonal bezüglich dieses inneren Produktes. Damit können wir diese Einschränkung aus der Beschreibung der zweidimensionalen orthogonalen Abbildungen von oben ablesen: Ist der Eigenwert von oben gleich 1, dann ist für $\det(f) = 1$ die Abbildung f eine Drehung um die Achse $\{tv : t \in \mathbb{R}\}$ während wir für $\det(f) = -1$ ein Spiegelung an einer Ebene erhalten, die v enthält.

Ist der Eigenwert von oben gleich -1 und ist $\det(f) = 1$, dann muss die Einschränkung von f auf W Determinante -1 haben, also eine Spiegelung sein. Damit erhalten wir aber einen zweidimensionalen Eigenraum zum Eigenwert -1 und einen eindimensionalen Eigenraum zum Eigenwert 1. Geometrisch können wir f als "Spiegelung" an der Geraden interpretieren, die durch den Eigenraum zum Eigenwert Eins beschrieben wird. Im letzten Fall, also Eigenwert gleich -1 und $\det(f) = -1$ muss die Einschränkung von f auf W Determinante Eins haben, also eine Drehung sein. Damit ist f aber die Komposition einer Drehung um die Achse $\{tv : t \in \mathbb{R}\}$ mit der Spiegelung an $W = \{v\}^\perp$. Im Spezialfall des Winkels π erhalten wir $f = -\mathrm{id}$, was wir auch als Punktspiegelung im Nullpunkt interpretieren können.

Normale, selbstadjungierte und symmetrische lineare Abbildungen

Wir besprechen nun eine Version von Diagonalisierbarkeit, die den Ideen von Orthogonalität angepasst ist. Überraschenderweise ist Diagonalisierbarkeit in diesem Sinn sehr einfach zu charakterisieren.

9.15. Orthogonale und unitäre Diagonalisierbarkeit. Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer (unitärer) Vektorraum. Eine lineare Abbildung $f : V \to V$ heißt *orthogonal (unitär) diagonalisierbar*, wenn es eine Orthonormalbasis von V gibt, die aus Eigenvektoren von f besteht.

Analog wie in 7.2 ist die orthogonale (unitäre) Diagonalisierbarkeit von f äquivalent dazu, dass es eine Orthonormalbasis $\mathcal{B}$ für V gibt, sodass $[f]_{\mathcal{B}}$ eine Diagonalmatrix ist. Das Konzept der orthogonalen (unitären) Diagonalisierbarkeit macht natürlich auch für Matrizen Sinn, wobei man für $A \in M_n(\mathbb{K})$ einfach die lineare Abbildung $\mathbb{K}^n \to \mathbb{K}^n$, $x \mapsto Ax$ betrachtet. Da die Basiswechsel zwischen zwei Orthonormalbasen nach Teil (3) von Satz 9.11 genau den orthogonalen (unitären) Matrizen entsprechen, ist $A \in M_n(\mathbb{K})$ genau dann orthogonal (unitär) diagonalisierbar, wenn es eine orthogonale (unitäre) Matrix $U \in M_n(\mathbb{K})$ gibt (die nach Korollar 9.11 automatisch invertierbar ist), sodass UAU^{-1} eine Diagonalmatrix ist. Man bemerke, dass UAU^{-1} nach Definition für orthogonales U gleich UAU^t und für unitäres U gleich UAU^* ist.

Betrachten wir zunächst den komplexen Fall. Sei $f : V \to V$ unitär diagonalisierbar und $f^* : V \to V$ die adjungierte Abbildung zu f. Ist $\mathcal{B}$ eine Orthonormalbasis für V, die aus Eigenvektoren von f besteht, dann ist $[f]_{\mathcal{B}}$ eine Diagonalmatrix. Nach Satz 9.10 ist dann $[f^*]_{\mathcal{B}} = ([f]_{\mathcal{B}})^*$, also ebenfalls eine Diagonalmatrix, nur sind die

Eintragungen auf der Hauptdiagonale gerade die Konjugierten der ursprünglichen Eintragungen. Jedenfalls gilt aber $[f]_{\mathcal{B}}[f^*]_{\mathcal{B}} = [f^*]_{\mathcal{B}}[f]_{\mathcal{B}}$, und damit ist $f \circ f^* = f^* \circ f$. Man nennt lineare Abbildung mit dieser Eigenschaft *normal*. Man bemerke, dass insbesondere unitäre Abbildungen normal sind, weil sie nach Korollar 9.11 $f^* = f^{-1}$ und damit $f \circ f^* = f^* \circ f = \mathrm{id}$ erfüllen. Überraschenderweise charakterisiert diese Eigenschaft schon die unitär diagonalisierbaren linearen Abbildungen, denn es gilt:

Satz 9.15. *Sei $(V, \langle\ ,\ \rangle)$ ein unitärer Vektorraum. Dann ist eine lineare Abbildung $f : V \to V$ genau dann unitär diagonalisierbar, wenn sie normal ist, also $f \circ f^* = f^* \circ f$ erfüllt.*

Beweis. Wir müssen nur noch zeigen, dass eine normale lineare Abbildung $f : V \to V$ unitär diagonalisierbar ist, und dazu benutzen wir Induktion nach $n := \dim(V)$. Für $n = 1$ ist jede lineare Abbildung unitär diagonalisierbar. Nehmen wir also induktiv an, dass $n \geq 2$ gilt, und der Satz für alle $k < n$ bereits bewiesen wurde. Da $\mathbb{C}$ algebraisch abgeschlossen ist, besitzt f mindestens einen Eigenwert $\lambda \in \mathbb{C}$ und der zugehörige Eigenraum $V_\lambda^f \subset V$ ist ein Teilraum der Dimension ≥ 1. Ist nun $W := (V_\lambda^f)^\perp \subset V$, dann ist $\dim(W) < \dim(V)$.

Wir behaupten, dass der Teilraum W f–invariant ist. Zum Beweis bemerken wir zunächst, dass V_λ^f invariant unter f^* ist. Ist nämlich $v \in V_\lambda^f$, dann ist $f(f^*(v)) = f^*(f(v)) = \lambda f^*(v)$ wegen der Normalität von f, also $f^*(v) \in V_\lambda^f$. Ist nun aber $w \in W$ und $v \in V_\lambda^f$, dann ist $\langle v, f(w)\rangle = \langle f^*(v), w\rangle = 0$, weil $f^*(v) \in V_\lambda^f$ gilt, also gilt $f(w) \in W$.

Nun können wir das hermitische innere Produkt auf W einschränken und natürlich ist die Einschränkung $f|_W : W \to W$ von f auf W normal bezüglich dieses inneren Produktes. Damit gibt es aber nach Induktionsvoraussetzung eine Orthonormalbasis für W, die aus Eigenvektoren für f besteht. Andererseits gibt es nach Korollar 9.6 eine Orthonormalbasis für V_λ^f. Weil $W = (V_\lambda^f)^\perp$ gilt, ist die Vereinigung der beiden Orthonormalbasen eine Orthonormalbasis für V, also folgt die Behauptung. □

Korollar 9.15. *Sei $(V, \langle\ ,\ \rangle)$ ein n–dimensionaler unitärer Vektorraum, $f : V \to V$ eine unitäre lineare Abbildung. Dann gibt es eine Orthonormalbasis $\{v_1, \dots, v_n\}$ für V und Elemente $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ mit $|\lambda_j| = 1$ für alle j, sodass $f(v_j) = \lambda_j v_j$ für alle $j = 1, \dots, n$ gilt.*

Beweis. Wie wir bereits festgestellt haben ist jede unitäre lineare Abbildung normal, also nach dem Satz unitär diagonalisierbar. Nach Korollar 9.11 hat jeder Eigenwert von f Betrag Eins, also folgt die Behauptung. □

9.16. Selbstadjungierte und symmetrische Abbildungen. Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer (unitärer) Vektorraum. Eine lineare Abbildung $f : V \to V$ heißt *symmetrisch (selbstadjungiert)*, wenn $f^* = f$ gilt.

Eine Matrix $A \in M_n(\mathbb{R})$ heißt *symmetrisch*, wenn $A^t = A$ gilt und eine Matrix $B \in M_n(\mathbb{C})$ heißt *selbstadjungiert* oder *hermitisch*, wenn $B^* = B$ gilt.

Nach Definition ist eine lineare Abbildung $f : V \to V$ also genau dann symmetrisch (selbstadjungiert), wenn $\langle f(v), w\rangle = \langle v, f(w)\rangle$ für alle $v, w \in V$ gilt. Nach Satz 9.10 ist f genau dann symmetrisch (selbstadjungiert) wenn eine (oder äquivalent jede) Matrixdarstellung von f bezüglich einer Orthonormalbasis von V eine symmetrische (selbstadjungierte) Matrix ist.

Natürlich sind selbstadjungierte lineare Abbildungen auf einem komplexen Vektorraum automatisch normal, weil ja $f^* \circ f = f \circ f = f \circ f^*$ gilt. Insbesondere sind also selbstadjungierte lineare Abbildungen nach Satz 9.15 immer unitär diagonalisierbar. Ist aber $v \in V$ ein Eigenvektor für f zum Eigenwert λ, dann ist $\langle f(v), v\rangle = \lambda\langle v, v\rangle$ aber $\langle v, f(v)\rangle = \bar{\lambda}\langle v, v\rangle$. Da v ein Eigenvektor ist, ist $\langle v, v\rangle \neq 0$, also muss $\lambda \in \mathbb{R}$ gelten. Somit erhalten wir

Proposition 9.16. *Sei $(V, \langle\ ,\ \rangle)$ ein unitärer Vektorraum und $f : V \to V$ eine selbstadjungierte lineare Abbildung. Dann ist f unitär diagonalisierbar und alle Eigenwerte von f sind reell.*

Man kann auch leicht direkt sehen, dass zwei Eigenvektoren v, w einer selbstadjungierten linearen Abbildung $f : V \to V$ zu *verschiedenen* Eigenwerten $\lambda \neq \mu$ automatisch orthogonal aufeinander stehen. Es gilt nämlich $\lambda\langle v, w\rangle = \langle f(v), w\rangle = \langle v, f(w)\rangle = \mu\langle v, w\rangle$ (wobei wir im letzten Schritt benutzt haben, dass μ reell ist), also $(\lambda - \mu)\langle v, w\rangle = 0$.

Daraus können wir aber nun die orthogonale Diagonalisierbarkeit auf euklidischen Vektorräumen charakterisieren.

Satz 9.16. *Sei $(V, \langle\ ,\ \rangle)$ ein euklidischer Vektorraum. Eine lineare Abbildung $f : V \to V$ ist genau dann orthogonal diagonalisierbar, wenn sie symmetrisch ist, also $f^* = f$ erfüllt.*

Beweis. Ist f orthogonal diagonalisierbar, dann sei $\mathcal{B}$ eine Orthonormalbasis aus Eigenvektoren. Dann ist $[f]_{\mathcal{B}}$ eine Diagonalmatrix, also insbesondere symmetrisch, also ist $[f^*]_{\mathcal{B}} = [f]_{\mathcal{B}}$, also $f^* = f$.

Ist umgekehrt $f : V \to V$ symmetrisch, dann beweisen wir mit Induktion nach $n = \dim(V)$, dass f diagonalisierbar ist. Für $n = 1$ ist nichts zu zeigen, also nehmen wir $n > 1$ an und der Satz sei für Vektorräume der Dimension $n - 1$ bereits bewiesen. Sei $\mathcal{B}$ eine beliebige Orthonormalbasis für V und $A = [f]_{\mathcal{B}}$. Dann ist A eine symmetrische reelle $n \times n$–Matrix, erfüllt also als komplexe Matrix betrachtet die Gleichung $A^* = A^t = A$. Damit wissen wir aber aus unseren Überlegungen über selbstadjungierte lineare Abbildungen auf unitären Vektorräumen von oben, dass alle Eigenwerte von A reell sind.

Insbesondere hat f mindestens einen reellen Eigenwert a und dazu finden wir einen Eigenvektor v mit $\|v\| = 1$. Sei nun $W = \{v\}^\perp$. Für $w \in W$ ist $\langle f(w), v\rangle = \langle w, f(v)\rangle = a\langle w, v\rangle = 0$, also ist W ein f–invarianter Teilraum. Das innere Produkt schränkt sich zu einem inneren Produkt auf W ein, bezüglich dem f symmetrisch ist. Nach Induktionsvoraussetzung finden wir eine Orthonormalbasis für W, die aus Eigenvektoren für f besteht, geben wir zu dieser Basis v dazu, dann erhalten wir eine Orthonormalbasis für V aus Eigenvektoren. □

Damit können wir nun auch ein vollständiges Schema angeben, wie man eine symmetrische Matrix $A \in M_n(\mathbb{R})$ orthogonal diagonalisiert. Zunächst bestimmt man die Eigenwerte. Für jeden Eigenraum findet man mit Hilfe des Gauß'schen Algorithmus eine Basis, die man mit Hilfe des Gram–Schmidt Verfahrens orthonormalisiert. Vereinigt man die Orthonormalbasen für die verschiedenen Eigenräume, dann erhält man eine Orthonormalbasis für V, die aus Eigenvektoren für A besteht. Schreibt man diese Basisvektoren als Spaltenvektoren in eine Matrix und invertiert diese, dann erhält man eine orthogonale Matrix U, sodass UAU^t eine Diagonalmatrix ist.

Analog kann man natürlich bei normalen Matrizen in $M_n(\mathbb{C})$ beziehungsweise bei symmetrischen (normalen) linearen Abbildungen auf euklidischen (unitären) Vektorräumen vorgehen.

9.17. Anwendung: Klassifikation von Kurven zweiten Grades. Eine Funktion zweiten Grades auf $\mathbb{R}^n$ ist eine Funktion $\kappa : \mathbb{R}^n \to \mathbb{R}$ der Form

$$\kappa(x_1, \dots, x_n) = \sum_{j=1}^{n} \alpha_j x_j^2 + \sum_{j<k} \beta_{jk} x_j x_k + \sum_{\ell=1}^{n} \gamma_\ell x_\ell + \delta,$$

wobei $\alpha_i, \beta_{jk}, \gamma_\ell, \delta \in \mathbb{R}$, und mindestens ein α oder ein β ungleich Null ist. Eine Hyperfläche zweiten Grades in $\mathbb{R}^n$ ist eine Teilmenge der Form $\{v \in \mathbb{R}^n : \kappa(v) = 0\}$, wobei κ eine Funktion zweiten Grades ist. Wir wollen solche Funktionen (bzw. Hyperflächen) zweiten Grades durch Translationen und orthogonale Abbildungen in eine einfache Form bringen, wobei wir den Fall $n = 2$ von *Kurven zweiten Grades* im Detail betrachten werden.

Der Schlüssel dazu ist, dass man die Funktion κ von oben mit Hilfe des Standard inneren Produktes schön anschreiben kann: Sei dazu $A = (a_{ij}) \in M_n(\mathbb{R})$ gegeben durch $a_{ii} = \alpha_i$ für $i = 1, \dots, n$, $a_{ij} = \frac{1}{2}\beta_{ij}$ für $i < j$ und $a_{ij} = a_{ji}$ für $i > j$. Weiters sei $b = (\gamma_1, \dots, \gamma_n) \in \mathbb{R}^n$. Dann erhalten wir für $x = (x_1, \dots, x_n)$

$$\langle Ax, x\rangle + \langle b, x\rangle + \delta = \sum_{i=1}^{n} x_i (\sum_{j=1}^{n} a_{ij} x_j) + \sum_{k=1}^{n} \gamma_k x_k + \delta = \kappa(x).$$

Nach Definition ist die Matrix A symmetrisch.

Wir wollen nun versuchen, die Funktion

$$(*) \qquad \kappa(x) = \langle Ax, x\rangle + \langle b, x\rangle + \delta$$

durch Translationen und orthogonale Abbildungen zu vereinfachen, um die Nullstellenmenge gut beschreiben zu können. Um den Effekt einer Translation zu bestimmen, berechnen wir

$$\kappa(x - v) = \langle Ax - Av, x - v\rangle + \langle b, x - v\rangle + \delta.$$

Dabei benutzen wir, dass $A^t = A$ und damit $\langle Ax, -v\rangle = \langle -Av, x\rangle$ gilt, und erhalten

$$\langle Ax, x\rangle + \langle b - 2Av, x\rangle + \langle Av, v\rangle - \langle b, v\rangle + \delta = \langle Ax, x\rangle + \langle \tilde{b}, x\rangle + \tilde{\delta},$$

wobei $\tilde{b} = b - 2Av$ und $\tilde{\delta} = \delta - \langle b, v\rangle + \langle Av, v\rangle$.

Setzen wir $\varphi(x) = Ax$, dann ist $\varphi^* = \varphi$ und nach Satz 9.10 ist $\mathrm{Ker}(\varphi)^\perp = \mathrm{Im}(\varphi^*) = \mathrm{Im}(\varphi)$. Damit kann nach Korollar 9.6 jedes Element $w \in \mathbb{R}^n$ eindeutig in der Form $w = w_0 + w_1$ mit $w_0 \in \mathrm{Ker}(\varphi)$ und $w_1 \in \mathrm{Im}(\varphi)$ geschrieben werden. Natürlich kann man φ auf den Teilraum $\mathrm{Im}(\varphi)$ einschränken und erhält so eine lineare Abbildung $\varphi : \mathrm{Im}(\varphi) \to \mathrm{Im}(\varphi)$. Da $\mathrm{Ker}(\varphi) \cap \mathrm{Im}(\varphi) = \{0\}$ gilt, ist diese Abbildung injektiv, also ein linearer Isomorphismus. Nun zerlegen wir $b = b_0 + b_1$ und $v = v_0 + v_1$ in dieser Weise, und erhalten $\tilde{b} = b_0 + (b_1 - 2Av_1)$ und $\tilde{\delta} = \delta - \langle b_0, v_0\rangle - \langle b_1, v_1\rangle - \langle Av_1, v_1\rangle$. Nun können wir v_1 eindeutig so wählen, dass $2Av_1 = b_1$, also $\tilde{b} = b_0$ gilt. Nun unterschieden wir zwei Fälle:

Fall 1: Ist $\tilde{b} = b_0 = 0$, dann beeinflusst die Wahl von v_0 weder $\tilde{b}$ noch $\tilde{\delta}$, wir können also einfach $v_0 = 0$ setzen und keine weitere Normalisierung erreichen.

Fall 2: Ist $\tilde{b} = b_0 \neq 0$, dann ist $\langle b_0, b_0\rangle \neq 0$, also können wir

$$v_0 := \frac{\delta - \frac{3}{2}\langle b_1, v_1\rangle}{\langle b_0, b_0\rangle} b_0$$

setzen, um $\tilde{\delta} = 0$ zu erreichen. Dazu könnten wir noch Elemente von $\mathrm{Ker}(\varphi)$ addieren, die zusätzlich orthogonal zu b_0 sind, das ändert aber wieder nichts mehr.

Zusammenfassend kann man sagen, dass man durch eine Translation erreichen kann, dass man in der Formel $(*)$ für die Funktion κ von oben entweder $b = 0$ oder $b \neq 0$, $Ab = 0$ und $\delta = 0$ annehmen kann.

Der zweite Schritt der Normalisierung ist noch einfacher: Wir berechnen einfach in $(*)$ $\kappa(Ux)$ für eine orthogonale Matrix U und erhalten

$$\langle AUx, Ux\rangle + \langle b, Ux\rangle + \delta = \langle U^tAUx, x\rangle + \langle U^tb, x\rangle + \delta.$$

Das ersetzt also nur die Matrix A durch $U^tAU = U^{-1}AU$ und b durch $U^tb = U^{-1}b$, und da $U^{-1}AUU^{-1}b = U^{-1}Ab$ gilt, bleiben die vereinfachenden Annahmen von oben einfach in der gleichen Form gültig. Da $A = A^t$ gilt, können wir die Matrix U nach Satz 9.16 so wählen, dass U^tAU diagonal mit den Eigenwerten von A (in beliebiger Reihenfolge) auf der Hauptdiagonale ist. Davon ausgehend kann man nun in allgemeinen Dimensionen eine Klassifikation von Hyperflächen zweiten Grades durchführen, wir werden uns aber auf den Fall $n = 2$ von *Kurven zweiten Grades* beschränken.

Nach Voraussetzung ist die Matrix A ungleich Null und symmetrisch, sie hat also zwei reelle Eigenwerte α und β, von denen mindestens einer ungleich Null ist, und durch eine orthogonale Transformation wie oben können wir erreichen, dass A diagonal ist. Nun betrachten wir die beiden oben angeführten Fälle:

Fall 1: Ist $b = 0$, dann müssen wir noch nach dem Rang von A Unterfälle unterscheiden:

Fall 1a: Ist $\operatorname{rg}(A) = 2$, dann können wir durch eine orthogonale Transformation wie oben erreichen, dass unsere Matrix die Form $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ mit $\alpha, \beta \neq 0$ hat. Das liefert die Funktion zweiten Grades

$$\alpha(x_1)^2 + \beta(x_2)^2 + \delta,$$

und wir können noch mit einem beliebigen Faktor $\neq 0$ multiplizieren, ohne die Nullstellenmenge zu ändern. Ist $\delta = 0$, dann multiplizieren wir mit $1/\alpha$ und erhalten die Gleichung $(x_1)^2 + \frac{\beta}{\alpha}(x_2)^2 = 0$. Für $\frac{\beta}{\alpha} > 0$ (d.h. wenn α und β gleiches Vorzeichen haben) Ist das nur der Nullpunkt. Für $\frac{\beta}{\alpha} < 0$ erhält man $x_1 = \pm\sqrt{-\frac{\beta}{\alpha}}x_2$, also zwei Gerade, die sich in Null schneiden.

Ist $\delta \neq 0$, dann dividieren wir durch $-\delta$ und erhalten dadurch die Gleichung $\frac{-\alpha}{\delta}(x_1)^2 + \frac{-\beta}{\delta}(x_2)^2 = 1$. Sind die Faktoren $\frac{-\alpha}{\delta}$ und $\frac{-\beta}{\delta}$ beide < 0, dann beschreibt das die leere Menge. Ist $\frac{-\alpha}{\delta} > 0$ und $\frac{-\beta}{\delta} < 0$, dann setzt man $c = \sqrt{\frac{-\alpha}{\delta}}$ und $d = \sqrt{\frac{\beta}{\delta}}$ und erhält die Gleichung $(\frac{x_1}{c})^2 - (\frac{x_2}{d})^2 = 1$, die eine Hyperbel in erster Hauptlage mit Hauptachsenlänge c und Nebenachsenlänge d beschreibt. Analog erhält man für die umgekehrte Konfiguration der Vorzeichen eine Hyperbel in zweiter Hauptlage. Sind schließlich beide Faktoren positiv, dann setzt man $c = \sqrt{\frac{-\alpha}{\delta}}$ und $d = \sqrt{\frac{-\beta}{\delta}}$ und erhält die Gleichung $(\frac{x_1}{c})^2 + (\frac{x_2}{d})^2 = 1$ und damit eine Ellipse.

Fall 1b: Ist $\operatorname{rg}(A) = 1$, dann können wir durch eine orthogonale Transformation wie oben erreichen, dass unsere Matrix die Form $\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}$ mit $\alpha \neq 0$ hat. Das liefert die Funktion zweiten Grades

$$\alpha(x_1)^2 + \delta,$$

und wir können wieder mit einem beliebigen Faktor $\neq 0$ multiplizieren. Für $\delta = 0$ dividieren wir durch α und erhalten $(x_1)^2 = 0$, und damit die x_2–Achse (eigentlich doppelt gezählt) als Nullstellenmenge. Für $\delta \neq 0$ dividieren wir durch $-\delta$ und erhalten

$\frac{-\alpha}{\delta}(x_1)^2 = 1$. Das liefert entweder (für $\frac{\alpha}{\delta} > 0$) die leere Menge oder (für $\frac{\alpha}{\delta} < 0$) $x_1 = \pm\sqrt{\frac{-\alpha}{\delta}}$, also zwei parallele Gerade.

Fall 2: Ist $b \neq 0$, dann muss A nichttrivialen Kern haben, also $\operatorname{rg}(A) = 1$ gelten. Damit erreichen wir durch eine Orthogonale Transformation wieder die Matrix $\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}$ mit $\alpha \neq 0$. Weiters muss $b_0 \neq 0$ von dieser Matrix auf Null abgebildet werden, also ein Vielfaches von e_2 sein, sagen wir $b = \lambda e_2$. Damit erhalten wir als Funktion zweiten Grades $\alpha(x_1)^2 + \lambda x_2$ und wir dürfen wieder durch einen beliebigen Faktor $\neq 0$ dividieren. In diesem Fall ist die übliche Konvention durch $-\frac{\lambda}{2}$ zu dividieren, was zur Gleichung $\frac{-2\alpha}{\lambda}(x_1)^2 = 2x_2$ und damit zu einer Parabel führt.

9.18. Anwendung 2: Klassifikation der symmetrischen Bilinearformen. Sei V ein endlichdimensionaler reeller Vektorraum und seien $b, \tilde{b} : V \times V \to \mathbb{R}$ symmetrische Bilinearformen. Wir nennen die Formen b und $\tilde{b}$ *äquivalent*, wenn es einen linearen Isomorphismus $f : V \to V$ gibt, sodass $\tilde{b}(v, w) := b(f(v), f(w))$ gilt. Das definiert eine Äquivalenzrelation auf der Menge aller symmetrischen Bilinearformen auf V, und wir wollen entscheiden, wann zwei Formen in diesem Sinne äquivalent sind. Dazu werden wir wieder eine Normalform für eine Bilinearform bestimmen, d.h. eine Basis finden, in der die Bilinearform möglichst einfach aussieht. Durch Anwenden eines linearen Isomorphismus dürfen wir ohne Beschränkung der Allgemeinheit $V = \mathbb{R}^n$ annehmen. Der Schlüssel zu diesem Problem liegt wieder darin, dass man es mit Hilfe des Standard inneren Produktes auf eine Frage über symmetrische Matrizen zurückführen kann.

Sei also $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ ein symmetrische Bilinearform. Definiere die Matrix $A = (a_{ij}) \in M_n(\mathbb{R})$ zu b durch $a_{ij} = b(e_i, e_j)$, wobei $\{e_1, \dots, e_n\}$ die Standardbasis bezeichnet. Da b symmetrisch ist, ist A eine symmetrische Matrix. Für $x = (x_1, \dots, x_n)$ und $y = (y_1, \dots, y_n) \in \mathbb{R}^n$ ist $x = \sum x_i e_i$ und $y = \sum y_j e_j$, also erhalten wir wegen der Bilinearität von b die Gleichung

$$b(x, y) = b(\sum x_i e_i, \sum y_j e_j) = \sum_{i,j} x_i y_j b(e_i, e_j) = \sum_i x_i (\sum_j a_{ij} y_j) = \langle x, Ay \rangle.$$

Umgekehrt definiert für jede Matrix $A = (a_{ij}) \in M_n(\mathbb{R})$ natürlich $(x, y) \mapsto \langle x, Ay \rangle$ eine Bilinearform β auf $\mathbb{R}^n$ mit $a_{ij} = \beta(e_i, e_j)$ und wegen $\langle y, Ax \rangle = \langle Ax, y \rangle = \langle x, A^t y \rangle$ ist β genau dann symmetrisch wenn die Matrix A symmetrisch ist. Damit erhalten wir eine Bijektion zwischen der Menge der symmetrischen Bilinearformen und der Menge der symmetrischen Matrizen.

Jeder lineare Isomorphismus $f : \mathbb{R}^n \to \mathbb{R}^n$ ist von der Form $x \mapsto Tx$ für eine invertierbare Matrix $T \in M_n(\mathbb{R})$. Damit ist aber $b(Tx, Ty) = \langle Tx, ATy \rangle = \langle x, T^t ATy \rangle$. Damit sind aber die Bilinearformen zu symmetrischen Matrizen $A, B \in M_n(\mathbb{R})$ genau dann äquivalent, wenn es eine invertierbare Matrix T gibt, sodass $B = TAT^t$ gilt. (Beachte, dass mit T auch T^t invertierbar ist, und $(T^t)^{-1} = (T^{-1})^t$ gilt.)

Als nächstes stellen wir die Frage, wann $b(x, y) = \langle x, Ay \rangle$ nicht entartet ist. Definiere dazu den *Nullraum* von b als $V_0^b := \{x \in \mathbb{R}^n : b(x, y) = 0 \quad \forall y \in \mathbb{R}^n\}$. Offensichtlich ist dies ein Teilraum von $\mathbb{R}^n$. Der *Rang* $\operatorname{rg}(b)$ der symmetrischen Bilinearform b ist definiert als $n - \dim(V_0^b)$. Weil $\langle\ ,\ \rangle$ nicht entartet ist, ist aber $\langle x, Ay \rangle = \langle Ax, y \rangle$ genau dann für alle $y \in \mathbb{R}^n$ gleich Null, wenn $Ax = 0$ gilt. Damit ist aber V_0^b genau der Kern der linearen Abbildung $x \mapsto Ax$, also stimmt der Rang von b mit dem Rang der Matrix A überein. Insbesondere ist b genau dann nicht entartet, wenn A invertierbar ist.

Satz 9.18 (Trägheitssatz von Sylvester). *Sei V ein n–dimensionaler reeller Vektorraum und sei $b : V \times V \to \mathbb{R}$ eine symmetrische Bilinearform. Dann gibt es eindeutig bestimmte Zahlen $p, q \in \mathbb{N}$ mit $p + q = \operatorname{rg}(b) \leq n$ sowie eine Basis $\{v_1, \dots, v_n\}$ für V, sodass $b(v_i, v_j) = 0$ für $i \neq j$, und $b(v_i, v_i)$ gleich 1 für $1 \leq i \leq p$, gleich -1 für $p + 1 \leq i \leq p + q$ und gleich 0 für $i > p + q$ gilt. Man sagt dann, b hat Signatur (p, q).*

Zwei symmetrische Bilinearformen auf V sind genau dann äquivalent, wenn sie die gleiche Signatur haben.

Beweis. Wie oben erklärt dürfen wir $V = \mathbb{R}^n$ annehmen. Sei $A \in M_n(\mathbb{R})$ die Matrix zu b. Da A symmetrisch ist, finden wir eine Orthonormalbasis $\{\tilde{v}_1, \dots, \tilde{v}_n\}$ aus Eigenvektoren für A, die wir so anordnen, dass erst Eigenvektoren zu positiven Eigenwerten, dann solche zu negativen Eigenwerten und dann solche zum Eigenwert Null kommen. Sind p und q die Anzahlen der positiven bzw. negativen Eigenwerte, dann ist $A\tilde{v}_i = \lambda_i \tilde{v}_i$ mit $\lambda_i > 0$ für $i = 1, \dots, p$, $\lambda_i < 0$ für $i = p + 1, \dots, p + q$ und $\lambda_i = 0$ für $i > p + q$. Bemerke, dass $p+q$ gleich dem Rang von A, also dem Rang von b ist. Nach Konstruktion ist $b(\tilde{v}_i, \tilde{v}_j) = \langle A\tilde{v}_i, \tilde{v}_j\rangle = \lambda_i \langle \tilde{v}_i, \tilde{v}_j\rangle$, also gleich 0 für $i \neq j$ und gleich λ_i für $i = j$. Setzt man nun $v_i = (\lambda_i)^{-1/2}\tilde{v}_i$ für $1 \leq i \leq p$, $v_i = (-\lambda_i)^{-1/2}\tilde{v}_i$ für $p+1 \leq i \leq p+q$ und $v_i = \tilde{v}_i$ für $i \geq p + q$, dann hat die Basis $\{v_1, \dots, v_n\}$ die gewünschten Eigenschaften.

Zur Eindeutigkeit von p und q haben wir bereits bemerkt, dass $p+q$ gleich dem Rang von b ist, also genügt es zu zeigen, dass p eindeutig bestimmt ist. Sei also $\{w_1, \dots, w_n\}$ eine weitere Basis für V, sodass $b(w_i, w_j) = 0$ für $i \neq j$ und $b(w_i, w_i) > 0$ für $1 \leq i \leq p'$ und $b(w_i, w_i) \leq 0$ für $i > p'$. Dann behaupten wir, dass die Menge $\{v_1, \dots, v_p, w_{p'+1}, \dots, w_n\}$ linear unabhängig ist. Ist nämlich $\sum_{i=1}^p \lambda_i v_i + \sum_{j=p'+1}^n \mu_j w_j = 0$, dann ist $\sum_{i=1}^p \lambda_i v_i = -\sum_{j=p'+1}^n \mu_j w_j$, und damit

$$b\Big(\sum_{i=1}^p \lambda_i v_i, \sum_{i=1}^p \lambda_i v_i\Big) = b\Big(\sum_{j=p'+1}^n \mu_j w_j, \sum_{j=p'+1}^n \mu_j w_j\Big).$$

Nach Konstruktion liefert aber die linke Seite $\sum_{i=1}^p (\lambda_i)^2 \geq 0$ und die rechte Seite $\sum_{j=p'+1}^n (\mu_j)^2 b(w_j, w_j) \leq 0$. Damit kann Gleichheit nur gelten, wen beide Seiten gleich Null sind. Damit sind insbesondere alle $\lambda_i = 0$, und wegen der linearen Unabhängigkeit von $\{w_{p'+1}, \dots, w_n\}$ müssen auch alle μ_j Null sein. Damit muss aber $p + (n - p') \leq n$, also $p \leq p'$ gelten, und vertauscht man die Rollen der beiden Basen, dann folgt $p' \leq p$, also $p = p'$. Damit ist die Signatur wohldefiniert, und zwei Bilinearformen können nur dann äquivalent sein, wenn sie die selbe Signatur haben.

Sind umgekehrt b und $\tilde{b}$ symmetrische Bilinearformen mit der selben Signatur, dann finden wir entsprechende Basen $\{v_1, \dots, v_n\}$ und $\{w_1, \dots, w_n\}$. Ist $f : V \to V$ die eindeutige lineare Abbildung, die $f(v_i) = w_i$ für alle i erfüllt, dann ist für $v = \sum x_i v_i$ das Bild $f(v) = \sum x_i w_i$ und daraus folgt sofort $\tilde{b}(f(v), f(w)) = b(v, w)$ für alle $v, w \in V$. □

Literaturverzeichnis

[1] A. Čap, *Einführung in die Lineare Algebra und Geometrie*, Skriptum Sommersemester 2010, online erhältlich via http://www.mat.univie.ac.at/~cap/lectnotes.html

[2] H. Schichl, R. Steinbauer, *Einführung in das mathematische Arbeiten*, Springer–Verlag 2009.