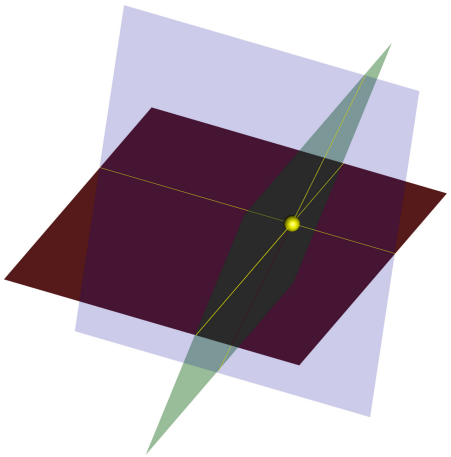
Thomas Krämer

Lineare Algebra II

HU Berlin, Sommer 25



(Version vom 15. Juli 2025)

Inhaltsverzeichnis

Kapitel I
Die Jordan-Normalform

Zusammenfassung Wir haben gesehen, dass man viele Matrizen durch geeigneten Basiswechsel in eine Diagonalform bringen kann. Nun wenden wir uns der Frage zu, wie sehr sich nicht-diagonalisierbare Matrizen durch Basiswechsel vereinfachen lassen. Über algebraisch abgeschlossenen Körpern ist jede Matrix trigonalisierbar, d.h. sie lässt sich auf eine Dreiecksform bringen. Allgemeiner gilt dies für jede Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt. Die Wahl einer Trigonalisierung lässt noch viele Freiheiten; das diesbezüglich optimale Resultat ist die Jordan-Normalform, die alle trigonalisierbare Matrizen bis auf Ähnlichkeit klassifiziert und mit der man fast wie mit Diagonalmatrizen rechnen kann.

1 Einführung

Wir wollen für einen gegebenen Endomorphismus f eines endlich-dimensionalen Vektorraumes über einem Körper K eine Basis finden, bezüglich der f durch eine möglichst einfache Abbildungsmatrix beschrieben wird. Wenn wir von einer festen Basis ausgehen, läuft dies hinaus auf die Suche nach einem guten Basiswechsel:

Definition 1.1. Zwei Matrizen $A, B \in \mathrm{Mat}(n \times m, K)$ heißen *äquivalent zueinander*, wenn es eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ gibt mit $B = S^{-1}AS$.

Dieser Begriff definiert eine Äquivalenzrelation $\sim$ auf $\mathrm{Mat}(m \times n, K)$, und wir suchen in jeder Äquivalenzklasse einen möglichst einfachen Repräsentanten. Im einfachsten Fall könnte das so aussehen:

Definition 1.2. Eine Matrix $A \in \mathrm{Mat}(n \times m, K)$ heißt *diagonalisierbar*, wenn eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ existiert, sodass gilt:

$$S^{-1}AS \;=\; \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \;:=\; \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{mit} \quad \lambda_1, \ldots, \lambda_n \in K$$

Wenn wir so eine Diagonalisierung finden können, ist das sehr praktisch für das Berechnen von Matrixpotenzen: Es gilt dann

$$A^k \;=\; S\cdot\begin{pmatrix}\lambda_1 & & 0\\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}\cdot S^{-1} \quad \text{für alle} \quad k\in\mathbb{N}.$$

Für $K=\mathbb{R}$ erhalten wir dann z.B. einen einfachen Beweis für die Konvergenz der Exponentialreihe

$$e^A \;=\; \sum_{k=0}^{\infty}\frac{1}{k!}A^k \;=\; S\cdot\begin{pmatrix}e^{\lambda_1} & & 0\\ & \ddots & \\ 0 & & e^{\lambda_n}\end{pmatrix}\cdot S^{-1}$$

und können damit lineare Differentialgleichungssysteme lösen:

Beispiel 1.3. Gesucht seien für $1\le i\le n$ differenzierbare Funktionen $y_i:\mathbb{R}\longrightarrow\mathbb{R}$ mit der Eigenschaft

$$\begin{cases} y_1'(x) &= a_{11}y_1(x)+\cdots+a_{1n}y_n(x)\\ &\vdots\\ y_n'(x) &= a_{n1}y_1(x)+\cdots+a_{nn}y_n(x)\end{cases}$$

Dies ist ein lineares Differentialgleichungssystem, das sich in der Matrixform

$$y'(x)\;=\;A\cdot y(x)\quad\text{für}\quad y(x)\;=\;\begin{pmatrix}y_1(x)\\ \dots\\ y_n(x)\end{pmatrix},\quad A\;=\;(a_{ij}\in\mathrm{Mat}(n\times m,\mathbb{R}))$$

darstellen lässt. Aus dieser letzten Darstellung können wir im diagonalisierbaren Fall sofort ablesen, dass die allgemeine Lösung des Systems gegeben ist durch

$$y(x)\;=\;e^{xA}\cdot y(0).$$

Mit elementaren Abschätzungen kann man zeigen, dass die Exponentialreihe auch für nicht diagonalisierbare Matrizen konvergiert und die obige Formel für $y(x)$ auch in diesem Fall richtig bleibt. Aber wie berechnet man e^{xA} dann?

Für solche Anwendungen möchten wir auch Matrizen $A\in\mathrm{Mat}(n\times m,K)$, die nicht diagonalisierbar sind, durch Basiswechsel in eine möglichst einfache Form bringen. Wir definieren dazu das *Spektrum* $S(A)\subset K$ als die Menge der Eigenwerte von A. Für $\lambda\in S(A)$ betrachten wir

- den Eigenraum $E(A,\lambda):=\ker(A-\lambda\mathrm{i})$,
- seine geometrische Vielfachheit $d(A,\lambda)=\dim_K E(A,\lambda)$,
- seine algebraische Vielfachheit $e(A,\lambda)=\mathrm{ord}_{t=\lambda}\,\chi_A(t)$.

Bei der Diskussion von diagonalisierbaren Matrizen in Teil I der Vorlesung hatten wir

$$\bigoplus_{\lambda \in S(A)} E(A,\lambda) \subseteq K^n \quad \text{und} \quad d(A,\lambda) \leq e(A,\lambda)$$

gesehen. Wir hatten uns außerdem überlegt, dass folgende Äquivalenzen gelten:

$$\begin{aligned} \text{A diagonalisierbar} \quad &\Longleftrightarrow \quad \bigoplus_{\lambda} E(A,\lambda) = K^n \\ &\Longleftrightarrow \quad \sum_{\lambda} d(A,\lambda) = n \\ &\Longleftrightarrow \quad \chi_A(t) \text{ zerfällt über } K \text{ in Linearfaktoren} \\ &\qquad\quad \text{und } d(A,\lambda) = e(A,\lambda) \text{ für alle } \lambda \in S(A). \end{aligned}$$

Beispiel 1.4. Für $\lambda \in \mathbb{R}$ betrachte man die Matrix

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

Hier ist $\chi_A(t) = \det(t \cdot \mathbf{1} - A) = (t-\lambda)^2$ und die Matrix A ist nicht diagonalisierbar, denn

$$d(A,\lambda) = 1 < e(a,\lambda) = 2.$$

Dennoch kann man mit dieser Matrix prima rechnen: Denn es ist $A = \lambda \cdot \mathbf{1} + N$ für die Matrix

$$N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{mit} \quad N^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

und somit folgt

$$A^k = (\lambda \mathbf{1} + N)^k = \lambda^k \cdot \mathbf{1} + k \cdot \lambda^{k-i} \cdot N = \begin{pmatrix} \lambda^k & 0 \\ k \cdot \lambda^{k-1} & \lambda^k \end{pmatrix}$$

Wir wollen uns in diesem Kapitel überlegen, welche Matrizen man durch einen Basiswechsel auf eine ähnlich einfache Dreiecksgestalt bringen kann.

2 Trigonalisierbare Matrizen

Sei V ein endlich-dimensionaler Vektorraum über einem Körper K.

Definition 2.1. Ein Endomorphismus $f \in \mathrm{End}_K(V)$ heißt *trigonalisierbar (über K)*, wenn eine Basis $\mathscr{B}$ von V existiert, bezüglich der er dargestellt wird durch eine Dreiecksmatrix

$$M_{\mathscr{B}}(f) = \begin{pmatrix} \lambda_1 & & 0 \\ \vdots & \ddots & \\ * & \dots & \lambda_n \end{pmatrix}.$$

Wir wollen zeigen, dass dies genau dann der Fall ist, wenn das charakteristische Polynom $\chi_f(t)$ über K in Linearfaktoren zerfällt. In diesem Kontext ist der folgende Begriff wichtig:

Definition 2.2. Ein Untervektorraum $U \subseteq V$ heißt *f-invariant*, wenn gilt:

$$f(u) \in U \quad \text{für alle} \quad u \in U.$$

Beispiel 2.3. Seien $f, g \in \mathrm{End}_K(V)$ mit $f \circ g = g \circ f$ gegeben. Dann gilt:

a) Der Kern $\ker(g) \subseteq V$ ein f-invarianter Untervektorraum, denn

$$u \in \ker(g) \implies g(f(u)) = f(g(u)) = f(0) = 0 \implies f(u) \in \ker(g)$$

b) Das Bild $\mathrm{im}(g) \subseteq V$ ist ein f-invarianter Untervektorraum, denn

$$u \in \mathrm{im}(g) \implies \exists w \in V : u = g(w) \implies f(u) = f(g(w)) = g(f(w)) \in \mathrm{im}(g)$$

Für $\lambda \in K$ erhalten wir insbesondere f-invariante Untervektorräume

$$\ker((f - \lambda \cdot id)^k) \subseteq V$$
$$\mathrm{im}((f - \lambda \cdot id)^k) \subseteq V$$

Die Bedeutung f-invarianter Untervektorräume erklärt sich aus dem

Lemma 2.4. *Sei $U \subseteq V$ ein $f-$invarianter Untervektorraum und $W := V/U$.*

a) f induziert Endomorphismen

$$f_U := f|_U \in \mathrm{End}_K(U)$$
$$f_W := (f \mod U) \in \mathrm{End}_K(W)$$

b) Sei $\mathscr{A} = (v_1, \ldots, v_d)$ eine Basis von U und $\mathscr{B} = (v_1, \ldots, v_d, v_{d+1}, \ldots, v_n)$ eine daraus mittels des Basisergänzungssatzes gewonnene Basis von V. Dann bilden die Restklassen $[v_i] := (v + U) \in W = V/U$ für $d < i \leq n$ eine Basis $\mathscr{C}$ von W und es gilt

$$M_{\mathscr{B}}(f) = \begin{pmatrix} M_{\mathscr{A}}(f_U) & * \\ 0 & M_{\mathscr{C}}(f_W) \end{pmatrix}. \tag{I.1}$$

Beweis. *a*) Für f_U ist dies klar. Für f_W setzen wir $f_W(w) := [f(v)]$ für $w = [v] \in W$ und rechnen nach, dass dies wohldefiniert ist:

$$\begin{aligned} [v] = [v'] \in W &\implies v' = v + u \text{ für ein } u \in U \\ &\implies f(v') = f(v) + f(u) \\ &\implies [f(v')] = [f(v)] \in W \end{aligned}$$

b) Sei $M_{\mathscr{B}}(f) = (a_{ij})$. Dann gilt

$$f(v_j) \;=\; \sum_{i=1}^{n} a_{ij}\cdot v_i \;=\; \underbrace{\sum_{i=1}^{d} a_{ij}v_i}_{\in U} + \underbrace{\sum_{i=d+1}^{n} a_{ij}v_i}_{\in \langle v_{d+1},\ldots,v_n\rangle}$$

Für $j \le d$ ist dabei $v_j \in U$, also auch $f(v_j) \in U = \langle v_1,\ldots,v_d\rangle$. Somit folgt $a_{ij} = 0$ für alle Indexpaare (i,j) mit $i > d$ und $j \le d$, und wir erhalten die angegebene Blockform für die Abbildungsmatrix. □

Bemerkung 2.5. Wir haben hier eine obere Blockdreiecksmatrix erzeugt. Wenn wir die Basis umnumerieren gemäß

$$\tilde{A} \;=\; (v_d,\ldots,v_1), \quad \tilde{B} \;=\; (v_n,v_{n-1},\ldots,v_d,\ldots,v_1), \quad \tilde{C} \;=\; ([v_n],\ldots,[v_{d+1}]),$$

erhalten wir stattdessen eine untere Blockdreiecksmatrix

$$M_{\tilde{B}}(f) \;=\; \begin{pmatrix} M_{\tilde{C}}(f_w) & 0 \\ * & M_{\tilde{A}}(f_u) \end{pmatrix}.$$

Die Einträge $*$ sind Null genau dann, wenn der Untervektorraum $\langle v_{d+1},\ldots,v_n\rangle \le V$ ebenfalls f-invariant ist. Das kann man nicht immer erreichen! Unabhängig davon gilt jedoch in der Situation des obigen Lemmas stets

$$\chi_f(t) \;=\; \chi_{f_U}(t)\cdot\chi_{f_W}(t).$$

Dies führt auf die folgende Charakterisierung trigonalisierbarer Endomorphismen:

Satz 2.6. *Für $f \in \mathrm{End}_K(V)$ sind äquivalent:*

a) f ist trigonalisierbar.

b) $\chi_f(t) = \prod_{i=1}^{n}(t-\lambda_i)$ mit $\lambda_i \in K$.

c) Es gibt eine Kette von f-invarianten Untervektorräumen

$$0 \;=\; V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n \;=\; V \quad \textit{mit} \quad \dim_K V_i \;=\; i \quad \textit{für alle } i.$$

Beweis. Aus *a*) folgt sofort *b*). Aus *b*) erhält man *c*): Wenn $\chi_f(t) = \prod_i(t-\lambda_i)$ ist, hat f insbesondere einen Eigenwert $\lambda_1 \in K$. Sei $v_1 \in V$ ein zugehöriger Eigenvektor, dann ist $V_1 = \langle v_1\rangle_K$ ein f-invarianter Untervektorraum der Dimension $\dim_K V_1 = 1$. Wir betrachten nun den Quotienten

$$W \;=\; V/V_1.$$

Wegen $\chi_f(t) = (t-\lambda_1)\cdot\chi_{f|_W}(t)$ ist $\chi_{f|_W}(t) = \prod_{i>1}(t-\lambda_i)$. Per Induktion über die Dimension gibt es somit eine Kette f-invarianter Untervektorräume

$$0 \;=\; W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq W_{n-1} \;=\; W \quad \text{mit} \quad \dim_K W_i \;=\; i \quad \text{für alle } i.$$

Für $i \geq 1$ definieren wir $V_i \subseteq V$ als das Urbild von W_{i-1}, dann gilt $c)$. Aus $c)$ folgt wiederum $a)$, indem man eine Basis $(v_n, \ldots, v_1)$ von V wählt mit

$$V_i = \langle v_1, \ldots, v_i \rangle_K \quad \text{für alle } i,$$

denn in einer solchen Basis wird f durch eine Dreiecksmatrix dargestellt. □

Korollar 2.7. *Falls K algebraisch abgeschlossen ist, dann ist jedes $f \in \mathrm{End}_K(V)$ trigonalisierbar.*

Man beachte, dass die Trigonalisierbarkeit einer Matrix noch viel Freiraum für Wünsche lässt: Z.B. ist die Matrix

$$\begin{pmatrix} \lambda & 0 \\ 1 & \mu \end{pmatrix}$$

in Dreiecksform, aber für $\lambda \neq \mu$ wäre sie sogar diagonalisierbar. Wir wollen als nächstes alle trigonalisierbaren Matrizen auf eine möglichst einfache Dreiecksform bringen (die im diagonalisierbaren Fall eine Diagonalmatrix sein wird).

3 Die Jordan-Normalform

[siehe handschriftliche Notizen]

4 Eindeutigkeit der JNF

[siehe handschriftliche Notizen]

5 Existenz und Berechnung der JNF

[siehe handschriftliche Notizen]

6 Die Jordan-Chevalley Zerlegung

Die Jordan-Normalform liefert insbesondere eine Zerlegung von Endomorphismen in zwei einfache Bestandteile: Die Eigenwerte auf der Diagonalen, und die Einsen auf der Nebendiagonalen. Sei allgemeiner ein Vektorraum V endlicher Dimension über K gegeben. Ein Endomorphismus $f \in \mathrm{End}_K(V)$ heißt *nilpotent*, wenn $f^k = 0$

für geeignetes $k \in \mathbb{N}$ ist. Aus der Jordan-Normalform erhalten wir die nützliche Folgerung:

Satz 6.1 (Additive Jordan-Chevalley Zerlegung). *Sei V ein Vektorraum endlicher Dimension über einem Körper K. Jedes trigonalisierbare $f \in \mathrm{End}_K(V)$ hat dann eine eindeutige Zerlegung*

$$f \;=\; f_d + f_n$$

mit $f_d \in \mathrm{End}_K(V)$ diagonalisierbar, $f_n \in \mathrm{End}_K(V)$ nilpotent und $f_d \circ f_n = f_n \circ f_d$.

Beweis. In einer passenden Basis wird f durch eine Matrix A in Jordan-Normalform dargestellt, für die Existenz der gesuchten Zerlegung genügt es daher, den Fall einer Matrix in Jordan-Normalform zu betrachten. Wenn wir die Existenz der Zerlegung für jeden Jordanblock einzeln zeigen können, folgt sie für die gesamte Matrix. Es genügt also, einen einzelnen Jordanblock zu betrachten. In diesem Fall leistet die Zerlegung

$$\begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{pmatrix} + \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$$

das Gewünschte. Zu zeigen bleibt nur die Eindeutigkeit. Dazu sei eine beliebige Zerlegung $f = f_d + f_n$ mit f_d diagonalisierbar, f_n nilpotent und $f_d \circ f_n = f_n \circ f_d$ gegeben. Insbesondere liefert die Diagonalisierbarkeit von f_d eine Zerlegung als direkte Summe

$$V \;=\; \bigoplus_{\lambda \in K} V_\lambda \quad \text{für die Eigenräume} \quad V_\lambda \;=\; \ker(f_d - \lambda \cdot \mathbf{1}).$$

Durch diese Zerlegung ist f_d und damit auch $f_n = f - f_d$ eindeutig festgelegt, wir müssen also nur zeigen, dass die direkten Summanden in der obigen Zerlegung durch f eindeutig bestimmt sind. Dazu vergleichen wir diese Zerlegung mit der Hauptraumzerlegung

$$V \;=\; \bigoplus_{\lambda \in K} \ker(f - \lambda \cdot id_V)^e \quad \text{für genügend großes} \quad e \gg 0.$$

Es genügt zu zeigen, dass

$$V_\lambda \;\subseteq\; \ker(f - \lambda \cdot id_V)^e$$

ist für alle $\lambda \in K$, denn aus Dimensionsgründen gilt dann sogar Gleichheit. Um die obige Inklusion zu zeigen, beachte man zunächst, dass aus $f_n \circ f_d = f_d \circ f_n$ auch folgt:

$$f \circ f_d \;=\; (f_d + f_n) \circ f_d \;=\; f_d \circ (f_d + f_n) \;=\; f_d \circ f$$

Alle betrachteten Endomorphismen kommutieren daher mit f_d und schränken sich ein zu Endomorphismen von $V_\lambda = \ker(f_d - \lambda id_V)$. Insbesondere erhalten wir also Endomorphismen

$$\begin{aligned} f_n|_{V_\lambda}: \quad V_\lambda &\longrightarrow V_\lambda \\ (f-\lambda id_V)|_{V_\lambda}: \quad V_\lambda &\longrightarrow V_\lambda \end{aligned}$$

Diese sind gleich, denn

$$\begin{aligned} (f-\lambda id_V)|_{V_\lambda} &= (f_d + f_n - \lambda id_V)|_{V_\lambda} && \text{wegen } f = f_d + f_n \\ &= (f_d - \lambda id_V)|_{V_\lambda} + f_n|_{V_\lambda} && \text{durch Umstellen} \\ &= f_n|_{V_\lambda} && \text{wegen } (f_d - \lambda id_V)|_{V_\lambda} = 0 \end{aligned}$$

Da f_n nilpotent ist, folgt wie gewünscht $(f-\lambda id_V)^e|_{V_\lambda} = 0$ für $e \gg 0$. □

Die obige Zerlegung als Summe eines diagonalisierbaren und eines nilpotenten Teils hat ein multiplikatives Analogon, wobei Endomorphismen zu ersetzen sind durch Automorphismen. Wir nennen $f \in \mathrm{Aut}_K(V)$ *unipotent*, falls $f - id_V$ nilpotent ist. Es gilt:

Korollar 6.2 (Multiplikative Jordan-Chevalley Zerlegung). *Wie zuvor sei V ein Vektorraum endlicher Dimension über einem Körper K. Dann zerlegt sich jedes trigonalisierbare $f \in \mathrm{Aut}_K(V)$ eindeutig in der Form*

$$f = f_d \circ f_u$$

mit $f_d \in \mathrm{Aut}_K(V)$ diagonalisierbar, $f_u \in \mathrm{Aut}_K(V)$ unipotent und $f_d \circ f_u = f_u \circ f_d$.

Beweis. Sei $f = f_d + f_n$ die additive Jordan-Chevalley Zerlegung aus Satz 6.1. Aus dem Beweis des Satzes wissen wir, dass die Eigenwerte von f übereinstimmen mit denen von f_d. Da f ein Automorphismus ist, sind die Eigenwerte alle von Null verschieden und folglich ist auch f_d ein Automorphismus. Wir können daher f_u definieren durch

$$f_u = id_V + f_d^{-1} \circ f_n$$

und erhalten eine Zerlegung mit den gewünschten Eigenschaften. Die Eindeutigkeit folgt analog aus der Eindeutigkeit in der additiven Jordan-Chevalley Zerlegung. □

Die additive Zerlegung in einen diagonalisierbaren und einen nilpotenten Teil ist nicht nur von theoretischer Bedeutung, sondern hilft auch für das Rechnen mit konkreten Matrizen: Seien $D, N \in \mathrm{Mat}(n \times n, K)$ zwei Matrizen mit $DN = ND$, dann gilt

$$(D+N)^m = \sum_{i=0}^{m} \tbinom{k}{k} \cdot D^{m-i} \cdot N^i \quad \text{für alle} \quad m \in \mathbb{N}.$$

Wenn D eine Diagonalmatrix ist, können wir die Potenzen D^{m-i} sofort ausrechnen, und für nilpotente Matrizen N folgt aus der Jordan-Normalform sofort $N^i = 0$ für alle $i \geq n$, sodass in der obigen Summe nur die Terme mit $i < n$ auftreten.

Beispiel 6.3. Die Matrix

$$A = \begin{pmatrix} 8 & 6 & 9 \\ 0 & 2 & 0 \\ -4 & -4 & -4 \end{pmatrix} \in \mathrm{Mat}(3\times 3, \mathbb{C})$$

besitzt nur $\lambda = 2$ als Eigenwert. In der Jordan-Chevalley-Zerlegung $A = D + N$ ist somit der diagonalisierbare Anteil gegeben durch $D = 2 \cdot \mathbf{1}$, denn skalare Vielfache der Einheitsmatrix sind nur zu sich selber ähnlich. Der nilpotente Anteil ist dann gegeben durch

$$N = A - D = \begin{pmatrix} 6 & 6 & 9 \\ 0 & 0 & 0 \\ -4 & -4 & -6 \end{pmatrix}.$$

Offenbar ist $\dim\ker(N) = 3 - \mathrm{rk}(N) = 2$. Insbesondere folgt $N^i = 0$ für alle $i \geq 2$ ohne weitere Rechnung aus der Jordan-Normalform für nilpotente Matrizen, und wir erhalten für beliebige $m \in \mathbb{N}$ die Formel

$$A^m = (D+N)^m = D^m + m \cdot D^{m-1} \cdot N = 2^m \cdot \begin{pmatrix} 1+3m & 3m & 9m/2 \\ 0 & 1 & 0 \\ -2m & -2m & 1-3m \end{pmatrix}.$$

Die Jordan-Normalform ist hier

$$J = SAS^{-1} = \left(\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 2 & 0 \\ 0 & 1 & 2 \end{array}\right) \quad \text{für geeignetes} \quad S \in \mathrm{GL}_3(\mathbb{C}),$$

aber den Basiswechsel S haben wir für die obige Formel nicht explizit berechnen müssen. Das ist der Vorteil der Jordan-Chevalley-Zerlegung!

Falls eine Matrix schon in Jordan-Normalform gegeben ist, dann lassen sich ihre Potenzen blockweise ausrechnen, indem wir die Jordanblöcke potenzieren. Hierfür erhalten wir mit der additiven Jordan-Chevalley Zerlegung die folgende Formel:

Lemma 6.4. *Sei $A = J_n(\lambda)$ ein Jordanblock der Länge n zum Eigenwert λ. Dann gilt*

$$A^m = \begin{pmatrix} \lambda^m & & & & \\ \binom{m}{1}\lambda^{m-1} & \lambda^m & & & \\ \binom{m}{2}\lambda^{m-2} & \binom{m}{1}\lambda^{m-1} & \lambda^m & \ddots & \\ \ddots & \ddots & \ddots & \ddots & \\ & \ddots & \binom{m}{2}\lambda^{m-2} & \binom{m}{1}\lambda^{m-1} & \lambda^m \end{pmatrix}$$

wobei wir für $k > m$ formal $\binom{m}{k}\lambda^{m-k+1} = 0$ setzen.

Beweis. Die Jordan-Chevalley Zerlegung hat die Form $A = D + N$ mit

$$D = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{pmatrix} \quad \text{und} \quad N = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}.$$

Die Potenzen N^i sind dabei Matrizen, die Einsen auf der i-ten Nebendiagonalen haben und deren übrigen Einträge alle Null sind. □

7 Polynome von Matrizen

In der Hauptraumzerlegung haben wir für Matrizen $A \in \mathrm{Mat}(n \times n, K)$ die Kerne der Matrizen $(A - \lambda \cdot \mathbf{1})^k$ für $k \in \mathbb{N}$ betrachtet. Wir haben dabei die Matrix A für die Variable t in

$$(t - \lambda)^k \in K[t]$$

eingesetzt, was Sinn ergibt, da man Matrizen in $\mathrm{Mat}(n \times n, K)$ addieren, potenzieren und mit Skalaren multiplizieren kann. Allgemeiner können wir in Polynome in $K[t]$ für die Variable t Elemente einer beliebigen K-Algebra einsetzen:

Proposition 7.1. *Sei S eine K-Algebra. Dann gibt es für jedes $s \in S$ genau einen Homomorphismus von K-Algebren*

$$ev_s : \quad K[t] \longrightarrow S \quad \textit{mit} \quad t \mapsto s.$$

Wir nennen ev_s die Evaluations- *oder* Auswertungsabbildung *im Punkt s.*

Beweis. Direktes Nachrechnen. □

Die obige universelle Eigenschaft erklärt die Bedeutung von Polynomringen für die gesamte Algebra. Man beachte, dass die K-Algebra S nicht kommutativ sein muß. Wenn wir $S = \mathrm{Mat}(n \times n, K)$ wählen, erhalten wir für $A \in \mathrm{Mat}(n \times n, K)$ einen Homomorphismus

$$ev_A : \quad K[t] \longrightarrow \mathrm{Mat}(n \times n, K), \quad f \mapsto f(A)$$

von K-Algebren, d.h. wir können die Matrix A in beliebige Polynome einsetzen.

Beispiel 7.2. Wenn wir die Matrix

$$A = \begin{pmatrix} -3 & 4 \\ -2 & 3 \end{pmatrix} \in \mathrm{Mat}(2 \times 2, \mathbb{Q})$$

in das Polynom $p(t) = t^2 - 1 \in \mathbb{Q}[t]$ einsetzen, erhalten wir

$$p(A) = A^2 - \mathbf{1} = \begin{pmatrix} -3 & 4 \\ -2 & 3 \end{pmatrix} \cdot \begin{pmatrix} -3 & 4 \\ -2 & 3 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Allgemein gilt:

Lemma 7.3. *Für jedes $A \in \mathrm{Mat}(n \times n, K)$ gibt es ein $p \in K[t] \setminus \{0\}$ mit $p(A) = 0$.*

Beweis. Wir betrachten in dem Vektorraum $\mathrm{Mat}(n \times n, K)$ die unendliche Folge aller Potenzen

$$\mathbf{1},\ A,\ A^2,\ A^3,\ \ldots \in \mathrm{Mat}(n \times n, K).$$

Diese unendlich vielen Potenzen können wegen $\dim_K \mathrm{Mat}(n \times n, K) = n^2 < \infty$ keine linear unabhängige Familie bilden. Es gibt also lineare Relationen zwischen ihnen, etwa

$$c_n A^n + c_{n-1} A^{n-1} + \cdots + c_1 A + c_0 \mathbf{1} = 0$$

für geeignete $c_0, \ldots, c_n \in K$, die nicht alle Null sind. □

Das folgende Lemma liefert für eine gegebene Matrix eine Beschreibung sämtlicher Polynome, welche bei Einsetzen dieser Matrix Null ergeben:

Lemma 7.4. *Sei $A \in \mathrm{Mat}(n \times n, K)$. Dann gibt es genau ein Polynom $\mu_A(t) \in K[t]$ mit Leitkoeffizient 1, sodass für alle Polynome $p(t) \in K[t]$ die folgende Äquivalenz gilt:*

$$p(A) = 0 \quad \Longleftrightarrow \quad \begin{array}{l} p(t) \text{ is durch } \mu_A(t) \text{ teilbar, d.h.} \\ \exists\, q(t) \in K[t] \colon\ p(t) = q(t) \cdot \mu_A(t). \end{array}$$

Beweis. Wir beweisen zunächst die Existenz eines Polynoms $\mu_A(t) \in K[t]$ mit der gewünschten Eigenschaft: Lemma 7.3 liefert von Null verschiedene Polynome, die bei Einsetzen von A Null ergeben. Wir wählen $\mu_A(t)$ als ein solches von kleinstem möglichem Grad. Nach Multiplikation mit einem Skalar dürfen wir annehmen, dass

sein Leitkoeffizient 1 ist. Für jedes andere $p(t) \in K[t]$ liefert Division mit Rest zwei Polynome $q(t), r(t) \in K[t]$ mit

$$p(t) \;=\; q(t) \cdot \mu_A(t) + r(t) \quad \text{und} \quad \deg r(t) \;<\; \deg \mu_A(t).$$

Dabei ist $r(A) = p(A) - q(A) \cdot \mu_A(A) = 0 - q(A) \cdot 0 = 0$. Wegen $\deg r(t) < \deg \mu_A(t)$ und der vorausgesetzten Minimalität von $\deg \mu_A(t)$ ist dies nur möglich, wenn $r(t)$ das Nullpolynom ist. Dann ist $p(t) = q(t) \cdot \mu_A(t)$ wie gewünscht.

Die behauptete Eindeutigkeit folgt analog: Ist $p(t) \in K[t]$ ein weiteres Polynom mit den genannten Eigenschaften, so ist p ein Teiler von μ_A und umgekehrt. Das geht nur, wenn p ein skalares Vielfaches von μ_A ist. Aber da beide den Leitkoeffizient 1 haben, ist dann $p = \mu_A$. □

Definition 7.5. Wir nennen μ_A das *Minimalpolynom* von $A \in \mathrm{Mat}(n \times n, K)$.

Für Endomorphismen $f \in \mathrm{End}_K(V)$ eines K-Vektorraumes V mit $\dim_K V < \infty$ setzen wir

$$\mu_f(t) \;:=\; \mu_A(t) \quad \text{für die Abbildungsmatrix} \quad A \;=\; M_{\mathscr{B}}(f),$$

wobei $\mathscr{B}$ eine Basis von V sei. Da die Abbildungsmatrizen zu je zwei verschiedenen Basen zueinander ähnlich sind und da ähnliche Matrizen dasselbe Minimalpolynom haben, hängt $\mu_f(t)$ nicht von der gewählten Basis $\mathscr{B}$ ab.

Beispiel 7.6. Es gilt:

a) Es ist $\deg \mu_A(t) \geq 1$ für alle $A \in \mathrm{Mat}(n \times n, K)$.

b) Es ist $\mu_A(t) = t - \alpha$ genau dann, wenn $A = \alpha \cdot \mathbf{1}$ ist.

c) Für Diagonalmatrizen $A = \mathrm{Diag}(\alpha_1, \alpha_2) \in \mathrm{Mat}(2 \times 2, K)$ gilt

$$\mu_A(t) \;=\; \begin{cases} t - \alpha & \text{für } \alpha_1 = \alpha_2 = \alpha, \\ (t - \alpha_1)(t - \alpha_2) & \text{für } \alpha_2 \neq \alpha_1. \end{cases}$$

Allgemeiner gilt für Blockdiagonalmatrizen:

Lemma 7.7. *Sei $n = n_1 + \cdots + n_k$, und seien $A_i \in \mathrm{Mat}(n_i \times n_i, K)$ gegeben. Für die Blockdiagonalmatrix*

$$A \;=\; \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_k \end{pmatrix} \;\in\; \mathrm{Mat}(n \times n, K)$$

gilt dann

$$\begin{aligned} \mu_A(t) \;&=\; \mathrm{kgV}(\mu_{A_1}(t), \ldots, \mu_{A_k}(t)), \\ \chi_A(t) \;&=\; \chi_{A_1}(t) \cdots \chi_{A_k}(t). \end{aligned}$$

Beweis. Für das charakteristische Polynom folgt das direkt aus der Multiplikativität der Determinante für Blockdiagonalmatrizen, wir müssen daher nur die Aussage über das Minimalpolynom zeigen. Dazu beachte man, dass sich die Potenzen von Blockdiagonalmatrizen berechnen als

$$A^i = \begin{pmatrix} A_1^i & & 0 \\ & \ddots & \\ 0 & & A_k^i \end{pmatrix}$$

für alle $i \in \mathbb{N}_0$. Für $P(t) \in K[t]$ folgt

$$P(A) = \begin{pmatrix} P(A_1) & & 0 \\ & \ddots & \\ 0 & & P(A_k) \end{pmatrix}$$

und wir erhalten aus der Definition des Minimalpolynoms:

$$\begin{aligned} P(A) = 0 &\iff \forall i \in \{1,\dots,k\} \colon P(A_i) = 0 \\ &\iff \forall i \in \{1,\dots,k\} \colon P(t) \text{ ist ein Vielfaches von } \mu_{A_i}(t) \\ &\iff P(t) \text{ ist ein Vielfaches von } \mathrm{kgV}(\mu_{A_1}(t),\dots,\mu_{A_k}(t)) \end{aligned}$$

Somit folgt die Behauptung. □

Um das Minimalpolynom einer Matrix in Jordan-Normalform abzulesen, müssen wir daher nur die Minimalpolynome von Jordanblöcken kennen. Diese sind leicht zu beschreiben:

Lemma 7.8. *Für einen Jordanblock $A = J_n(\lambda)$ der Länge n zum Eigenwert $\lambda \in K$ gilt*

$$\mu_A(t) = (t-\lambda)^n = \chi_A(t).$$

Beweis. Zu zeigen ist nur noch die Aussage über das Minimalpolynom. Wegen der Identität $J_n(\lambda) = J_n(0) + \lambda \cdot \mathbf{1}$ genügt es, den Spezialfall $\lambda = 0$ zu betrachten, denn der allgemeine Fall folgt dann sofort mittels der Variablensubstitution $t \mapsto t - \lambda$ wegen

$$Q(A - \lambda \cdot \mathbf{1}) = P(A) \quad \text{für} \quad Q(t) = P(t-\lambda).$$

Sei also ab jetzt $A = J_n(0)$. Für $i = 0, 1, \dots, n-1$ ist dann A^i die Matrix, deren einzige von Null verschiedene Einträge Einsen entlang der i-ten Nebendiagonalen sind. Die Matrizen $\mathbf{1}, A, A^2, \dots, A^{n-1}$ sind daher offensichtlich linear unabhängig, sodass also $\deg \mu_A(t) \geq n$ gelten muß. Wegen $A^n = 0$ folgt dann $\mu_A(t) = t^n$. □

Um das Minimalpolynom und das charakteristische Polynom von Matrizen durch ihre Jordan-Normalform auszudrücken, führen wir die folgende Notation ein: Für trigonalisierbare Matrizen $A \in \mathrm{Mat}(n \times n, K)$ sei

- $r(A,\lambda)$ die Länge des größten Jordan-Blocks zum Eigenwert λ,
- $d(A,\lambda)$ die Summe der Längen aller Jordan-Blöcke zum Eigenwert λ,

in der Jordan-Normalform von A. Dann gilt:

Korollar 7.9. *Für trigonalisierbare $A \in \mathrm{Mat}(n\times n,K)$ ist*

$$\mu_A(t) \;=\; \prod_\lambda (t-\lambda)^{r(A,\lambda)} \quad \textit{und} \quad \chi_A(t) \;=\; \prod_\lambda (t-\lambda)^{d(A,\lambda)}$$

Beweis. Für alle $S \in \mathrm{GL}_n(K)$ und $P \in K[t]$ gilt $P(S^{-1}\cdot A\cdot S) = S^{-1}\cdot P(A)\cdot S$, also haben ähnliche Matrizen dasselbe Minimalpolynom und dasselbe charakteristische Polynom. Es genügt daher, die Aussage für Matrizen A in Jordan-Normalform zu zeigen. Für diese folgt sie aber sofort aus den vorigen beiden Lemmata. □

Als unmittelbare Folgerung erhalten wir, dass das Minimalpolynom ein Teiler des charakteristischen Polynoms ist. Für diese letzte Aussage müssen wir uns nicht auf trigonalisierbare Matrizen beschränken:

Satz 7.10 (Cayley-Hamilton). *Für alle $A \in \mathrm{Mat}(n\times n,K)$ ist $\chi_A(A) = 0$.*

Beweis. Wenn wir K durch einen größeren Körper ersetzen, der ihn als Teilkörper enthält, dann ändert sich dabei weder das Polynom $\chi_A(t) = \det(t\cdot\mathbf{1}-A) \in K[t]$ noch die Matrix $\chi_A(A) \in \mathrm{Mat}(n\times n,K)$. In der Algebra zeigt man, dass jeder Körper K sich als Teilkörper eines algebraisch abgeschlossenen Körpers auffassen lässt. Wir dürfen daher annehmen, dass K algebraisch abgeschlossen ist.

Dann zerfällt $\chi_A(t)$ in $K[t]$ in Linearfaktoren und somit ist A trigonalisierbar. In diesem Fall folgt die Aussage sofort aus Korollar 7.9 wegen $r(A,\lambda) \le d(A,\lambda)$. □

Bemerkung 7.11. (a) Es gibt für den Satz von Cayley-Hamilton viele alternative Beweise, die ohne die Jordan-Normalform und ohne den algebraischen Abschluß auskommen. Wir haben also hier mehr Technik investiert als nötig — dafür aber einen sehr simplen Beweis erhalten, der keinerlei Ideen oder Tricks benötigt.

(b) Auf den ersten Blick möchte man den Satz von Cayley-Hamilton gerne in einer Zeile beweisen:

$$\chi_A(A) \;=\; \det(t\cdot\mathbf{1}-A)|_{t=A} \;\overset{?!}{=}\; \det(A\cdot\mathbf{1}-A) \;=\; \det(0) \;=\; 0$$

Die zweite Gleichung ist hier aber Unsinn, denn in $\chi_A(t) = \det(t\cdot\mathbf{1}-A)$ nimmt t die Rolle eines Skalars ein und steht in den Diagonaleinträgen. Mit dem Matrixprodukt hat die Notation $t\cdot\mathbf{1}$ nichts zu tun: Um in $\chi_A(t)$ eine Matrix einzusetzen, muß man zuerst $\det(t\cdot\mathbf{1}-A)$ als Polynom in t schreiben und dann die Potenzen von t durch Potenzen der Matrix ersetzen. Im Satz von Cayley-Hamilton steht auf der rechten Seite die Nullmatrix $0 \in \mathrm{Mat}(n\times n,K)$, nicht zu verwechseln mit dem Skalar $0 \in K$ auf der rechten Seite der obigen falschen Gleichungskette.

Die Nullstellen des charakteristischen Polynoms einer Matrix sind bekanntlich genau ihre Eigenwerte. Aus dem Satz von Cayley-Hamilton folgt, dass dasselbe auch für das Minimalpolynom gilt:

Korollar 7.12. *Sei $A \in \mathrm{Mat}(n \times n, K)$. Für $\lambda \in K$ gilt dann:*

$$\mu_A(\lambda) \;=\; 0 \quad \Longleftrightarrow \quad \chi_A(\lambda) \;=\; 0 \quad \Longleftrightarrow \quad \lambda \text{ ist ein Eigenwert von } A$$

Beweis. Aus dem Satz von Cayley-Hamilton folgt, dass jede Nullstelle von $\mu_A(t)$ auch eine Nullstelle von $\chi_A(t)$ und damit ein Eigenwert von A ist. Sei umgekehrt ein Eigenwert $\lambda \in K$ der Matrix A gegeben, und sei $v \in K^n \setminus \{0\}$ ein hierzu gehöriger Eigenvektor. Dann ist $A^i \cdot v = \lambda^i \cdot v$ für alle $i \in \mathbb{N}_0$, woraus

$$P(A) \cdot v \;=\; P(\lambda) \cdot v \quad \text{für alle} \quad P(t) \;\in\; K[t]$$

folgt. Indem wir dies speziell auf das Minimalpolynom $P(t) = \mu_A(t)$ anwenden, erhalten wir $\mu_A(\lambda) \cdot v = \mu_A(A) \cdot v = 0 \cdot v = 0$, also $\mu_A(\lambda) = 0$ wegen $v \neq 0$. □

Wir wissen bereits, dass ein Endomorphismus trigonalisierbar ist genau dann, wenn sein charakteristisches Polynom in Linearfaktoren zerfällt. Dasselbe gilt auch für das Minimalpolynom, und letzteres liefert zugleich sogar ein Kriterium für die Diagonalisierbarkeit ohne Bezug auf die Dimensionen der Eigenräume:

Satz 7.13. *Sei V ein endlich-dimensionaler Vektorraum über K und $f \in \mathrm{End}_K(V)$.*

a) f ist trigonalisierbar genau dann, wenn $\mu_f(t)$ über K in Linearfaktoren zerfällt.

b) f ist diagonalisierbar genau dann, wenn $\mu_f(t)$ über K in Linearfaktoren zerfällt und nur einfache Nullstellen besitzt.

Beweis. Die Richtung $\Longrightarrow$ ist in *a)* und *b)* klar. Für $\Longleftarrow$ nehmen wir an, $\mu_f(t)$ zerfalle in Linearfaktoren. Dann hat es insbesondere eine Nullstelle $\lambda \in K$. Nach Korollar 7.12 ist λ ein Eigenwert von f. Wir setzen $N = f - \lambda \cdot id_V$ und wählen $k \in \mathbb{N}$ so groß, dass

$$U \;:=\; \ker(N^k) \;=\; \ker(N^{k+1}) \;=\; \cdots \;=\; E_\infty(f, \lambda)$$

ist. Wie wir im Beweis der Hauptraumzerlegung gesehen haben, erhalten wir dann eine Zerlegung

$$V \;=\; U \oplus W \quad \text{mit} \quad W \;:=\; \mathrm{im}(N^k),$$

und beide Summanden in dieser Zerlegung sind f-invariante Unterräume. Wenn wir eine Basis in jedem Summanden wählen, erhalten wir durch Vereinigung der beiden Basen eine Basis von V und in dieser wird f durch eine Blockdiagonalmatrix dargestellt. Das Lemma 7.7 liefert somit

$$\mu_f(t) \;=\; \mathrm{kgV}(\mu_{f_U}(t), \mu_{f_W}(t)).$$

Wenn ein Polynom in Linearfaktoren zerfällt, so gilt dasselbe auch für alle seine Teiler. Mit $\mu_f(t)$ zerfallen somit nach der obigen Gleichung auch $\mu_{f_U}(t)$ und $\mu_{f_W}(t)$

in Linearfaktoren und sind per Induktion über die Dimension trigonalisierbar, was die Trigonalisierbarkeit von f impliziert. Die Aussage zur Diagonalisierbarkeit folgt ebenfalls per Induktion über die Dimension, denn nach der obigen Gleichung für Minimalpolynome gilt: Wenn $\mu_f(t)$ nur einfache Nullstellen besitzt, dann haben auch $\mu_{f_U}(t)$ und $\mu_{f_W}(t)$ nur einfache Nullstellen. □

8 Potenzreihen von Matrizen

Wir wissen bereits, wie man Potenzen von Jordan-Blöcken berechnet. Polynome von Jordan-Blöcken lassen sich bequem mit formalen Ableitungen hinschreiben:

Definition 8.1. Die *formale Ableitung* eines Polynoms $p(t) = \sum_{n=0}^{d} c_n t^n \in K[t]$ ist definiert als

$$\tfrac{d}{dt} p(t) \;:=\; \sum_{n=1}^{d} n \cdot c_n t^{n-1} \;\in\; K[t].$$

Für $i \in \mathbb{N}$ setzen wir

$$p^{(i)}(t) \;:=\; \left(\tfrac{d}{dt}\right)^i p(t) \;=\; \sum_{n=i}^{d} n(n-1)\cdots(n-i+1)\, c_n\, t^{n-i}$$

Lemma 8.2. *Sei K ein Körper mit $\mathbb{Q} \subset K$, und sei $A = J_n(\lambda)$ ein Jordanblock der Länge n zum Eigenwert $\lambda \in K$. Dann gilt für beliebige Polynome $p(t) \in K[t]$ die Formel*

$$p(A) \;=\; \begin{pmatrix} p(\lambda) & & & & \\ \frac{1}{1!}p'(\lambda) & p(\lambda) & & & \\ \frac{1}{2!}p''(\lambda) & \frac{1}{1!}p'(\lambda) & p(\lambda) & & \\ \vdots & \ddots & \ddots & \ddots & \\ \frac{1}{(n-1)!}p^{(n-1)}(\lambda) & \cdots & \frac{1}{2!}p''(\lambda) & \frac{1}{1!}p'(\lambda) & p(\lambda) \end{pmatrix}$$

Beweis. Die Einträge der Potenzen des Jordanblocks sind nach Lemma 6.4 von der Form

$$\tbinom{k}{i} \cdot \lambda^{k-i} \;=\; \tfrac{1}{i!} \cdot \left(\tfrac{d}{dt}\right)^i t^k|_{t=\lambda}$$

wobei die Division durch $i!$ in K möglich ist wegen $\mathbb{Q} \subset K$. □

Über $K = \mathbb{R}, \mathbb{C}$ lässt sich die Matrix im obigen Lemma auch für Potenzreihen $p(t)$ mit Konvergenzradius $R > 0$ lesen, sofern nur $|\lambda| < R$ ist: Denn für eine beliebige Potenzreihe

$$p(t) \;=\; \sum_{k=0}^{\infty} c_k t^i$$

mit dem Konvergenzradius $R > 0$ ist die zunächst als formale Potenzreihe definierte Ableitung

$$p'(t) \;=\; \sum_{k=1}^{\infty} k \cdot c_k \cdot t^{k-1}$$

nach einem Resultat der Analysis konvergent in jedem Punkt $t = \lambda \in \mathbb{C}$ mit $|\lambda| < R$.

Wir wollen dies nutzen, um Matrizen in konvergente Potenzreihen einsetzen zu können. Sei dazu $p(t) = \sum_{k=0}^{\infty} c_k t^k$ eine Potenzreihe mit Koeffizienten $c_i \in \mathbb{C}$ und mit Konvergenzradius $R > 0$. Für $N \in \mathbb{N}$ definieren wir ihre Partialsummen als die Polynome

$$p_N(t) \;:=\; \sum_{k=0}^{N} c_k t^k \;\in\; \mathbb{C}[t].$$

Sei $A \in \mathrm{Mat}(n \times n, \mathbb{C})$. Die Potenzreihe

$$p(A) \;=\; \sum_{k=0}^{\infty} c_k A^k$$

heißt *konvergent*, wenn die Folge der Matrixeinträge von $p_N(A) \in \mathrm{Mat}(n \times n, \mathbb{C})$ in jeder festen Zeile und Spalte für $N \to \infty$ gegen eine komplexe Zahl konvergiert. Wir schreiben dann $p(A)$ für die Matrix mit diesen Grenzwerten als Einträge.

Beispiel 8.3. Sei $A \in \mathrm{Mat}(n \times n, \mathbb{C})$ diagonalisierbar, es gebe also ein $S \in \mathrm{GL}_n(\mathbb{C})$ mit

$$A \;=\; SDS^{-1} \quad \text{für} \quad D \;=\; \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \quad \text{mit } \lambda_1, \ldots, \lambda_n \in \mathbb{C}.$$

Sei $p(t) = \sum_{k=0}^{\infty} c_k t^k$ eine Potenzreihe mit Konvergenzradius $R > 0$. Für $N \in \mathbb{N}$ ist offenbar

$$p_N(A) \;=\; p_N\big(SDS^{-1}\big) \;=\; S \cdot p_N(D) \cdot S^{-1} \;=\; S \cdot \mathrm{Diag}(p_N(\lambda_1), \ldots, p_N(\lambda_n)) \cdot S^{-1}$$

Für $R > \max_i |\lambda_i|$ konvergieren diese Matrizen für $N \to \infty$ und wir erhalten eine konvergente Matrixreihe mit Grenzwert

$$p(A) \;=\; S \cdot \mathrm{Diag}(p(\lambda_1), \ldots, p(\lambda_n)) \cdot S^{-1} \;\in\; \mathrm{Mat}(n \times n, \mathbb{C}).$$

Allgemeiner gilt:

Satz 8.4. *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{C})$ mit Eigenwerten $\lambda_i \in \mathbb{C}$, und sei $p(t) = \sum_{k=0}^{\infty} c_k t^k$ eine Potenzreihe mit dem Konvergenzradius $R > \max_i |\lambda_i|$. Dann konvergiert die Potenzreihe $p(A)$, und ihr Wert ist*

$$p(A) \;=\; \sum_{k=0}^{n-1} \tfrac{1}{k!}\, p^{(k)}(D) \cdot N^k \;\in\; \mathrm{Mat}(n \times n, \mathbb{C})$$

für die Jordan-Zerlegung $A = D+N$ mit D diagonalisierbar, N nilpotent, $DN = ND$.

Beweis. Wie im Beweis von Lemma 6.4 gilt

$$A^m \;=\; (D+N)^m \;=\; \sum_{k=0}^{m} \tbinom{m}{k}\, D^{m-k} N^k$$

Durch Linearkombination solcher Relationen folgt

$$q(D+N) \;=\; \sum_{k=0}^{d} \tfrac{1}{k!} q^{(k)}(D) \cdot N^k$$

für beliebige $q \in \mathbb{C}[t]$ vom Grad d. Dabei ist $N^k = 0$ für $k \geq n$. Indem wir dies auf die Partialsummen anwenden, folgt die behauptete Konvergenz und die Formel. □

Beispiel 8.5. In der Analysis zeigt man, dass die Exponentialreihe $\exp(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!}$ den Konvergenzradius unendlich besitzt. Nach dem obigen Satz ist somit für jede Matrix $A \in \mathrm{Mat}(n \times n, \mathbb{C})$ die Reihe

$$\exp(A) \;:=\; \sum_{k=0}^{\infty} \tfrac{1}{k!} A^k$$

konvergent gegen eine wohldefinierte Matrix $\exp(A) \in \mathrm{Mat}(n \times n, \mathbb{C})$. Wie in der Analysis zeigt man ferner

$$\exp(A) \cdot \exp(B) \;=\; \exp(A+B) \quad \text{für alle Matrizen } A, B \text{ mit } AB = BA.$$

Indem man speziell $B = -A$ wählt, sieht man, dass die Matrix $\exp(A)$ invertierbar ist mit der inversen Matrix $\exp(A)^{-1} = \exp(-A)$. Insbesondere erhalten wir durch Betrachten der skalaren Vielfachen einer gegebenen Matrix $A \in \mathrm{Mat}(n \times n, \mathbb{C})$ einen Homomorphismus

$$(\mathbb{C}, +) \;\longrightarrow\; \mathrm{GL}_n(\mathbb{C}), \quad t \;\mapsto\; \exp(tA)$$

von der additiven Gruppe der komplexen Zahlen in die multiplikative Gruppe aller invertierbaren Matrizen. Solche Homomorphismen spielen eine wichtige Rolle für die Klassifikation der Untergruppen von $\mathrm{GL}_n(\mathbb{C})$.

Zum Abschluß betrachten wir noch eine Anwendung aus der Analysis: Gesucht seien differenzierbare reelle Funktionen $f_1, \ldots, f_n : \mathbb{R} \longrightarrow \mathbb{R}$, deren Ableitungen das Gleichungssystem

$$\begin{aligned} f_1' &= a_{11}f_1 + \cdots + a_{1n}f_n \\ f_2' &= a_{21}f_1 + \cdots + a_{2n}f_n \\ &\vdots \\ f_n' &= a_{n1}f_1 + \cdots + a_{nn}f_n \end{aligned}$$

für gegebene $a_{ij} \in \mathbb{R}$ erfüllen. Gleichungen, die neben einer gesuchten Funktion auch ihre Ableitungen beinhalten, nennt man *Differentialgleichungen*; sie treten in vielen Anwendungen auf. Das obige System linearer Differentialgleichungen kann man kompakter schreiben in Vektorform

$$f' = A \cdot f \quad \text{für} \quad f = \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

mit der Matrix $A = (a_{ij}) \in \mathrm{Mat}(n \times n, \mathbb{R})$. Wir erhalten:

Satz 8.6. *Die Lösungen des obigen Systems linearer Differentialgleichungen sind genau die Funktionen*

$$f(t) = \exp(tA) \cdot c$$

wobei $c = f(0) \in \mathbb{R}^n$ ein beliebig wählbarer Vektor von Anfangswerten ist.

Beweis. Wir überlegen uns zunächst, dass die angegebenen Funktionen Lösungen der Differentialgleichungssystems bilden. Per Definition ist

$$\exp(tA) = \sum_{k=0}^{\infty} \tfrac{t^k}{k!} \cdot A^k$$

eine Matrix, deren Einträge Potenzreihen in t sind. Nach dem Satz 8.4 konvergieren diese Potenzreihen für alle $t \in \mathbb{R}$. Aus der Analysis wissen wir, dass solche überall konvergenten Potenzreihen differenzierbare Funktionen sind, deren Ableitung sich gliedweise berechnen lässt. Wenn wir die Ableitung einer Matrix $G(t) = (g_{ij}(t))$ von Funktionen definieren als die Matrix $\frac{d}{dt}G(t) = (g_{ij}'(t))$, erhalten wir für die Exponentialreihe

$$\tfrac{d}{dt}\exp(tA) = \tfrac{d}{dt}\sum_{k=0}^{\infty} \tfrac{t^k}{k!} \cdot A^k = \sum_{k=1}^{\infty} \tfrac{k \cdot t^{k-1}}{k!} \cdot A^k = A \cdot \sum_{k=1}^{\infty} \tfrac{t^{k-1}}{(k-1)!} \cdot A^{k-1} = A \cdot \exp(tA).$$

Für jedes $c \in \mathbb{R}^n$ ist der Funktionenvektor $f(t) = \exp(tA) \cdot c$ eine Linearkombination der Spalten der Matrix $\exp(tA)$ und erfüllt daher ebenso wie die gesamte Matrix das Differentialgleichungssystem $f'(t) = A \cdot f(t)$.

Sei umgekehrt eine beliebige Lösung $f(t)$ gegeben. Für $g(t) = \exp(-tA) \cdot f(t)$ gilt dann

$$\tfrac{d}{dt}g(t) = \tfrac{d}{dt}(\exp(-tA)) \cdot f(t) + \exp(-tA) \cdot \tfrac{d}{dt}f(t) = -A \cdot g(t) + A \cdot g(t) = 0.$$

Da dies für alle $t \in \mathbb{R}$ gilt, müssen die Einträge des Vektors $g(t)$ konstant sein, es gibt also ein $c \in \mathbb{R}^n$ mit $g(t) = c$ für alle $t \in \mathbb{R}$. Damit folgt $f(t) = \exp(tA) \cdot c$. □

Bemerkung 8.7. Für näherungsweise numerische Berechnungen sollte man *nicht* die Jordan-Normalform verwenden, denn sie ist numerisch instabil: Kleine Fehler in einer Matrix können große Änderungen in ihrer Jordan-Normalform zur Folge haben. Man vergleiche etwa die Jordan-Normalform von

$$\begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \lambda & 0 \\ 1 & \lambda + \varepsilon \end{pmatrix}$$

für beliebig kleine, aber von Null verschiedene Fehler $\varepsilon \in \mathbb{C} \setminus \{0\}$!

Kapitel II
Euklidische und unitäre Vektorräume

Zusammenfassung In diesem Kapitel betrachten wir Vektorräume über $\mathbb{R}$ und $\mathbb{C}$ mit einem Skalarprodukt, das es erlaubt, Längen und im reellen Fall auch Winkel zu messen. Wir werden Bilinear- und Sesquilinearformen durch Matrizen beschreiben und im positiv definiten Fall Orthonormalbasen konstruieren. Lineare Abbildungen, die das Skalarprodukt erhalten, heißen orthogonale bzw. unitäre. Hauptziel dieses Kapitels ist der Spektralsatz, ein Kriterium für die Diagonalisierbarkeit einer Matrix durch orthogonale bzw. unitäre Basiswechsel. Als Anwendungen erhalten wir die Hauptachsentransformation, den Satz von Sylvester und die Singulärwertzerlegung.

1 Bilinear- und Sesquilinearformen

Bisher haben wir meist Vektorräume über beliebigen Körpern betrachtet, in diesem Kapitel soll es speziell um reelle und komplexe Vektorräume gehen. Die metrische Struktur auf den reellen Zahlen erlaubt es hier, Längen und Winkel zu messen:

Beispiel 1.1. Die *Länge* $\|v\| \in \mathbb{R}_{\geq 0}$ eines Vektors $v = (v_1, v_2)^t \in \mathbb{R}^2$ in der Ebene ist nach Pythagoras

$$\|v\| \;=\; \sqrt{v_1^2 + v_2^2}$$

Den *Winkel* $\gamma \in \mathbb{R}/2\pi\mathbb{Z}$ zwischen zwei Vektoren $v = (v_1, v_2)^{\mathsf{t}}, w = (w_1, w_2)^{\mathsf{t}} \in \mathbb{R}^2$ kann man aus ihren Koordinaten leicht berechnen: Wir schreiben die Koordinaten als

$$\begin{aligned} v_1 &= \|v\|\cos(\alpha), & w_1 &= \|w\|\cos(\beta), \\ v_2 &= \|v\|\sin(\alpha), & w_2 &= \|w\|\sin(\beta), \end{aligned}$$

Den gesuchten Winkel $\gamma = \beta - \alpha$ erhalten wir nach dem Additionstheorem aus

$$\|v\| \cdot \|w\| \cdot \cos(\gamma) \;=\; \|v\| \cdot \|w\| \cdot (\cos(\alpha)\cos(\beta) + \sin(\alpha)\sin(\beta)) \;=\; v_1 w_1 + v_2 w_2.$$

Den Ausdruck auf der rechten Seite nennen wir das *Skalarprodukt* von v und w und schreiben kurz $\langle v,w\rangle := v_1w_1 + v_2w_2$, wenn keine Verwechslungsgefahr mit der linearen Hülle von zwei Vektoren besteht. Im Fall $\|w\| = 1$ ist $\langle v,w\rangle$ die Länge des Vektors, den man durch Orthogonalprojektion von v auf die reelle Gerade $\mathbb{R}w$ erhält. Allgemein hängt $\langle v,w\rangle$ linear von jedem der Vektoren v,w ab, wenn der je andere Vektor festgehalten wird. Die Länge eines Vektors ergibt sich aus $\|v\|^2 = \langle v,v\rangle$. Für die Länge von $v-w$ erhalten wir den Cosinussatz:

$$\begin{aligned}\|v-w\|^2 \;&=\; \langle v-w, v-w\rangle \;=\; \langle v,v\rangle - \langle v,w\rangle - \langle w,v\rangle + \langle w,w\rangle \\ &=\; \|v\|^2 + \|w\|^2 - 2\,\|v\|\cdot\|w\|\cdot\cos(\gamma)\end{aligned}$$

Beispiel 1.2. Analog ist die Länge $\|v\| \in \mathbb{R}_{\geq 0}$ eines Vektors $v = (v_1,v_2,v_3) \in \mathbb{R}^3$ nach Pythagoras

$$\|v\| \;=\; \sqrt{v_1^2+v_2^2+v_3^2}$$

Den Winkel $\gamma \in \mathbb{R}/2\pi\mathbb{Z}$ zwischen Vektoren $v = (v_1,v_2,v_3), w = (w_1,w_2,w_3) \in \mathbb{R}^3$ können wir berechnen, indem wir den Cosinussatz anwenden in der von den beiden Vektoren aufgespannten Ebene:

$$\|v\|\cdot\|w\|\cdot\cos(\gamma) \;=\; \frac{\|v\|^2+\|w\|^2-\|v-w\|^2}{2} \;=\; v_1w_1+v_2w_2+v_3w_3.$$

Allgemein machen wir folgende

Definition 1.3. Sei $n \in \mathbb{N}$. Das *Standard-Skalarprodukt* auf dem Vektorraum $\mathbb{R}^n$ ist definiert durch

$$\langle\cdot,\cdot\rangle: \quad \mathbb{R}^n\times\mathbb{R}^n \;\longrightarrow\; \mathbb{R}, \quad \langle v,w\rangle \;:=\; \sum_{i=1}^{n} v_i\cdot w_i.$$

Die *Länge* oder *Norm* von $v \in \mathbb{R}^n$ ist definiert als $\|v\| := \sqrt{\langle v,v\rangle} \in \mathbb{R}_{\geq 0}$.

Für komplexe Vektorräume sollten wir die Definition modifizieren. Das sieht man bereits im Fall $n = 1$, denn den Absolutbetrag einer komplexen Zahl $z \in \mathbb{C}$ erhält man nicht durch Quadrieren von z, sondern durch $|z|^2 = \overline{z}\cdot z$. Wir machen daher die

Definition 1.4. Sei $n \in \mathbb{N}$. Das *Standard-Skalarprodukt* auf dem Vektorraum $\mathbb{C}^n$ ist definiert durch

$$\langle\cdot,\cdot\rangle: \quad \mathbb{C}^n\times\mathbb{C}^n \;\longrightarrow\; \mathbb{C}, \quad \langle v,w\rangle \;:=\; \sum_{i=1}^{n} \overline{v}_i\cdot w_i.$$

Der *Länge* oder die *Norm* von $v \in \mathbb{C}^n$ ist definiert als $\|v\| := \sqrt{\langle v,v\rangle} \in \mathbb{R}_{\geq 0}$.

Um den reellen und den komplexen Fall gleichzeitig zu behandeln und nicht von der Wahl einer Basis abzuhängen, arbeiten wir in folgendem abstrakten Rahmen:

Definition 1.5. Im Folgenden sei K ein Körper und $\sigma : K \to K, a \mapsto \overline{a}$ ein gegebener Körperautomorphismus; man denke an die reellen oder komplexen Zahlen mit der komplexen Konjugation. Eine *Sesquilinearform* auf einem K-Vektorraum V ist eine Abbildung

$$\langle \cdot, \cdot \rangle : \quad V \times V \longrightarrow K, \quad (v,w) \mapsto \langle v,w \rangle,$$

sodass für alle $a,b \in K$ und alle $u,v,w \in V$ gilt:

$$\begin{aligned} \langle u + av, w \rangle &= \langle u,w \rangle + \overline{a} \langle v,w \rangle, \\ \langle u, v + aw \rangle &= \langle u,v \rangle + a \langle u,w \rangle. \end{aligned}$$

Das Präfix *sesqui-* ist lateinisch für anderthalb: "Halb linear" in der ersten und linear in der zweiten Variablen. Man beachte aber, dass der Spezialfall $\sigma = id$ durchaus erlaubt ist; in diesem Spezialfall nennen wir $\langle \cdot, \cdot \rangle$ eine *Bilinearform*. Da wir den Spezialfall $\sigma = id$ erlauben, werden wir unter dem Begriff einer Sesquilinearform den Fall einer Bilinearform stets mit behandeln.

Nach Wahl einer Basis können wir Sesquilinearformen konkret angeben durch quadratische Matrizen:

Definition 1.6. Wie zuvor bezeichnen wir mit $\sigma : K \to K, a \mapsto \overline{a}$ einen gegebenen Körperautomorphismus. Die durch Anwenden dieses Automorphismus auf jeden der Einträge einer Matrix $A = (a_{ij}) \in \mathrm{Mat}(m \times n, K)$ erhaltene Matrix bezeichnen wir mit $\overline{A} = (\overline{a_{ij}})$. Insbesondere setzen wir

$$\overline{v} := \begin{pmatrix} \overline{v}_1 \\ \vdots \\ \overline{v}_n \end{pmatrix} \in K^n \quad \text{für} \quad w = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$$

Für Matrizen $A \in \mathrm{Mat}(n \times n, K)$ betrachten wir auf dem Standardvektorraum $V = K^n$ die Paarung

$$V \times V \longrightarrow K, \quad (v,w) \mapsto \langle v,w \rangle_A := \overline{v}^{\mathrm{t}} \cdot A \cdot w.$$

Konkret in Koordinaten ausgeschrieben für $v^{\mathrm{t}} = (v_1, \ldots, v_n), w^{\mathrm{t}} = (w_1, \ldots, w_n) \in K^n$ und $A = (a_{ij})$ erhalten wir

$$\langle v,w \rangle_A = \overline{v}^{\mathrm{t}} \cdot A \cdot w = \left(\overline{v}_1, \ldots, \overline{v}_n\right) \cdot \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \sum_{i,j=1}^{n} a_{ij} \cdot \overline{v}_i \cdot w_j.$$

Wenn wir $A = \mathbf{1}$ wählen, ist dies genau das Standard-Skalarprodukt über den reellen bzw. den komplexen Zahlen. Allgemein gilt:

Proposition 1.7 (Sesquilinearformen und Matrizen). *Für alle $A \in \mathrm{Mat}(n \times n, K)$ ist die Abbildung*

$$\langle \cdot, \cdot \rangle_A : \quad K^n \times K^n \longrightarrow K, \quad (v, w) \mapsto \overline{v}^{\mathrm{t}} \cdot A \cdot w$$

eine Sesquilinearform. Umgekehrt hat jede Sesquilinearform $\langle \cdot, \cdot \rangle : K^n \times K^n \to K$ diese Form für genau eine Matrix $A = (a_{ij}) \in \mathrm{Mat}(n \times n, K)$. Die Einträge dieser Matrix sind gegeben durch

$$a_{ij} = \langle e_i, e_j \rangle.$$

Beweis. Dass für jede Matrix $A \in \mathrm{Mat}(n \times n, K)$ die Abbildung $(v, w) \mapsto \overline{v}^{\mathrm{t}} \cdot A \cdot w$ eine Sesquilinearform ist, folgt aus den Rechenregeln für das Matrizenprodukt. Um zu sehen, dass man jede Sesquilinearform auf $V = K^n$ so erhält, sei eine beliebige Sesquilinearform $\langle \cdot, \cdot \rangle : V \times V \to K$ gegeben. Der Wert der Sesquilinearform auf einem beliebigen Paar von Vektoren $x = x_1 e_1 + \cdots + x_n e_n$ und $y = y_1 e_1 + \cdots + y_n e_n$ ist per Sesquilinearität

$$\begin{aligned} \langle x, y \rangle = \langle x_1 e_1 + \cdots + x_n e_n, y \rangle &= \sum_{i=1}^{n} \overline{x}_i \cdot \langle e_i, y \rangle \\ &= \sum_{i=1}^{n} \overline{x}_i \cdot \langle e_i, y_1 e_1 + \cdots + y_n e_n \rangle \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{x}_i \cdot y_j \cdot \langle e_i, e_j \rangle = \langle x, y \rangle_A \end{aligned}$$

für die Matrix $A = (a_{ij})$ mit den Einträgen $a_{ij} = \langle e_i, e_j \rangle$. □

Korollar 1.8. *Sei V ein endlich-dimensionaler K-Vektorraum. Sei $\mathscr{B} = (v_1, \ldots, v_n)$ eine Basis und*

$$\Phi : \quad K^n \xrightarrow{\sim} V, \quad (a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i v_i$$

der zugehörige Isomorphismus. Für $\Psi = \Phi^{-1}$ sind die Sesquilinearformen auf V genau die Abbildungen

$$\langle \cdot, \cdot \rangle : \quad V \times V \longrightarrow K, \quad (v, w) \mapsto \langle \Psi(v), \Psi(w) \rangle_A$$

mit $A \in \mathrm{Mat}(n \times n, K)$. Dabei ist die Matrix $A = (a_{ij})$ eindeutig durch die Werte der Sesquilinearform auf den Paaren von Basisvektoren bestimmt, es gilt $a_{ij} = \langle v_i, v_j \rangle$.

Beweis. Das Diagramm

$$\begin{array}{ccc} V \times V & \xrightarrow{\langle \cdot, \cdot \rangle} & K \\ {\scriptstyle \Psi \times \Psi}\downarrow & & \| \\ K^n \times K^n & \longrightarrow & K \end{array}$$

liefert eine Bijektion zwischen Sesquilinearformen auf V und auf K^n. Man wende nun die vorige Proposition 1.7 auf die untere Zeile an. □

Definition 1.9. Sei $\mathscr{B} = (v_1, \ldots, v_n)$ eine Basis des Vektorraumes V über K. Für Sesquilinearformen

$$\langle \cdot, \cdot \rangle : V \times V \longrightarrow K$$

bezeichnen wir die im vorigen Korollar auftretende Matrix

$$A := \mathrm{Gram}_{\mathscr{B}} \langle \cdot, \cdot \rangle = \begin{pmatrix} \langle v_1, v_1 \rangle & \cdots & \langle v_1, v_n \rangle \\ \vdots & & \vdots \\ \langle v_n, v_1 \rangle & \cdots & \langle v_n, v_n \rangle \end{pmatrix} \in \mathrm{Mat}(n \times n, K)$$

als die *Gram'sche Matrix* der Sesquilinearform bezüglich der Basis $\mathscr{B}$.

Gram'sche Matrizen stellen also Sesquilinearformen in Koordinaten dar, ähnlich wie wir lineare Abbildungen durch Matrizen beschrieben hatten. Man beachte aber, dass sich die Gram'sche Matrix einer Sesquilinearform unter Basiswechsel anders transformiert als Abbildungsmatrizen:

Proposition 1.10 (Transformation von Gram-Matrizen). *Sei V ein K-Vektorraum endlicher Dimension und*

$$\langle \cdot, \cdot \rangle : \quad V \times V \longrightarrow K.$$

eine Sesquilinearform mit Gram-Matrizen

- $A = \mathrm{Gram}_{\mathscr{A}} \langle \cdot, \cdot \rangle$ *bezüglich einer Basis* $\mathscr{A} = (v_1, \ldots, v_n)$,
- $B = \mathrm{Gram}_{\mathscr{B}} \langle \cdot, \cdot \rangle$ *bezüglich einer Basis* $\mathscr{B} = (w_1, \ldots, w_n)$.

Dann gilt $B = \overline{S}^{\mathsf{t}} \cdot A \cdot S$ für den Basiswechsel $S = (s_{ki}) \in \mathrm{GL}_n(K)$ mit $w_i = \sum_{k=1}^n s_{ki} v_k$.

Beweis. Wir schreiben $A = (a_{ij})$ und $B = (b_{ij})$. Dann gilt

$$\begin{aligned} b_{ij} = \langle w_i, w_j \rangle = \langle Sv_i, Sv_j \rangle = \Big\langle \sum_{k=1}^n s_{ki} v_k, \sum_{l=1}^n s_{lj} v_l \Big\rangle &= \sum_{k,l=1}^n \overline{s}_{ki} \cdot s_{lj} \cdot \langle v_k, v_l \rangle \\ &= \sum_{k,l=1}^n \overline{s}_{ki} \cdot a_{kl} \cdot s_{lj}. \end{aligned}$$

Die Summe auf der rechten Seite ist genau der (i,j)-Eintrag der Matrix $\overline{S}^{\mathsf{t}} A S$. □

Definition 1.11. Die *adjungierte Matrix* von $S = (s_{ij}) \in \mathrm{Mat}(n \times n, K)$ ist definiert als die Matrix

$$S^\dagger := \overline{S}^{\mathsf{t}} = (\overline{s}_{ji}) \in \mathrm{Mat}(n \times n, K),$$

also die Matrix, die man erhält, indem man die gegebene Matrix S transponiert und zusätzlich alle ihre Einträge konjugiert. Achtung: Diese hat nichts zu tun mit der in der Cramer'schen Formel auftretenden komplementären Matrix, auch wenn in der Literatur leider die Bezeichnungen nicht einheitlich verwendet werden!

Wir fassen als Slogan zusammen: Unter einem Basiswechsel $S \in \mathrm{GL}_n(K)$ gilt die Transformationsregel

- $B = S^{-1}AS$ für Abbildungsmatrizen A, B von Endomorphismen,
- $B = S^{\mathrm{t}}AS$ für Gram-Matrizen A, B von Bilinearformen.
- $B = S^{\dagger}AS$ für Gram-Matrizen A, B von Sesquilinearformen,

Wie für Endomorphismen stellt sich auch für Bilinear- oder Sesquilinearformen die Frage, welche Basiswechsel sie in die einfachste Form bringen. Wir werden dies später für Bilinear- und Sesquilinearformen mit einigen zusätzlichen Eigenschaften beantworten. Insbesondere werden wir die folgende Symmetrieeigenschaft fordern, die für das Standard-Skalarprodukt auf $\mathbb{R}^n$ und $\mathbb{C}^n$ gilt:

Definition 1.12. Sei V ein K-Vektorraum.

a) Eine Bilinearform $\langle \cdot, \cdot \rangle : V \times V \longrightarrow K$ heißt *symmetrisch*, falls für alle $v, w \in V$ gilt:
$$\langle v, w \rangle \;=\; \langle w, v \rangle$$

b) Wir nehmen nun an, dass $\sigma^2 = id_K$ für den Automorphismus $\sigma : K \to K, a \mapsto \overline{a}$ gilt. Eine Sesquilinearform $\langle \cdot, \cdot \rangle : V \times V \longrightarrow K$ heißt *hermitesch*, falls für alle Vektoren $v, w \in V$ gilt:
$$\langle v, w \rangle \;=\; \overline{\langle w, v \rangle}$$

Der Begriff Sesquilinearform schließt weiterhin den Fall von Bilinearformen mit ein; symmetrische Bilinearformen sind folglich ein Spezialfall von hermiteschen Sesquilinearformen. Der Klarheit halber werden wir die zentralen Resultate aber in beiden Fällen explizit formulieren und nur in den Beweisen die Arbeit halbieren.

Beispiel 1.13. Es gilt:

a) Für $a, b, c, d \in \mathbb{R}$ wird auf $V = \mathbb{R}^2$ durch
$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \;=\; ax_1y_1 + bx_1y_2 + cx_2y_1 + dx_2y_2$$
eine Bilinearform definiert. Diese ist symmetrisch genau für $b = c$.

b) Für $a, b, c, d \in \mathbb{C}$ wird auf $V = \mathbb{C}^2$ durch
$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \;=\; a\overline{x}_1y_1 + b\overline{x}_1y_2 + c\overline{x}_2y_1 + d\overline{x}_2y_2$$
eine Sesquilinearform definiert. Diese ist hermitesch genau für $a, d \in \mathbb{R}$, $c = \overline{b}$.

Allgemeiner kann man aus der Gram-Matrix einer Bilinear- oder Sesquilinearform leicht ablesen, ob diese symmetrisch bzw. hermitesch ist:

Lemma 1.14. *Sei V ein endlich-dimensionaler Vektorraum über K, und sei $\mathscr{B}$ eine beliebige Basis des Vektorraumes. Dann gilt:*

a) Eine Bilinearform $\langle\cdot,\cdot\rangle : V \times V \longrightarrow K$ mit der Gram-Matrix $A = \mathrm{Gram}_{\mathscr{B}}\langle\cdot,\cdot\rangle$ ist symmetrisch genau für

$$A^{\mathsf{t}} = A.$$

b) Eine Sesquilinearform $\langle\cdot,\cdot\rangle : V \times V \longrightarrow K$ mit der Gram-Matrix $A = \mathrm{Gram}_{\mathscr{B}}\langle\cdot,\cdot\rangle$ ist hermitesch genau für

$$A^{\dagger} = A.$$

Beweis. Sei $\mathscr{B} = (v_1, \ldots, v_n)$ eine Basis. Wir zeigen b): Wenn $\langle\cdot,\cdot\rangle$ hermitesch ist, gilt insbesondere

$$\langle v_i, v_j\rangle = \overline{\langle v_j, v_i\rangle}$$

für alle i, j. Links stehen per Definition die Einträge der Gram-Matrix $A = (a_{ij})$, diese erfüllen also $a_{ij} = \overline{a}_{ji}$ und somit folgt $A^{\dagger} = A$. Sei nun umgekehrt diese letzte Gleichung vorausgesetzt. Dann ist die Sesquilinearform

$$\langle\cdot,\cdot\rangle_A : \quad K^n \times K^n \longrightarrow K, \quad (v, w) \mapsto \overline{v}^{\mathsf{t}} \cdot A \cdot w$$

hermitesch, denn für beliebige Vektoren $v, w \in K^n$ gilt:

$$\begin{aligned}
\langle w, v\rangle_A &:= \overline{w}^{\mathsf{t}} \cdot A \cdot v && \text{per Definition}\\
&= \overline{w}^{\mathsf{t}} \cdot A^{\dagger} \cdot v && \text{nach unserer Annahme } A^{\dagger} = A\\
&= \overline{w}^{\mathsf{t}} \cdot \overline{A}^{\mathsf{t}} \cdot \overline{\overline{v}} && \text{da } v = \overline{\overline{v}} \text{ wegen } \sigma^2 = id\\
&= \overline{w^{\mathsf{t}} \cdot A^{\mathsf{t}} \cdot \overline{v}} && \text{da } \sigma \text{ ein Körperhomomorphismus}\\
&= \overline{(\overline{v}^{\mathsf{t}} \cdot A \cdot w)^{\mathsf{t}}} && \text{da } X^{\mathsf{t}} \cdot Y^{\mathsf{t}} = (Y \cdot X)^{\mathsf{t}} \text{ für Matrizen } X, Y\\
&= \overline{\overline{v}^{\mathsf{t}} \cdot A \cdot w} && \text{da } \alpha^{\mathsf{t}} = \alpha \text{ für } 1 \times 1 \text{ Matrizen } \alpha\\
&= \overline{\langle v, w\rangle_A} && \text{per Definition}
\end{aligned}$$

Wegen $\langle\cdot,\cdot\rangle = \langle\Psi(\cdot), \Psi(\cdot)\rangle_A$ für den Isomorphismus $\Psi = \Phi_{\mathscr{B}}^{-1} : V \xrightarrow{\sim} K^n$ ist dann auch die gegebene Sesquilinearform $\langle\cdot,\cdot\rangle$ hermitesch. □

Definition 1.15. Eine Matrix $A \in \mathrm{Mat}(n \times n, K)$ heißt

a) *symmetrisch*, falls $A^{\mathsf{t}} = A$ ist,

b) *hermitesch*, falls $A^{\dagger} = A$ ist,

Wir können das Lemma 1.14 also zusammenfassen in der Aussage: Eine Bilinear- bzw. Sesquilinearform ist symmetrisch bzw. hermitesch genau dann, wenn ihre Gram-Matrix zu einer beliebigen Basis symmetrisch bzw. hermitesch ist.

Beispiel 1.16. Für $a, b, c, d \in \mathbb{C}$ betrachten wir auf $V = \mathbb{C}^2$ wie in Beispiel 1.13 die Sesquilinearform

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle = a\overline{x}_1 y_1 + b\overline{x}_1 y_2 + c\overline{x}_2 y_1 + d\overline{x}_2 y_2.$$

Ihre Gram-Matrix zur Standardbasis ist

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{mit der adjungierten Matrix} \quad A^\dagger = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}.$$

Wie erwartet ist diese Matrix hermitesch genau dann, wenn $a, d \in \mathbb{R}$ und $c = \overline{b}$ ist.

2 Skalarprodukte und Normen

Die Definition einer symmetrischen Bilinearform ergibt über beliebigen Körpern Sinn. Im Folgenden wollen wir Skalarprodukte zur Längen- und Winkelmessung benutzen; hierzu benötigen wir die metrische Struktur auf den reellen Zahlen und betrachten daher ausschließlich reelle und komplexe Vektorräume. Wir beginnen mit dem reellen Fall:

Definition 2.1. Sei V ein $\mathbb{R}$-Vektorraum. Eine Bilinearform $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ heißt

a) *positiv definit*, falls $\langle v, v \rangle > 0$ für alle $v \in V \setminus \{0\}$ ist.

b) *negativ definit*, falls $\langle v, v \rangle < 0$ für alle $v \in V \setminus \{0\}$ ist.

c) *positiv semidefinit*, falls $\langle v, v \rangle \geq 0$ für alle $v \in V$ ist.

d) *negativ semidefinit*, falls $\langle v, v \rangle \leq 0$ für alle $v \in V$ ist.

Eine Matrix $A \in \mathrm{Mat}(n \times n, \mathbb{R})$ heißt *positiv definit*, falls die Bilinearform $\langle \cdot, \cdot \rangle_A$ diese Eigenschaft besitzt; analog für die übrigen der genannten Eigenschaften.

Wenn man diese Definition auf Sesquiliearformen verallgemeinern will, sollte man beachten, dass diese komplexe Werte annehmen und dass sich der Körper $\mathbb{C}$ wegen $i^2 = -1$ nicht anordnen lässt. Für *hermitesche* Sesquilinearformen ist das aber zum Glück kein Problem – wobei wir ab jetzt mit Sesquilinearformen immer solche bezüglich der komplexen Konjugation meinen:

Bemerkung 2.2. Sei $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ eine hermitesche Sesquilinearform auf einem komplexen Vektorraum. Dann gilt

$$\langle v, v \rangle \in \mathbb{R} \quad \text{für alle} \quad v \in V.$$

Beweis. Für alle $v, w \in V$ gilt per Definition von "hermitesch" $\langle v, w \rangle = \overline{\langle w, v \rangle}$. Wenn wir $w = v$ wählen, folgt die Behauptung. □

Da für hermitesche Formen die Werte $\langle v, v \rangle$ reell sind, können wir die vorige Definition vom reellen direkt zum komplexen Fall übertragen:

Definition 2.3. Sei V ein $\mathbb{C}$-Vektorraum. Eine hermitesche Form $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ heißt

a) *positiv definit*, falls $\langle v,v\rangle > 0$ für alle $v \in V \setminus \{0\}$ ist.

b) *negativ definit*, falls $\langle v,v\rangle < 0$ für alle $v \in V \setminus \{0\}$ ist.

c) *positiv semidefinit*, falls $\langle v,v\rangle \geq 0$ für alle $v \in V$ ist.

d) *negativ semidefinit*, falls $\langle v,v\rangle \leq 0$ für alle $v \in V$ ist.

Eine Matrix $A \in \mathrm{Mat}(n\times n,\mathbb{C})$ heißt *positiv definit*, falls die hermitesche Form $\langle\cdot,\cdot\rangle_A$ diese Eigenschaft besitzt; analog für die übrigen der genannten Eigenschaften.

Um Schreibarbeit zu sparen, vereinbaren wir für den Rest dieses Kapitels, dass die Notation $\mathbb{K}$ immer für einen der Körper $\mathbb{R}$ oder $\mathbb{C}$ steht. Wir werden weiterhin beide Fälle möglichst parallel behandeln:

Definition 2.4. Sei V ein Vektorraum über $\mathbb{K}$. Unter einem *Skalarprodukt* auf V verstehen wir

a) im Fall $\mathbb{K} = \mathbb{R}$ eine positiv definite symmetrische Bilinearform $V \times V \to \mathbb{R}$,

b) im Fall $\mathbb{K} = \mathbb{C}$ eine positiv definite hermitesche Sesquilinearform $V \times V \to \mathbb{C}$.

Einen $\mathbb{K}$-Vektorraum zusammen mit einem Skalarprodukt $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{K}$ nennt man

a) im Fall $\mathbb{K} = \mathbb{R}$ einen *Euklidischen Raum*,

b) im Fall $\mathbb{K} = \mathbb{C}$ einen *unitären Raum*.

Die *Länge* oder *Norm* eines Vektors $v \in V$ bezüglich des Skalarproduktes ist dann definiert als

$$\|v\| \;:=\; \sqrt{\langle v,v\rangle} \;\in\; \mathbb{R}_{\geq 0}.$$

Ein Vektor $v \in V$ heißt ein *Einheitsvektor* oder *normiert*, wenn $\|v\| = 1$ ist.

Beispiel 2.5. Es gilt:

a) Auf $V = \mathbb{K}^n$ ist das Standard-Skalarprodukt $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{K}, (v,w) \mapsto \overline{v}^{\mathsf{t}} \cdot w$ ein Skalarprodukt: Es ist

$$\langle v,v\rangle \;=\; \sum_{i=1}^{n} \overline{v}_i \cdot v_i \;=\; \sum_{i=1}^{n} |v_i|^2 \;\geq\; 0 \quad \text{für} \quad v \;=\; \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

und Gleichheit kann offenbar nur dann gelten, wenn $v_1 = \cdots = v_n = 0$ ist.

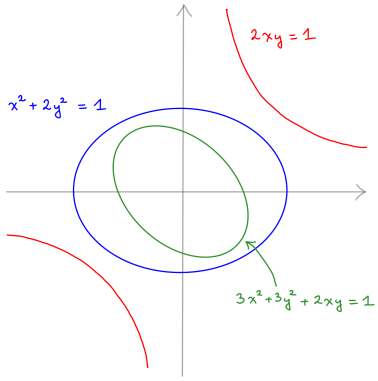
b) Auf der reellen Ebene $V = \mathbb{R}^2$ ist

$$V \times V \;\to\; \mathbb{R}, \quad (v,w) \;\mapsto\; v_1w_1 + 2v_2w_2 \qquad \text{ein Skalarprodukt,}$$

$$V \times V \;\to\; \mathbb{R}, \quad (v,w) \;\mapsto\; 3v_1w_1 + v_1w_2 + v_2w_1 + 3v_2w_2 \qquad \text{ein Skalarprodukt,}$$

$$V \times V \;\to\; \mathbb{R}, \quad (v,w) \;\mapsto\; v_1w_2 + v_2w_1 \qquad \text{kein Skalarprodukt.}$$

Die folgende Abbildung zeigt jeweils die Menge aller Vektoren v mit $\|v\| = 1$; es handelt sich hierbei um sogenannte *Quadriken*, also die Lösungsmengen einer quadratischen Gleichung in mehreren Variablen:



c) Auf dem reellen Vektorraum $V = C([0,1])$ der stetigen Funktionen $f : [0,1] \to \mathbb{R}$ wird durch

$$\langle f, g \rangle \;:=\; \int_0^1 f(x)g(x)dx$$

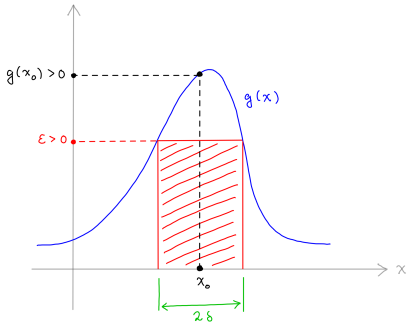
ein Skalarprodukt definiert: Die Bilinearität und Symmetrie sind klar, für die positive Definitheit beachte man

$$\langle f, f \rangle \;=\; \int_0^1 f(x)^2 dx \;\geq\; 0,$$

wobei Gleichheit nur für die Nullfunktion gilt: Wenn ein $x_0 \in [0,1]$ existiert mit $f(x_0) \neq 0$, können wir wegen der vorausgesetzten Stetigkeit der Funktion positive Zahlen $\varepsilon, \delta > 0$ finden mit der Eigenschaft, dass $[x_0 - \delta, x_0 + \delta] \subseteq [0,1]$ und

$$f(x)^2 \;>\; \varepsilon \quad \text{für alle} \quad x \;\in\; [x_0 - \delta, x_0 + \delta]$$

ist, und dann gilt die Abschätzung $\|f\|^2 \geq 2\varepsilon\delta > 0$.



Anders als das Skalarprodukt ist die zugehörige Norm eine Funktion in nur *einer* Variablen und lässt sich daher leichter visualisieren. Aus der Norm lässt sich das Skalarprodukt leicht rekonstruieren:

Lemma 2.6 (Polarisationsformel). *Sei V ein $\mathbb{K}$-Vektorraum mit Skalarprodukt.*

a) Im Fall $\mathbb{K} = \mathbb{R}$ gilt für alle $v, w \in V$ die Formel

$$\langle v, w\rangle \;=\; \frac{\|v+w\|^2 - \|v\|^2 - \|w\|^2}{2} \;=\; \frac{\|v+w\|^2 - \|v-w\|^2}{4}$$

b) Im Fall $\mathbb{K} = \mathbb{C}$ gilt für alle $v, w \in V$ die Formel

$$\langle v, w\rangle \;=\; \frac{\|v+w\|^2 + \|v-w\|^2}{4} - i \cdot \frac{\|v+iw\|^2 - \|v-iw\|^2}{4}$$

Beweis. Im komplexen Fall ist

$$\begin{aligned}
\|v+w\|^2 - \|v-w\|^2 \;&=\; \langle v+w, v+w\rangle - \langle v-w, v-w\rangle && \text{per Definition}\\
&=\; \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle + \langle w,w\rangle \\
&\quad - \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle - \langle w,w\rangle && \text{wegen Sesquilinearität}\\
&=\; 4\,\mathrm{Re}(\langle v,w\rangle) && \text{wegen } \langle w,v\rangle = \overline{\langle v,w\rangle}
\end{aligned}$$

und analog $\|v+iw\|^2 - \|v-iw\|^2 = -4\,\mathrm{Im}(\langle v,w\rangle)$. Hieraus folgt die Behauptung im komplexen Fall. Die Rechnung im reellen Fall geht genauso. □

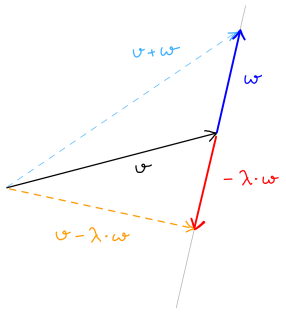
Skalarprodukte beliebiger Vektoren lassen sich durch ihre Norm abschätzen mit der folgenden wichtigen Ungleichung; für das Standardskalarprodukt auf $\mathbb{R}^2$ läuft diese hinaus auf $|\cos\gamma| \le 1$, aber wir wollen einen davon unabhängigen Beweis für Skalarprodukte auf beliebigen Euklidischen und unitären Vektorräumen geben:

Satz 2.7 (Cauchy-Schwarz-Ungleichung). *Es sei V ein Euklidischer oder unitärer Vektorraum. Dann ist*

$$|\langle v, w\rangle| \;\le\; \|v\| \cdot \|w\| \quad \textit{für alle } v, w \in V$$

und dabei gilt Gleichheit genau dann, wenn v und w linar abhängig sind.

Beweis. Im Fall $w = 0$ wird die Ungleichung trivial, sei also $w \neq 0$. Die Idee ist es, einen Vektor minimaler Norm auf der affinen Geraden $\{v + \lambda w \mid \lambda \in \mathbb{K}\}$ zu betrachten. Anschaulich ist klar, dass dazu $v + \lambda w$ senkrecht auf w stehen sollte:



Wir definieren also $\lambda \in \mathbb{K}$ durch $\langle w, v - \lambda w\rangle = 0$, d.h.

$$\lambda \;=\; \frac{\langle w, v\rangle}{\|w\|^2}$$

Für die Norm des so gewählten Vektors $v - \lambda w$ erhalten wir

$$\begin{aligned}
0 \;\leq\; & \|v - \lambda w\|^2 && \text{wegen positiver Definitheit}\\
=\; & \langle v - \lambda w, v - \lambda w\rangle && \text{per Definition der Norm}\\
=\; & \langle v, v\rangle - \overline{\lambda}\langle w, v\rangle - \lambda\langle v, w\rangle + \lambda\overline{\lambda}\langle w, w\rangle && \text{wegen Sesquilinearität}\\
=\; & \|v\|^2 - \frac{|\langle v, w\rangle|^2}{\|w\|^2} && \text{wegen } \lambda = \langle w, v\rangle / \|w\|^2
\end{aligned}$$

und somit folgt die Behauptung durch Multiplikation mit $\|w\|^2 > 0$. □

Wir erhalten insbesondere die Dreiecksungleichung, die anschaulich besagt, dass in einem Dreieck die Länge jeder Seite höchstens gleich der Summe der übrigen beiden Seitenlängen ist:

Korollar 2.8 (Dreiecksungleichung). *Es sei V ein Euklidischer oder ein unitärer Vektorraum. Dann ist*

$$\|v + w\| \;\leq\; \|v\| + \|w\| \quad \text{für alle } v, w \in V$$

und dabei gilt Gleichheit genau dann, wenn v und w linear abhängig sind.

Beweis. Es gilt

$$\begin{aligned}
\|v+w\|^2 &= \langle v+w, v+w\rangle && \text{per Definition der Norm}\\
&= \|v\|^2 + \langle v,w\rangle + \langle w,v\rangle + \|w\|^2 && \text{wegen Sesquilinearität}\\
&= \|v\|^2 + 2\mathrm{Re}(\langle v,w\rangle) + \|w\|^2 && \text{wegen } \langle w,v\rangle = \overline{\langle v,w\rangle}\\
&\leq \|v\|^2 + 2\,\|v\|\,\|w\| + \|w\|^2 && \text{nach Cauchy-Schwarz}\\
&= \big(\|v\| + \|w\|\big)^2
\end{aligned}$$

und da auf beiden Seiten positive reelle Zahlen stehen, folgt die Behauptung durch Wurzelziehen. □

Die wichtigsten Eigenschaften der durch ein Skalarprodukt $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{K}$ definierten Norm $\|\cdot\| : V \to \mathbb{R}$ werden in der folgenden allgemeineren Definition zusammengefasst:

Definition 2.9. Eine *Norm* auf einem $\mathbb{K}$-Vektorraum V ist eine Abbildung

$$\|\cdot\| : \quad V \longrightarrow \mathbb{R}_{\geq 0}$$

sodass für alle $v, w \in V$ und alle $\lambda \in \mathbb{K}$ gilt:

a) Skalierungsinvarianz: $\|\lambda \cdot v\| = |\lambda| \cdot \|v\|$.

b) Positive Definitheit: $\|v\| > 0$ für alle $v \neq 0$.

c) Dreiecksungleichung: $\|v+w\| \leq \|v\| + \|w\|$.

Einen Vektorraum zusammen mit einer Norm nennt man einen *normierten Raum*.

Normierte Räume spielen eine wichtige Rolle in der Analysis, da man in ihnen einen Abstandsbegriff hat. So können wir die Kugel vom Radius $\varepsilon > 0$ um $v \in V$ definieren durch

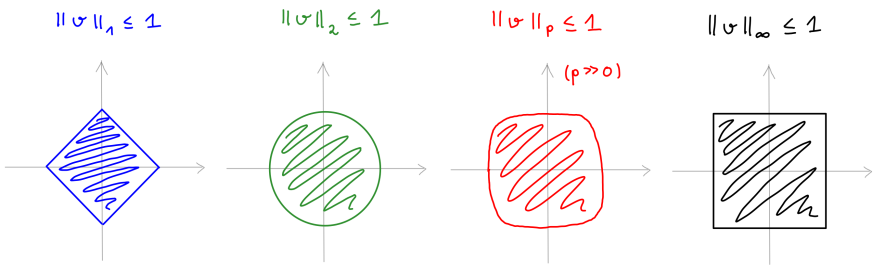
$$B_\varepsilon\big(v, \|\cdot\|\big) := \{w \in V \mid \|w-v\| < \varepsilon\}$$

Das folgende Beispiel zeigt, dass solche Kugeln unterschiedlich aussehen können und dass nicht jede Norm von einem Skalarprodukt kommt:

Beispiel 2.10. Sei $p \in \mathbb{N} \cup \{\infty\}$. Man sieht leicht, dass die Abbildung $\|\cdot\|_p : \mathbb{R}^n \to \mathbb{R}$ definiert durch

$$\|v\|_p := \begin{cases} \sqrt[p]{|v_1|^p + \cdots + |v_n|^p} & \text{für } p \in \mathbb{N},\\ \max\{|v_1|, \ldots, |v_n|\} & \text{für } p = \infty, \end{cases}$$

eine Norm ist. Für $p = 2$ ist dies die von dem Standardskalarprodukt induzierte Norm. Die folgende Abbildung zeigt die "Einheitskreise" in der Ebene bezüglich einiger dieser Normen:



Im Fall $n \geq 2$ ist die soeben betrachtete Norm $\|\cdot\|_p : \mathbb{R}^n \to \mathbb{R}$ nur für $p = 2$ von einem Skalarprodukt induziert. Um dies nachzuprüfen, kann man das folgende allgemeine Resultat verwenden, das ein notwendiges und hinreichendes Kriterium dafür gibt, wann eine gegebene Norm von einem Skalarprodukt kommt:

Satz 2.11. *Sei $\|\cdot\| : V \to \mathbb{R}$ eine Norm. Dann sind äquivalent:*

a) Es gibt ein Skalarprodukt $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{K}$ mit $\|v\|^2 = \langle v, v\rangle$ für alle $v \in V$.

b) Es gilt die Parallelogrammgleichung

$$\|v+w\|^2 + \|v-w\|^2 \;=\; 2\|v\|^2 + 2\|w\|^2 \quad \textit{für alle } v, w \in V.$$

Beweis. Wenn a) gilt, berechnet man

$$\begin{aligned} \|v+w\|^2 + \|v-w\|^2 \;&=\; \|v\|^2 + \langle v, w\rangle + \langle w, v\rangle + \|w\|^2 \\ &\quad + \|v\|^2 - \langle v, w\rangle - \langle w, v\rangle + \|w\|^2 \\ &=\; 2\|v\|^2 + 2\|w\|^2 \end{aligned}$$

und somit gilt die Parallelogrammgleichung b). Ist umgekehrt letzteres der Fall, so erinnern wir uns an die Polarisationsformel in Lemma 2.6 und *definieren* eine Abbildung durch

$$\langle v, w\rangle \;:=\; \begin{cases} \frac{\|v+w\|^2 - \|v-w\|^2}{4} & \text{im Fall } \mathbb{K} = \mathbb{R}, \\ \frac{\|v+w\|^2 - \|v-w\|^2}{4} - i\frac{\|v+iw\|^2 - \|v-iw\|^2}{4} & \text{im Fall } \mathbb{K} = \mathbb{C}. \end{cases}$$

Direkt aus der Definition folgt, dass $\langle v, v\rangle = \|v\|^2$ die gegebene Norm ist. Wir wollen zeigen, dass $\langle\cdot,\cdot\rangle$ tatsächlich ein Skalarprodukt ist. Die positive Definitheit folgt aus der vorigen Gleichung und der Positivität von Normen. Zudem ist $\langle w, v\rangle \;=\; \overline{\langle v, w\rangle}$ in unsere Definition eingebaut. Zu zeigen bleibt, dass für alle $u, v, w \in V$ und $a \in \mathbb{K}$ gilt:

$$\langle u, v + a\cdot w\rangle \;=\; \langle u, v\rangle + a\cdot\langle u, w\rangle$$

Für $a = 1$ folgt dies aus der Parallelogrammgleichung durch geduldiges Einsetzen, im reellen Fall beispielsweise

$$
\begin{aligned}
4\langle u,v\rangle + 4\langle u,w\rangle &= \|u+v\|^2 - \|u-v\|^2 + \|u+w\|^2 - \|u-w\|^2 && \text{per Definition}\\
&= \|u+v\|^2 + \|w\|^2 && \\
&\quad - \|u-v\|^2 - \|w\|^2 && \\
&\quad + \|u+w\|^2 + \|v\|^2 && \text{durch Ergänzen}\\
&\quad - \|u-w\|^2 - \|v\|^2 && \text{von Nullen}\\
&= \tfrac{1}{2}\big(\|u+v+w\|^2 + \|u+v-w\|^2\big) && \\
&\quad + \tfrac{1}{2}\big(\|u+v+w\|^2 + \|u-v+w\|^2\big) && \text{wegen der}\\
&\quad - \tfrac{1}{2}\big(\|u-v+w\|^2 + \|u-v-w\|^2\big) && \text{Parallelogramm-}\\
&\quad - \tfrac{1}{2}\big(\|u+v-w\|^2 + \|u-v-v\|^2\big) && \text{gleichung}\\
&= \|u+v+w\|^2 - \|u-v-w\|^2 && \\
&= 4\langle u,v+w\rangle && \text{per Definition}
\end{aligned}
$$

Induktiv folgt dann auch der Fall $a \in \mathbb{N}$ und hieraus nach Division durch natürliche Zahlen der Fall $a \in \mathbb{Q}$. Da beide Seiten der zu beweisenden Gleichung stetig von a abhängen, folgt dann die Gleichung für alle $a \in \mathbb{R}$. Im komplexen Fall gilt sie sogar für alle $a \in \mathbb{C}$, da sie für $a = i$ direkt aus der Definition folgt. □

Oft sind wir gar nicht an der genauen Form der Norm $\|\cdot\| : V \to \mathbb{R}$ interessiert, sondern nur daran, welche Teilmengen $U \subseteq V$ *offen* sind in dem Sinn, dass sie um jeden ihrer Punkte eine kleine Kugel bezüglich der gegebenen Norm enthält. Die Kollektion aller solcher offenen Teilmengen bezeichnet man auch als die durch die Norm definierte *Topologie* auf dem Vektorraum. Sie hängt von der Norm nur bis auf die folgende Äquivalenzrelation ab:

Definition 2.12. Zwei Normen $\|\cdot\|_1, \|\cdot\|_2 : V \longrightarrow \mathbb{R}$ heißen *äquivalent*, wenn es Konstanten $c, d \in \mathbb{R}_{>0}$ gibt mit

$$c \cdot \|v\|_1 \;\le\; \|v\|_2 \;\le\; d \cdot \|v\|_1 \quad \textit{für alle } v \in V.$$

In der Analysis zeigt man, dass auf *endlich-dimensionalen* $\mathbb{K}$-Vektorräumen je zwei Normen äquivalent sind; man denke an die Abbildung **??**! Daher werden wir hier nur Normen betrachten, die von Skalarprodukten kommen. Für Vektorräume unendlicher Dimension gibt es aber viel mehr Wahlmöglichkeiten, in der Analysis spielen daher allgemeinere normierte Räume eine wichtige Rolle:

Beispiel 2.13. Auf dem Raum $V = C([0,1])$ der stetigen Funktionen $f : [0,1] \to \mathbb{R}$ wird für jedes $p \in \mathbb{N} \cup \{\infty\}$ durch

$$\|\cdot\|_p : \quad V \longrightarrow \mathbb{R}_{\ge 0}, \quad \|f\|_p := \begin{cases} \sqrt[p]{\int_0^1 |f(x)|^p dx} & \text{für } p \in \mathbb{N}, \\ \max\{|f(x)| : x \in [0,1]\} & \text{für } p = \infty, \end{cases}$$

eine Norm definiert. Diese Normen sind paarweise nicht-äquivalent (Übung)!

3 Orthogonalität und das Gram-Schmidt Verfahren

Für $V = \mathbb{R}^3$ haben wir uns zu Beginn dieses Kapitels überlegt, dass sich Winkel γ zwischen zwei Vektoren $v, w \in \mathbb{R}^3$ mit dem Standardskalarprodukt berechnen lässt aus $\|v\|\|w\|\cos(\gamma) = \langle v, w\rangle$. Allgemeiner können wir wegen der Cauchy-Schwarz Ungleichung den Winkel zwischen zwei Vektoren $v, w \in \mathbb{R}^n \setminus \{0\}$ *definieren* durch die Gleichung

$$\cos(\gamma) \;:=\; \frac{\langle v, w\rangle}{\|v\|\|w\|} \;\in\; [-1, 1].$$

Diese Definition kann man ebenso in jedem Euklidischen Vektorraum lesen. In Fall von unitären Vektorräumen kann man zwar keine reellen Winkel zwischen Vektoren definieren, aber sowohl in Euklidischen wie auch in unitären Vektorräumen haben wir einen sinnvollen Begriff dafür, wann Vektoren senkrecht aufeinander stehen:

Definition 3.1. Sei V ein Euklidischer oder unitärer Vektorraum. Vektoren $v, w \in V$ heißen *orthogonal* oder *senkrecht* zueinander, wenn

$$\langle v, w\rangle \;=\; 0$$

gilt. Wir schreiben dann $v \perp w$. Ein System $(v_i)_{i\in I}$ von Vektoren $v_i \in V$ heißt

a) ein *Orthogonalsystem*, wenn $v_i \perp v_j$ für alle $i \neq j$ gilt,

b) ein *Orthonormalsystem*, wenn zusätzlich $\|v_i\| = 1$ für alle i ist,

c) eine *Orthonormalbasis*, wenn es ein Orthogonalsystem und eine Basis ist.

Beispiel 3.2. In $V = \mathbb{K}^n$ bildet die Standardbasis eine Orthonormalbasis bezüglich des Standardskalarproduktes.

Orthonormalbasen besitzen die schöne Eigenschaft, dass sich die Koeffizienten in der Basisdarstellung von Vektoren einfach als Skalarprodukte ablesen lassen:

Lemma 3.3. *Sei V ein Euklidischer oder unitärer Vektorraum. Dann gilt:*

a) Jedes Orthonormalsystem ist linear unabhängig.

b) Sei $e_1, \ldots, e_n \in V$ eine Orthonormalbasis. Dann besitzt jedes $v \in V$ die eindeutige Darstellung

$$v \;=\; \sum_{i=1}^{n} a_i e_i \quad \text{mit} \quad a_i \;=\; \langle e_i, v\rangle.$$

Beweis. Sei $e_1, \ldots, e_n \in V$ ein Orthogonalsystem und $v = \sum_{i=1}^n a_i e_i$ mit $a_i \in K$, dann folgt

$$\langle e_j, v\rangle \;=\; \sum_{i=1}^{n} a_i \langle e_j, e_i\rangle \;=\; \sum_{i=1}^{n} a_i \delta_{ij} \;=\; a_i.$$

Indem wir $v = 0$ wählen, sehen wir, dass die Vektoren $e_1, \ldots, e_n$ linear unabhängig sind. Wenn sie außerdem ein Erzeugendensystem bilden, können wir jeden anderen Vektor $v \in V$ aus ihnen linearkombinieren und erhalten die Formel in b). □

Wir wollen zeigen, dass jeder endlich-dimensionale Euklidische oder unitäre Vektorraum eine Orthogonalbasis besitzt, also in einer geeigneten Basis aussieht wie der Standardvektorraum mit dem Standardskalarprodukt. Wir beweisen dies per Induktion über die Dimension. Für Vektoren $v \in V$ und Teilmengen $U \subseteq V$ schreiben wir $v \perp U$, wenn $v \perp u$ für alle $u \in U$ ist. Offenbar gilt:

Bemerkung 3.4. Sei V ein Euklidischer oder unitärer Vektorraum, und sei $U \subseteq V$ ein Unterraum mit einem Erzeugendensystem $u_1, \ldots, u_n$. Für $v \in V$ sind dann äquivalent:

a) Es ist $v \perp U$.

b) Es ist $v \perp u_i$ für alle $i \in \{1, \ldots, n\}$.

Beweis. Jeder Vektor $u \in U$ hat die Form $u = \sum_{i=1}^{n} a_i u_i$ mit $a_i \in \mathbb{K}$. Wenn $v \in V$ die Eigenschaft b) besitzt, folgt aus der Linearität des Skalarproduktes in der zweiten Variable die Identität

$$\langle v, u\rangle \;=\; \sum_{i=1}^{n} a_i \cdot \langle v, u_i\rangle \;=\; \sum_{i=1}^{n} a_i \cdot 0 \;=\; 0,$$

und da $u \in U$ beliebig war, folgt a). Die Umkehrung gilt per Definition. □

Für die induktive Konstruktion von Orthonormalbasen verwenden wir nun die folgende Beobachtung:

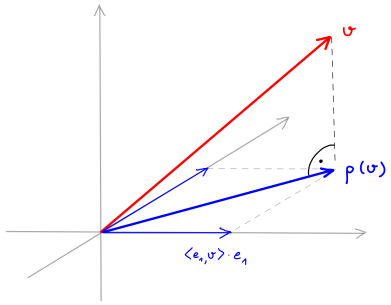
Lemma 3.5. *Sei V ein Euklidischer oder unitärer Vektorraum, und es sei $U \subseteq V$ ein Unterraum endlicher Dimension mit einer Orthonormalbasis $u_1, \ldots, u_n$. Dann gibt es genau eine lineare Abbildung*

$$p_U : \quad V \longrightarrow U$$

mit $(v - p_U(v)) \perp U$ für alle $v \in V$ und diese lineare Abbildung ist gegeben durch

$$p_U(v) \;=\; \sum_{i=1}^{n} \langle u_i, v\rangle \cdot u_i.$$

Wir nennen p_U die Orthogonalprojektion *von V auf den Untervektorraum U.*



Beweis. Für $v \in V$ und $w = v - \sum_{i=1}^{n} a_i u_i$ mit $a_i \in \mathbb{K}$ gilt:

$$\begin{aligned}
w \perp U &\iff w \perp u_i \text{ für } i = 1,\dots,n && \text{nach Bemerkung 3.4}\\
&\iff \langle u_i, w\rangle = 0 \text{ für } i = 1,\dots,n && \text{per Definition von } \perp\\
&\iff \langle u_i, v\rangle - \sum_{j=1}^{n} a_j \langle u_i, u_j\rangle = 0 && \text{wegen } w = v - \sum_{j=1}^{n} a_j u_j\\
&\iff a_i = \langle u_i, v\rangle && \text{wegen } \langle u_i, u_j\rangle = \delta_{ij}.
\end{aligned}$$

Damit folgt die Existenz und die behauptete Formel für p_U, insbesondere ist p_U eindeutig bestimmt. Dass p_U eine lineare Abbildung ist, folgt aus der angegebenen Formel wegen der Linearität des Skalarproduktes in der zweiten Variable. □

Wir erhalten das folgende konstruktive Verfahren, das man als eine Verfeinerung des Basisergänzungssatzes für Vektorräume mit Skalarprodukt betrachten kann:

Satz 3.6. *Sei V ein Euklidischer oder ein unitärer Vektorraum mit* $\dim_{\mathbb{K}}(V) < \infty$*, dann gilt:*

a) Jede Orthonormalbasis eines beliebigen Untervektorraumes $U \subseteq V$ lässt sich zu einer Orthonormalbasis von V ergänzen.

b) Insbesondere besitzt der Vektorraum V eine Orthonormalbasis.

Beweis. Es sei $U \subseteq V$ ein beliebiger Untervektorraum, und es sei $(v_1,\dots,v_n)$ eine Orthonormalbasis desselben. Im Fall $U = V$ ist nichts zu zeigen, wir dürfen also annehmen, dass ein Vektor $v \in V \setminus U$ existiert. Wir betrachten sein Bild unter der Orthogonalprojektion

$$p_U : \quad V \longrightarrow U$$

aus Lemma 3.5 und setzen

$$w \;=\; v - p_U(v) \;=\; v - \sum_{i=1}^{n} \langle u_i, v\rangle \cdot u_i.$$

Per Konstruktion gilt $w \perp U$ und $w \neq 0$. Wir gehen von w über zu dem normierten Vektor

$$v_{n+1} \;:=\; \frac{1}{\|w\|}\cdot w,$$

dann ist $(v_1,\ldots,v_{n+1})$ ein Orthonormalsystem und somit eine Orthonormalbasis des Untervektorraumes

$$U' \;:=\; \mathbb{R}u_1 \oplus \cdots \oplus \mathbb{R}u_{n+1} \;\subseteq\; V$$

Wir können nun induktiv fortfahren. Wegen $\dim_{\mathbb{K}}(U') = \dim_{\mathbb{K}}(U)+1$ endet das Verfahren nach $m-n$ Schritten für $m = \dim_{\mathbb{K}}(V)$. Damit folgt die Aussage $a)$, und Teil $b)$ erhält man als Spezialfall $U = \{0\}$. □

In der Praxis wendet man das obige Verfahren meistens auf ein vorgegebenes linear unabhängiges System von Vektoren an, um daraus eine Orthonormalbasis des hiervon aufgespannten Unterraumes zu konstruieren.

Algorithmus 3.7 (Gram-Schmidt Verfahren). Es seien $u_1,\ldots,u_n \in V$ ein linear unabhängiges System in einem Euklidischen oder unitären Vektorraum beliebiger Dimension. Für $i = 1,2,\ldots,n$:

- Betrachte den Vektor $v := u_i$.
- Berechne $w \;:=\; v - \sum_{k=1}^{i-1} \langle v_k, v\rangle \cdot v_k$.
- Normiere diesen Vektor zu $v_i := \frac{1}{\|w\|}\cdot w$.

Dann bilden $v_1,\ldots,v_n$ eine Orthonormalbasis von $U := \mathbb{K}u_1 + \cdots + \mathbb{K}u_n$.

Beispiel 3.8. Auf $V = \mathbb{R}^2$ betrachte man die Bilinearform $\langle\cdot,\cdot\rangle : V\times V \to \mathbb{R}$ mit der Gram-Matrix

$$A \;=\; \frac{1}{2}\cdot\begin{pmatrix} 2 & 1 & 1\\ 1 & 2 & 1\\ 1 & 1 & 2\end{pmatrix} \;\in\; \mathrm{Mat}(3\times 3,\mathbb{R})$$

in der Standardbasis. Die Bilinearform ist symmetrisch nach Lemma 1.14. Für alle Vektoren $v = (x,y,z)^{\mathrm{t}} \in V$ gilt

$$\langle v,v\rangle \;=\; x^2+y^2+z^2+xy+xz+yz \;=\; \frac{x^2+y^2+z^2+(x+y+z)^2}{2} \;\geq\; 0$$

mit Gleichheit nur für $v = 0$, also ist $\langle\cdot,\cdot\rangle$ ein Skalarprodukt. Die Standardbasis ist keine Orthonormalbasis für dieses Skalarprodukt. Um eine Orthonormalbasis zu finden, wenden wir das Gram-Schmidt Verfahren auf die Standardbasis an:

- Der Vektor $v_1 := e_1$ hat schon die Norm $\|v_1\|^2 = e_1^{\mathrm{t}}\cdot A\cdot e_1 = 1$.
- Als nächstes setzen wir $v := e_2$ und berechnen
  - das Skalarprodukt $\langle v_1, v\rangle = v_1^{\mathrm{t}}\cdot A\cdot v = \frac{1}{2}$
  - den Vektor $w := v - \langle v_1,v\rangle\cdot v_1 = \frac{1}{2}\cdot(-1,2,0)^{\mathrm{t}}$

– seine Norm $\|w\|^2 = w^{\mathsf{t}} \cdot A \cdot w = \frac{3}{4}$

– den normierten Vektor

$$v_2 \;:=\; \frac{1}{\|w\|} \cdot w \;=\; \frac{1}{\sqrt{3}} \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}.$$

- Als nächstes setzen wir $v := e_3$ und berechnen

  – die Skalarprodukte $\langle v_1, v\rangle = \frac{1}{2}$ und $\langle v_2, v\rangle = \frac{1}{2\sqrt{3}}$,

  – den Vektor $w := v - \langle v_1, v\rangle v_1 - \langle v_2, v\rangle v_2 = \frac{1}{3}(-1,-1,3)^{\mathsf{t}}$

  – seine Norm $\|w\|^2 = w^{\mathsf{t}} \cdot A \cdot w = \frac{2}{3}$,

  – den normierten Vektor

$$v_3 \;:=\; \frac{1}{\|w\|} \cdot w \;=\; \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix}$$

Dann ist (v_1, v_2, v_3) eine Orthonormalbasis für das gegebene Skalarprodukt. In der Tat gilt

$$\langle v_i, v_j\rangle \;=\; v_i^{\mathsf{t}} \cdot A \cdot v_j \;=\; \begin{cases} 1 & \text{für } i = j, \\ 0 & \text{für } i \neq j. \end{cases}$$

Bemerkung 3.9. Es sei $V = \mathbb{K}^n$ mit einem Skalarprodukt, welches bezüglich der Standardbasis durch eine Gram-Matrix $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ gegeben sei. Eine andere Basis $(v_1, \ldots, v_n)$ von $\mathbb{K}^n$ bildet genau dann eine Orthonormalbasis bezüglich dieses Skalarproduktes, wenn

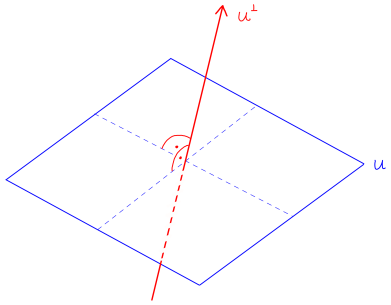
$$S^{\dagger} \cdot A \cdot S \;=\; \mathbf{1} \quad \text{für die Basiswechselmatrix} \quad S \;:=\; \begin{pmatrix} | & | & & | \\ v_1 & v_2 & \cdots & v_n \\ | & | & & | \end{pmatrix} \;\in\; Gl_n(\mathbb{K})$$

gilt. Wir werden diese Normalform von Gram-Matrizen später verallgemeinern auf nicht positiv definite hermitesche Sesquilinearformen.

Man kann sich die in Lemma 3.5 betrachtete Orthogonalprojektion vorstellen als die Projektion auf einen direkten Summanden. Dazu führen wir folgenden Begriff ein:

Definition 3.10. Sei V ein Euklidischer oder unitärer Vektorraum, und sei $U \subseteq V$ ein Untervektorraum. Unter dem *Orthokomplement* von U in V verstehen wir den Untervektorraum

$$\begin{aligned} U^{\perp} \;&:=\; \{\, v \in V \mid v \perp U \,\} \\ &=\; \{\, v \in V \mid \langle v, w\rangle = 0 \text{ für alle } w \in U \,\} \end{aligned}$$



Ein Untervektorraum hat viele Komplemente, aber nur ein Orthokomplement bezüglich eines vorgegebenen Skalarproduktes! Das folgende Lemma zeigt, dass Orthokomplemente ihren Namen verdienen:

Lemma 3.11. *Sei $U \subseteq V$ ein endlich-dimensionaler Unterraum eines Euklidischen oder unitären Vektorraums. Dann gilt*

$$V = U \oplus U^\perp \quad \textit{und} \quad (U^\perp)^\perp = U.$$

Beweis. Sei $p_U : V \to U$ die Orthogonalprojektion aus Lemma 3.5. Dann besitzt jedes $v \in V$ die Zerlegung

$$v = u + w \quad \text{mit} \quad \begin{cases} u := p_U(v) \in U \\ w := v - u \in U^\perp \end{cases}$$

und somit wird $V = U + U^\perp$ von U und $U^\perp$ erzeugt. Diese Summe ist direkt, denn es gilt:

$$\begin{aligned} v \in U \cap U^\perp &\implies v \in U \text{ und } v \perp u \text{ für alle } u \in U \\ &\implies v \perp v \quad \text{(indem man } u = v \text{ wählt)} \\ &\implies v = 0 \quad \text{(wegen positiver Definitheit des Skalarproduktes)} \end{aligned}$$

Also ist $U \cap U^\perp$ und somit ist die Summe $V = U \oplus U^\perp$ direkt. Zu zeigen bleibt nur noch die Aussage über das Orthokomplement des Orthokomplements. Dazu beachte man, dass für beliebige Vektoren $v = u + w$ mit der Zerlegung $u \in U$, $w \in U^\perp$ gilt:

$$\begin{aligned} v \in (U^\perp)^\perp &\iff \forall x \in U^\perp : \langle v, x \rangle = 0 \\ &\iff \forall x \in U^\perp : \langle u, x \rangle + \langle w, w' \rangle = 0 \\ &\iff \forall x \in U^\perp : \langle w, x \rangle = 0 \\ &\iff w = 0 \end{aligned}$$

wobei wir im letzten Schritt wieder die positive Definitheit des Skalarproduktes benutzt haben. Somit ist $(U^\perp)^\perp = U$ wie behauptet. □

Man beachte, dass wir hier nur vorausgesetzt hatten, dass der Unterraum $U \subseteq V$ endliche Dimension besitzt. Im Gegensatz dazu darf V durchaus ein Euklidischer oder unitärer Vektorraum unendlicher Dimension sein. Die Orthogonalprojektion in Lemma 3.5 kann dann z.B. zur Approximation von Funktionen durch endliche Linearkombinationen einfacherer Funktionen verwendet werden:

Übungsaufgabe 3.12. Sei $V = \{\text{ stetige Funktionen } f : [-1,1] \to \mathbb{R}\}$ versehen mit dem Skalarprodukt

$$\langle f, g\rangle \;:=\; \int_{-1}^{1} f(x)g(x)dx,$$

und es seien $e_n \in V$ definiert durch $e_0 := \frac{1}{\sqrt{2}}$ und $e_n(x) := \cos(n\pi x)$ für $n \in \mathbb{N}$.

a) Man zeige, dass $(e_n)_{n\in\mathbb{N}_0}$ ein Orthonormalsystem in V ist.

b) Für $n \in \mathbb{N}$ sei $U_n \subseteq V$ der von $e_0, e_1, \ldots, e_n$ aufgespannte Unterraum, und sei

$$p_n : \quad V \;\longrightarrow\; U_n \;:=\; \mathbb{R}e_1 + \cdots + \mathbb{R}e_n$$

die Orthogonalprojektion. Man finde $p_n(f)$ für die Funktion $f(x) := 1 - |x|$.

Wenn man die Funktionen $p_n(f)$ plottet, sieht man, dass sie eine Approximation von f durch trigonometrische Funktionen liefern. Solche Approximationen werden in der Fourieranalysis studiert, sie sind wichtig für die Signalverarbeitung und bei der Beschreibung von Klangfarben durch Obertonreihen.

Wir haben hier nur Orthogonalprojektionen auf Unterräume endlicher Dimension betrachtet. Für Unterräume unendlicher Dimension treten neue Phänomene auf:

Beispiel 3.13. Sei V der Vektorraum der stetigen Funktionen $f : [0,1] \to \mathbb{R}$ mit dem Skalarprodukt

$$\langle f, g\rangle \;:=\; \int_{0}^{1} f(x)g(x)dx.$$

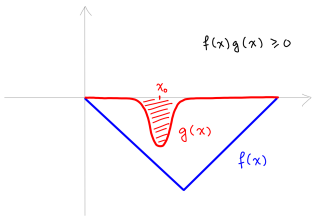
Sei $U \subseteq V$ der Unterraum der differenzierbaren Funktionen. Dann gilt $U \neq V$, aber trotzdem ist

$$U^{\perp} \;=\; \{0\} \quad \text{und somit} \quad (U^{\perp})^{\perp} \;=\; V$$

Denn für jede stetige, nicht identisch verschwindende Funktion $f \in V$ gibt es ein differenzierbares $g \in U$ mit

$$\int_{0}^{1} f(x)g(x)dx > 0$$

wie in der folgenden Abbildung skizziert:



Dass $U^\perp = \{0\}$ ist, sollte nicht als Pathologie betrachtet werden, es ist eine gute Nachricht: Es bedeutet, dass stetige Funktionen sich bezüglich der Norm

$$\|\cdot\|_2 : \quad V \times V \longrightarrow \mathbb{R}, \quad f \mapsto \int_0^1 |f(x)|^2 dx$$

beliebig gut durch differenzierbare Funktionen approximieren lassen.

4 Das Hauptminorenkriterium

Der Gram-Schmidt Algorithmus funktioniert nur, wenn wir es auch wirklich mit einem Skalarprodukt zu tun haben. Im Beispiel 3.8 hatten wir positive Definitheit durch eine ad hoc Umformung in eine Summe von Quadraten gezeigt. Wie kann man allgemein sehen, ob eine gegebene hermitesche Matrix positiv definit ist? Ein notwendiges Kriterium hierfür liefert die Determinante:

Lemma 4.1. *Sei* $A \in \mathrm{Mat}(n \times n, \mathbb{K})$.

a) Wenn A hermitesch ist, gilt $\det(A) \in \mathbb{R}$.

b) Wenn A hermitesch und positiv definit ist, gilt $\det(A) > 0$.

Beweis. Ist A hermitesch, so gilt per Definition $A = A^\dagger$ und somit

$$\det(A) \;=\; \det(A^\dagger) \;=\; \det(\overline{A^{\mathsf{t}}}) \;=\; \overline{\det(A^{\mathsf{t}})} \;=\; \overline{\det(A)},$$

also $\det(A) \in \mathbb{R}$. Ist die Matrix A zusätzlich positiv definit, so ist die zugehörige Sesquilinearform ein Skalarprodukt. Das Gram-Schmidt-Verfahren liefert nach der Bemerkung 3.9 eine Basiswechselmatrix $S \in Gl_n(\mathbb{K})$ mit $S^\dagger \cdot A \cdot S = \mathbf{1}$. Es folgt

$$\begin{aligned} 1 \;=\; \det(\mathbf{1}) \;&=\; \det(S^\dagger \cdot A \cdot S) \\ &=\; \det(S^\dagger) \cdot \det(A) \cdot \det(S) \\ &=\; \det(A) \cdot \overline{\det(S)} \cdot \det(S) \\ &=\; \det(A) \cdot |\det(S)|^2 \end{aligned}$$

und somit $\det(A) > 0$. □

Die Positivität der Determinante ist notwendig, aber nicht hinreichend für die positive Definitheit einer symmetrischen oder hermiteschen Matrix: Beispielsweise ist die Matrix $A = -\mathbf{1} \in \mathrm{Mat}(2\times 2,\mathbb{R})$ symmetrisch und erfüllt $\det(A) > 0$, aber die Matrix ist nicht positiv definit, denn

$$e_1^{\mathsf{t}} \cdot A \cdot e_1 \;=\; -1 \;<\; 0.$$

Um ein notwendiges und hinreichendes Kriterium für die positive Definitheit zu formulieren, betrachten wir auch die Determinanten gewisser Untermatrizen:

Definition 4.2. Unter einem k-ten *Minor* einer Matrix $A = (a_{ij}) \in \mathrm{Mat}(n\times n,\mathbb{K})$ verstehen wir die Determinante einer Untermatrix

$$A_{IJ} \;:=\; \begin{pmatrix} a_{i_1 j_1} & \cdots & a_{i_1 j_k} \\ \vdots & \ddots & \vdots \\ a_{i_k j_1} & \cdots & a_{i_k j_k} \end{pmatrix},$$

die man aus A durch Auswählen von genau k Zeilen und Spalten erhält, wobei die gewählten Zeilen und Spalten durch Indexmengen

$$\begin{aligned} I \;&=\; \{i_1,\ldots,i_k\} && \text{mit} \quad 1 \le i_1 < \cdots < i_k \le n, \\ J \;&=\; \{j_1,\ldots,j_k\} && \text{mit} \quad 1 \le j_1 < \cdots < j_k \le n, \end{aligned}$$

angegeben werden. Falls $I = J = \{1,\ldots,k\}$ für ein $k \le n$ ist, schreiben wir auch kurz

$$A_k \;:=\; A_{\{1,\ldots,k\},\{1,\ldots,k\}} \;\in\; \mathrm{Mat}(k\times k,\mathbb{K})$$

und nennen die Matrizen A_k für $k = 1,\ldots,n$ die *Hauptminoren* von A.

Der folgende Satz zeigt, dass sich die positive Definitheit einer symmetrischen oder hermiteschen Matrix an ihren Hauptminorem ablesen lässt; wir formulieren den Satz der Kürze halber für hermitesche Matrizen, schließen dabei aber den Fall symmetrischer Matrizen über $\mathbb{K} = \mathbb{R}$ mit ein:

Satz 4.3 (Hauptminorenkriterium). *Für hermitesche Matrizen $A \in \mathrm{Mat}(n\times n,\mathbb{K})$ sind äquivalent:*

a) Es ist A positiv definit.

b) Alle Hauptminoren von A sind positiv: $\det(A_k) > 0$ *für* $k = 1,\ldots,n$.

Beweis. Wenn $a)$ erfüllt ist, so ist die Sesquilinearform $(v,w) \mapsto \bar{v}^{\mathsf{t}} \cdot A \cdot w$ positiv definit. Aus der Definition ist klar, dass für eine positiv definite Sesquilinearform auch ihre Einschränkung auf jeden Unterraum positiv definit ist. Indem wir dies für $k = 1,\ldots,n$ auf den Untervektorraum $U_k := \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_k \subseteq \mathbb{K}^n$ anwenden, erhalten wir, dass die Sesquilinearform

$$U_k \times U_k \;\longrightarrow\; \mathbb{K}, \quad (v,w) \;\mapsto\; \bar{v}^{\mathsf{t}} \cdot A \cdot w$$

positiv definit ist. Aber bezüglich der Basis $(e_1,\dots,e_k)$ von U_k wird diese genau durch die Gram-Matrix A_k beschrieben. Damit ist der führende Hauptminor A_k eine positiv definite Matrix und nach Lemma 4.1 folgt $\det(A_k) > 0$, also gilt $b)$.

Gelte nun umbekehrt $b)$. Wir zeigen die positive Definitheit von A per Induktion über n. Für $n = 1$ ist die Behauptung klar. Für den Induktionsschritt betrachten wir nun die durch Streichen der letzten Zeile und Spalte von A erhaltene $B = A_{n-1}$. Da wir die Eigenschaft $b)$ voraussetzen, ist

$$\det(B_k) \;=\; \det(A_k) \;>\; 0 \quad \text{für} \quad k \;=\; 1,2,\dots,n-1.$$

Per Induktion wissen wir also, dass die Matrix B positiv definit ist. Nach Satz 3.6 existiert somit für die durch diese Matrix definierte Sesquilinearform $\langle\cdot,\cdot\rangle_B$ eine Orthonormalbasis von Vektoren

$$v_1,\dots,v_{n-1} \;\in\; U_{n-1} \;=\; \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_{n-1} \;\subseteq\; \mathbb{K}^n$$

Wie im Gram-Schmidt Verfahren (aber ohne zu wissen, ob A positiv definit ist) betrachten wir nun den Vektor

$$v_n \;:=\; e_n - \sum_{i=1}^{n-1} \langle v_i, e_n\rangle_A \cdot v_i.$$

Dann gilt $\langle v_i, v_n\rangle_A = 0$ für $1 \le i < n$. Für den Basiswechsel $S = (v_1,\dots,v_n) \in Gl_n(\mathbb{K})$ folgt

$$S^\dagger AS \;=\; \mathrm{Diag}(1,\dots,1,c)$$

Dabei ist a priori $c = \langle v_n, v_n\rangle_A \in \mathbb{K}$ ein beliebiger Skalar. Aber nach der Annahme $b)$ ist

$$c \;=\; \det(S^\dagger AS) \;=\; |\det(S)|^2 \cdot \det(A) \;\in\; \mathbb{R}_{>0}$$

und somit ist $S^\dagger AS$ positiv definit. Dann ist auch A positiv definit. □

Beispiel 4.4. Es gilt:

a) Für die bereits in Beispiel 3.8 betrachtete Matrix

$$A \;=\; \frac{1}{2}\cdot\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

ist $\det(A_1) = 1$, $\det(A_2) = \frac{3}{4}$, $\det(A_3) = \frac{1}{2}$. Wie erwartet ist also A positiv definit.

b) Die *Semi*definitheit von Matrizen lässt sich nicht an den Haupminoren ablesen, z.B. sind für die reellen symmetrischen Matrizen

$$A \;=\; \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B \;=\; \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad C \;=\; \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

alle Hauptminoren Null, es ist jedoch offensichtlich A positiv semidefinit, B negativ semidefinit und C indefinit.

5 Orthogonale und unitäre Abbildungen

In vielen Anwendungen spielen längenerhaltende lineare Abbildungen eine Rolle:

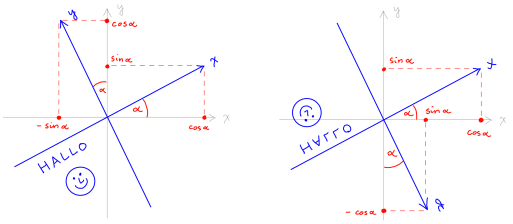
Definition 5.1. Es seien $(V_1, \|\cdot\|_1)$ und $(V_2, \|\cdot\|_2)$ zwei normierte Vektorräume. Eine lineare Abbildung

$$f: \quad V_1 \longrightarrow V_2$$

heißt eine *Isometrie*, falls gilt:

$$\|f(v)\|_2 \;=\; \|v\|_1 \quad \text{für alle} \quad v \in V_1 .$$

Beispielsweise ist in der reellen Ebene $V = \mathbb{R}^2$ mit der vom Standardskalarprodukt induzierten Norm jede Drehung um den Ursprung und jede Spiegelung an einer Geraden durch den Ursprung eine Isometrie:



Allgemein gilt:

Lemma 5.2. *Isometrien sind injektiv. Insbesondere bilden die Isometrien $f : V \to V$ jedes endlich-dimensionalen normierten Raumes $(V, \|\cdot\|)$ auf sich eine Untergruppe von $\mathrm{Aut}_{\mathbb{K}}(V)$, wir nennen diese die* Isometriegruppe *des normierten Raumes und bezeichnen sie mit*

$$\mathrm{Aut}_{\mathbb{K}}(V, \|\cdot\|) \;\subseteq\; \mathrm{Aut}_{\mathbb{K}}(V).$$

Beweis. Sei $f : V_1 \to V_2$ eine Isometrie. Dann gilt

$$f(v) = 0 \quad \Longleftrightarrow \quad \|f(v)\| = 0 \quad \Longleftrightarrow \quad \|v\| = 0 \quad \Longleftrightarrow \quad v = 0$$

und somit ist f injektiv. Im Fall $\dim_{\mathbb{K}}(V_1) = \dim_{\mathbb{K}}(V_2) < \infty$ ist f dann sogar bijektiv nach der Dimensionsformel. Indem man in den obigen Äquivalenzen $v = f^{-1}(w)$ für $w \in V_2$ wählt, sieht man, dass in diesem Fall das Inverse $f^{-1} : V_2 \to V_1$ ebenfalls eine Isometrie ist. Insbesondere bilden die Isometrien eines endlich-dimensionalen Euklidischen oder unitären Raumes $V = V_1 = V_2$ eine Gruppe, da id_V eine Isometrie ist und die Verkettung und das Inverse von Isometrien wieder Isometrien sind. □

Wir interessieren uns hier für Euklidische und unitäre Vektorräume. Für diese sind Isometrien automatisch mit dem Skalarprodukt verträglich; im reellen Fall ist also jede längenerhaltende Abbildung auch winkelerhaltend:

Lemma 5.3. *Sei $f : V_1 \to V_2$ eine Isometrie von Euklidischen oder unitären Räumen bezüglich der von den jeweiligen Skalarprodukten $\langle \cdot, \cdot \rangle_i : V_i \times V_i \to \mathbb{K}$ induzierten Normen. Dann gilt*

$$\langle f(v), f(w) \rangle_2 \;=\; \langle v, w \rangle_1 \quad \text{für alle} \quad v, w \;\in\; V_1 .$$

Beweis. Das folgt direkt aus der Polarisationsformel in Lemma 2.6. □

Wir wollen uns in diesem Abschnitt die Isometriegruppe von Euklidischen und unitären Vektorräumen ansehen. Ihre Elemente haben einen eigenen Namen:

Definition 5.4. Sei V ein Euklidischer oder unitärer Vektorraum und $f \in \mathrm{End}_{\mathbb{K}}(V)$ eine Isometrie. Dann nennen wir f eine

a) *orthogonale Abbildung* für $\mathbb{K} = \mathbb{R}$.

b) *unitäre Abbildung* für $\mathbb{K} = \mathbb{C}$.

Wenn man die Gram-Matrix des Skalarproduktes in einer gegebenen Basis kennt, lassen sich die Abbildungsmatrizen von orthogonalen bzw. unitären Abbildungen wie folgt charakterisieren:

Proposition 5.5. *Es sei V ein Euklidischer oder unitärer Vektorraum von endlicher Dimension und*

$$A \;=\; \mathrm{Gram}_{\mathscr{B}} \langle \cdot, \cdot \rangle$$

die Gram-Matrix seines Skalarproduktes in einer Basis $\mathscr{B}$. Für $f \in \mathrm{End}_{\mathbb{K}}(V)$ sind dann äquivalent:

a) Es ist f eine orthogonale oder unitäre Abbildung.

b) Es gilt $B^{\dagger} A B = A$ für die Abbildungsmatrix $B = M_{\mathscr{B}}(f)$.

Beweis. Sei $\Psi : V \xrightarrow{\sim} \mathbb{K}^n$ der Isomorphismus, der die Basis $\mathscr{B}$ abbildet auf die Standardbasis. Per Definition der Gram-Matrix haben wir dann ein kommutatives Diagramm

$$\begin{array}{ccc} V \times V & \xrightarrow{\quad\langle \cdot, \cdot \rangle\quad} & \mathbb{K} \\ {\scriptstyle \Psi \times \Psi}\big\downarrow & & \big\| \\ \mathbb{K}^n \times \mathbb{K}^n & \xrightarrow{\quad(v,w) \mapsto \bar{v}^{\mathrm{t}} \cdot A \cdot w\quad} & \mathbb{K} \end{array}$$

und dürfen somit im Folgenden annehmen, dass $V = \mathbb{K}^n$ mit der Standardbasis $\mathscr{B}$ und dem Skalarprodukt $\langle v, w \rangle = \bar{v}^{\mathrm{t}} \cdot A \cdot w$ ist. Nach Lemma 5.3 ist f orthogonal bzw. unitär genau dann, wenn

$$\langle f(v), f(w) \rangle \;=\; \langle v, w \rangle \quad \text{für alle} \quad v, w \;\in\; V$$

gilt. Indem wir $f(v) = B \cdot v$ und $f(w) = B \cdot w$ einsetzen und das Skalarprodukt durch die Gram-Matrix bezüglich der Standardbasis ausdrücken, wird diese Bedingung zu

$$\overline{v}^{\mathsf{t}} \cdot \overline{B}^{\mathsf{t}} \cdot A \cdot B \cdot w \;=\; \overline{v}^{\mathsf{t}} \cdot A \cdot w \quad \text{für alle} \quad v, w \;\in\; \mathbb{K}^n$$

Ist diese Bedingung erfüllt, so können wir insbesondere $v = e_i$ und $w = e_j$ setzen und erhalten für den (i,j)-Eintrag der Matrizen

$$(\overline{B}^{\mathsf{t}} \cdot A \cdot B)_{ij} \;=\; A_{ij}.$$

Da das für alle (i,j) gilt, folgt dann $\overline{B}^{\mathsf{t}} \cdot A \cdot B = A$ wie behauptet. Ist umgekehrt die letzte Gleichung erfüllt, dann offensichtlich auch die vorige Bedingung. □

Korollar 5.6. *Die zu $B \in \mathrm{Mat}(n \times n, \mathbb{K})$ gehörige Endomorphismus von $V = \mathbb{K}^n$ ist eine orthogonale bzw. unitäre Abbildung für das Standardskalarprodukt genau dann, wenn gilt:*

$$B^{\dagger} \cdot B \;=\; \mathbf{1}.$$

Beweis. Das ist der Spezialfall $A = \mathbf{1}$ der vorigen Proposition. □

Definition 5.7. Die obigen Matrizen haben einen eigenen Namen:

a) Eine Matrix $B \in \mathrm{Mat}(n \times n, \mathbb{R})$ heißt *orthogonal*, wenn $B^t B = \mathbf{1}$ ist.

b) Eine Matrix $B \in \mathrm{Mat}(n \times n, \mathbb{C})$ heißt *unitär*, wenn $B^{\dagger} B = \mathbf{1}$ ist.

Die Menge aller Matrizen mit dieser Eigenschaft ist nach Lemma 5.2 eine Gruppe, wir nennen sie die *orthogonale* bzw. *unitäre Gruppe* der Größe n und bezeichnen sie mit

$$O(n) \;:=\; \left\{ B \in Gl_n(\mathbb{R}) \mid B^{\mathsf{t}} = B^{-1} \right\} \;\subseteq\; Gl_n(\mathbb{R}),$$

$$U(n) \;:=\; \left\{ B \in Gl_n(\mathbb{C}) \mid B^{\dagger} = B^{-1} \right\} \;\subseteq\; Gl_n(\mathbb{C}).$$

Bemerkung 5.8. Für $B \in \mathrm{Mat}(n \times n, \mathbb{K})$ sind die folgenden Bedingungen äquivalent, wobei $\mathbb{K}^n$ mit dem Standardskalarprodukt versehen sei:

a) Die Matrix B ist orthogonal bzw. unitär.

b) Die Matrix B^{t} ist orthogonal bzw. unitär.

c) Die Spalten von B bilden ein Orthonormalsystem.

d) Die Zeilen von B bilden ein Orthonormalsystem.

Beweis. Per Definition ist eine Matrix B orthogonal bzw. unitär genau dann, wenn ihre Spalten ein Orthonormalsystem für das Standardskalarprodukt bilden. Die transponierte Matrix B^{t} ist also orthogonal bzw. unitär genau dann, wenn die Zeilen von B ein Orthonormalsystem bilden. Zu zeigen bleibt nur, dass $a)$ und $b)$ äquivalent sind. In der Tat gilt:

$$\begin{aligned} B \text{ ist orthogonal bzw. unitär} &\iff B^\dagger \cdot B = \mathbf{1} \\ &\iff B^\dagger = B^{-1} \\ &\iff B \cdot B^\dagger = \mathbf{1} \\ &\iff (B^{\mathsf{t}})^\dagger \cdot B^{\mathsf{t}} = \mathbf{1} \\ &\iff B^{\mathsf{t}} \text{ ist orthogonal bzw. unitär} \end{aligned}$$

wobei die vorletzte Äquivalenz die komplexe Konjugation und $\overline{\mathbf{1}} = \mathbf{1}$ benutzt. □

Beispiel 5.9. Eine Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2\times 2, \mathbb{R})$$

ist orthogonal genau dann, wenn gilt:

$$a^2 + c^2 = b^2 + d^2 = 1 \quad \text{und} \quad ab + cd = 0.$$

Die allgemeine Lösung der ersten beiden Gleichungen ist

$$\begin{aligned} a &= \cos(\alpha), \quad b = -\sin(\beta), \\ c &= \sin(\alpha), \quad d = \cos(\beta), \end{aligned}$$

mit $\alpha, \beta \in \mathbb{R}$. Die dritte Gleichung wird damit nach dem Additionstheorem für sin und cos zu

$$0 = ab + cd = -\cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta) = \sin(\alpha - \beta),$$

d.h. $\beta = \alpha + k\pi$ mit $k \in \mathbb{Z}$. Die Gruppe $O(2)$ enthält also zwei Typen von Matrizen:

a) Drehungen

$$A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

b) Spiegelungen

$$A = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}.$$

Orthogonale Matrizen vom Format 2×2 haben also immer die Determinante ± 1, und als Eigenwerte kommen nur ± 1 in Frage. Allgemeiner gilt:

Lemma 5.10. *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ eine orthogonale oder unitäre Matrix. Dann gilt:*

a) Es ist $|\det(A)| = 1$.

b) Jeder Eigenwert $\lambda \in \mathbb{K}$ von A hat Absolutbetrag $|\lambda| = 1$.

Beweis. Aus der Bedingung $A^\dagger \cdot A = \mathbf{1}$ folgt $|\det(A)|^2 = \det(\mathbf{1}) = 1$. Ist $\lambda \in \mathbb{K}$ ein Eigenwert und $v \in V \setminus \{0\}$ ein zugehöriger Eigenvektor, dann gilt

$$\|v\|^2 \;=\; \overline{v}^{\mathsf{t}} \cdot \mathbf{1} \cdot v \;=\; \overline{v}^{\mathsf{t}} \cdot A^\dagger \cdot A \cdot v \;=\; (Av)^\dagger \cdot (Av) \;=\; \overline{\lambda v}^{\mathsf{t}} \cdot (\lambda v) \;=\; |\lambda|^2 \cdot \|v\|^2$$

und somit $|\lambda| = 1$. □

Durch Einschränken des Gruppenhomomorphismus $\det : Gl_n(\mathbb{K}) \to \mathbb{K}^\times$ erhalten wir somit surjektive Homomorphismen

$$\begin{aligned} \det: \quad O(n) &\longrightarrow \{\pm 1\} \\ \det: \quad U(n) &\longrightarrow \mathbb{S}^1 := \{z \in \mathbb{C}^\times \mid |z| = 1\} \end{aligned}$$

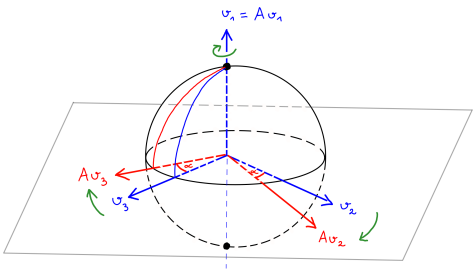
von Gruppen. Die *spezielle orthogonale* bzw. *spezielle unitäre Gruppe* ist definiert als der Kern dieser Homomorphismen, also

$$\begin{aligned} SO(n) &:= \{A \in O(n) \mid \det(A) = 1\}, \\ SU(n) &:= \{A \in U(n) \mid \det(A) = 1\}. \end{aligned}$$

Die Gruppe $SO(3)$ besteht genau aus den orientierungserhaltenden Isometrien des Raumes. Als Anwendung erhalten wir den Satz vom Fußball: Wenn zum Anpfiff der zweiten Halbzeit eines Fußballspiels der Ball in die Feldmitte gelegt wird, gibt es zwei gegenüberliegende Punkte des Balls, die sich an derselben Stelle wie zum Anpfiff der ersten Halbzeit befinden:

Korollar 5.11 (Satz vom Fußball). *Jede orientierungserhaltende Isometrie von $\mathbb{R}^3$ besitzt einen von Null verschiedenen Fixpunkt. Genauer ist jede solche Isometrie eine Drehung um eine Achse durch den Ursprung: Für jede Matrix $A \in SO(3)$ gibt es ein $S \in SO(3)$ und $\alpha \in \mathbb{R}$ mit*

$$S^{-1}AS \;=\; \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{array}\right)$$



Beweis. Sei $A \in SO(3)$. Dann besitzt das normierte Polynom $\chi_A(t) \in \mathbb{R}[t]$ den Grad drei und den konstanten Term $\chi_A(0) = -\det(A) = -1$. Der Zwischenwertsatz der Analysis zeigt, dass es mindestens eine positive Nullstelle $\lambda > 0$ besitzt. Diese ist ein Eigenwert, also folgt $\lambda = 1$ nach Lemma 5.10. Sei $v_1 = v \in \mathbb{R}^3$ ein Eigenvektor dazu mit $\|v\| = 1$. Wir ergänzen diesen zu einer Orthonormalbasis (v_1, v_2, v_3).

Dann wird $U := \mathbb{R}v_2 \oplus \mathbb{R}v_3 = (\mathbb{R}v_1)^\perp \subset \mathbb{R}^3$ von A auf sich abgebildet, denn es gilt

$$\begin{aligned} u \in U &\iff \langle u, v_1 \rangle = 0 \\ &\iff \langle Au, Av_1 \rangle = 0 \\ &\iff \langle Au, v_1 \rangle = 0 \\ &\iff Au \in U \end{aligned}$$

Sei $S = (v_1, v_2, v_3) \in O_3(\mathbb{R})$ der Basiswechsel von der Standardbasis zur gewählten Orthonormalbasis, dann erhalten wir

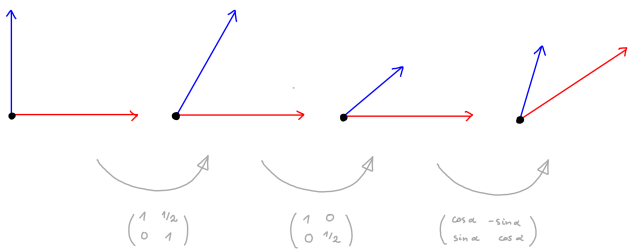
$$S^{-1}AS = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0^t & M \end{array}\right)$$

wobei M die Abbildungsmatrix der Einschränkung unserer Isometrie auf $U \subset \mathbb{R}^3$ bezüglich der Orthonormalbasis (v_2, v_3) ist. Diese Einschränkung ist eine Isometrie und es ist $\det(M) = \det(S^{-1}AS) = \det(A) = 1$. Da U eine Euklidische Ebene ist, muß M nach Beispiel 5.9 eine Drehmatrix sein. □

Orthogonale Matrizen sind auch für die Beschreibung beliebiger invertierbarer Matrizen hilfreich:

Beispiel 5.12. Jede Matrix $M \in Gl_2(\mathbb{R})$ lässt sich zerlegen als ein Produkt einer Scherung, einer Streckung der Koordinatenachsen und einer Drehung oder einer Spiegelung. Denn sei $r > 0$, sodass die erste Spalte von M aus dem Vektor $(r, 0) \in \mathbb{R}^2$ durch eine Drehung um den Winkel α hervorgeht. Dann folgt

$$M = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} r & 0 \\ 0 & t \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{s}{r} \\ 0 & 1 \end{pmatrix}$$



Die obige Zerlegung verallgemeinert sich wie folgt:

Satz 5.13 (Iwasawa-Zerlegung). *Für $n \in \mathbb{N}$ bezeichne $D_n \subseteq Gl_n(\mathbb{R})$ die Gruppe der reellen Diagonalmatrizen mit positiven Diagonaleinträgen, und für $\mathbb{K} = \mathbb{R}, \mathbb{C}$ sei $E_n(\mathbb{K}) \subseteq Gl_n(\mathbb{K})$ die Gruppe der oberen Dreiecksmatrizen mit Einsen auf der Diagonalen. Dann liefert die Matrixmultiplikation bijektive Abbildungen*

$$O(n) \times D_n \times E_n(\mathbb{R}) \xrightarrow{\sim} Gl_n(\mathbb{R}), \quad (A,B,C) \mapsto A \cdot B \cdot C,$$

$$U(n) \times D_n \times E_n(\mathbb{C}) \xrightarrow{\sim} Gl_n(\mathbb{C}), \quad (A,B,C) \mapsto A \cdot B \cdot C.$$

Beweis. Wir beweisen die Aussage im reellen Fall und schreiben kurz $E_n = E_n(\mathbb{R})$, denn der komplexe Fall geht völlig analog. Da $D_n, E_n \subseteq Gl_n(\mathbb{R})$ Untergruppen sind und $D_n \cap E_n = \{\mathbf{1}\}$ gilt, ist

$$D_n \times E_n \hookrightarrow Gl_n(\mathbb{R}), \quad (B,C) \mapsto B \cdot C$$

eine injektive Abbildung. Man beachte, dass diese kein Gruppenhmomorphismus ist, da für $A \in D_n$, $B \in E_n$ im Allgemeinen $AB \neq BA$ gilt. Aber das Bild dieser injektiven Abbildung besteht genau aus den oberen Dreiecksmatrizen mit positiven Diagonaleinträgen. Insbesondere ist das Bild eine Untergruppe $D_nE_n \subseteq Gl_n(\mathbb{R})$, und es gilt $O(n) \cap (D_nE_n) = \{\mathbf{1}\}$. Somit ist auch

$$O(n) \times (D_nE_n) \hookrightarrow Gl_n(\mathbb{R}), \quad (A,D) \mapsto A \cdot D$$

eine injektive Abbildung. Zu zeigen bleibt die Surjektivität:

Sei $M \in Gl_n(\mathbb{R})$ gegeben. Die Spalten von M bilden eine Basis $v_1, \ldots, v_n$ des Standardvektorraumes $\mathbb{R}^n$ und das Gram-Schmidt Verfahren konstruiert aus dieser eine Orthonormalbasis. Ein Blick auf das Verfahren zeigt, dass für die so erhaltene Orthonormalbasis $u_1, \ldots, u_n$ gilt:

$$u_i = a_{ii} \cdot v_i + a_{i,i-1} \cdot v_{i-1} + \cdots + a_{i1} \cdot v_1 \quad \text{mit} \quad a_{ij} \in \mathbb{R} \quad \text{und} \quad a_{ii} > 0$$

für alle i. Es gilt dann

$$\begin{pmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix} \cdot \begin{pmatrix} a_{11} & * & * \\ & \ddots & * \\ & & a_{nn} \end{pmatrix}$$

mit $a_{ii} \in \mathbb{R}_{>0}$ für alle i. Die Matrix auf der linken Seite liegt in $O(n)$, der zweite Faktor auf der rechten Seite in der Untergruppe $D_nE_n \subseteq Gl_n(\mathbb{R})$. Multiplikation von rechts mit seinem Inversen liefert die Behauptung. □

Für praktische Anwendungen wird die obige Zerlegung häufig in der folgenden Form verwendet:

Korollar 5.14 (QR-Zerlegung). *Es sei $M \in \mathrm{Mat}(m \times n, \mathbb{R})$ mit $\mathrm{rk}(M) = n$. Dann ist*

$$M \;=\; Q \cdot R$$

mit Matrizen Q, R von folgender Form:

- $Q \in \mathrm{Mat}(m \times n, \mathbb{R})$ *hat orthonormale Spalten,*
- $R \in \mathrm{Mat}(n \times n, \mathbb{R})$ *ist eine obere Dreiecksmatrix.*

Beweis. Wegen $\mathrm{rk}(M) = n$ ist insbesondere $m \geq n$, und die Spalten von M sind linear unabhängig. Wir ergänzen sie zu einer Basis und erhalten eine invertierbare Matrix

$$\widetilde{M} \;=\; \left(M \,\middle|\, *\right) \;\in\; Gl_m(\mathbb{R}).$$

Auf diese wenden wir die Iwasawa-Zerlegung in Satz 5.13 an und erhalten eine Zerlegung

$$\widetilde{M} \;=\; \widetilde{Q} \cdot \widetilde{R} \quad \text{mit} \quad \widetilde{Q} \;=\; \left(Q \,\middle|\, *\right) \;\in\; O(m) \quad \text{und} \quad \widetilde{R} \;=\; \left(\begin{array}{c|c} R & * \\ \hline 0 & * \end{array}\right)$$

wobei $\widetilde{R} \in D_m E_m \subseteq Gl_m(\mathbb{R})$ eine obere Dreiecksmatrix ist. □

Beispiel 5.15. Um ein lineares Gleichungssystem der Form $Mx = b$ mit $b \in \mathbb{R}^m$ zu lösen, kann man wie folgt vorgehen:

a) Schreibe $M = QR$ wie in Korollar 5.14.

b) Berechne den Hilfsvektor $y = Q^{\mathrm{t}} \cdot b$.

c) Berechne x durch "Rückwärtseinsetzen" aus $Rx = y$.

Man beachte, dass in b) nur die transponierte Matrix eingeht: Es ist kein explizites Invertieren einer Matrix notwendig, denn $Q^{\mathrm{t}} \cdot Q = \mathbf{1}$, wenn die Spalten von Q ein Orthonormalsystem bilden. Auch c) kostet keine Mühe, weil R hier ja eine obere Dreiecksmatrix ist. Es bleibt also nur die Frage, wie man eine Zerlegung $M = QR$ in a) möglichst effizient berechnet. Für numerische Rechnungen sollte man nicht das Gram-Schmidt Verfahren benutzen, da dies numerisch instabil ist; bessere Methoden für die Berechnung einer QR-Zerlegung lernen Sie in der Numerik.

6 Dualität und adjungierte Abbildungen

In diesem Abschnitt wollen wir uns überlegen, was Skalarprodukte mit Dualität zu tun haben. Wenn wir $V = \mathbb{R}^n$ als Vektorraum von Spaltenvektoren betrachten und den Dualraum $V^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ als Vektorraum von Zeilenvektoren ansehen, wird die Auswertungsabbildung

$$V^* \times V \;\longrightarrow\; \mathbb{R}, \quad (f, v) \;\mapsto\; f(v)$$

zum Matrizenprodukt

$$\mathrm{Mat}(1\times n,\mathbb{R})\times\mathrm{Mat}(n\times 1,\mathbb{R}) \longrightarrow \mathbb{R}, \quad (u^{\mathsf{t}},v)\mapsto u^{\mathsf{t}}\cdot v$$

von Zeilenvektoren mit Spaltenvektoren. Alternativ können wir dies auch verstehen als Standardskalarprodukt von zwei Spaltenvektoren. Allgemeiner gilt:

Lemma 6.1. *Sei V ein Euklidischer Vektorraum endlicher Dimension. Dann liefert das Skalarprodukt einen Isomorphismus*

$$V \xrightarrow{\sim} V^*, \quad u \mapsto \langle u,-\rangle.$$

Beweis. Aus der Linearität des Skalarproduktes in der zweiten Variable ist klar, dass für jedes feste $u\in V$ durch

$$\varphi_u := \langle u,-\rangle : \quad V \longrightarrow \mathbb{R}, \quad v \mapsto \langle u,v\rangle$$

eine Linearform definiert wird: Für alle $v,w\in V$ und $\alpha\in\mathbb{R}$ ist

$$\varphi_u(v+\alpha w) = \langle u,v+\alpha w\rangle = \langle u,v\rangle+\alpha\langle u,w\rangle = \varphi_u(v)+\alpha\varphi_u(w).$$

Die Linearität des Skalarproduktes in der ersten Variable liefert für $u,v\in V$, $\alpha\in\mathbb{R}$ ebenso

$$\varphi_{u+\alpha v} = \langle u+\alpha v,-\rangle = \langle u,-\rangle+\alpha\langle v,-\rangle = \varphi_u+\alpha\varphi_v$$

Daher wird durch $u\mapsto\varphi_u$ eine lineare Abbildung $V\to V^*$ definiert. Um zu zeigen, dass diese ein Isomorphismus ist, genügt es wegen der Vorassetzung $\dim_{\mathbb{R}}(V)<\infty$, die Injektivität zu zeigen. In der Tat gilt

$$\varphi_u = 0 \iff \langle u,v\rangle = 0 \text{ für alle } v\in V \iff u\in V^{\perp}=\{0\} \iff u = 0$$

wegen der Definitheit des Skalarproduktes, und somit folgt die Behauptung. □

Für unitäre Vektorräume kann man analog verfahren. Da das Skalarprodukt hier nicht bilinear, sondern sesquilinear ist, führen wir folgende Sprechweise ein:

Definition 6.2. Eine Abbildung $f: V\longrightarrow W$ zwischen komplexen Vektorräumen heißt *semilinear*, wenn

$$f(u+\alpha\cdot v) = f(u)+\overline{\alpha}\cdot f(v)$$

für alle $u,v\in V$ und alle $\alpha\in\mathbb{C}$ ist. Dann ist insbesondere f ein Homomorphismus von reellen Vektorräumen. Unter einem *semilinearen Isomorphismus* verstehen wir eine bijektive semilineare Abbildung. Wie zuvor gilt:

Lemma 6.3. *Sei V ein unitärer Vektorraum endlicher Dimension. Dann liefert das Skalarprodukt einen semilinaren Isomorphismus*

$$V \xrightarrow{\sim} V^*, \quad u \mapsto \langle u,-\rangle.$$

Beweis. Wie in Lemma 6.1. Die Sesquilinearität in der ersten Variable liefert in diesem Fall

$$\varphi_{u+\alpha v} \;=\; \langle u+\alpha v,-\rangle \;=\; \langle u,-\rangle + \overline{\alpha}\langle v,-\rangle \;=\; \varphi_u + \overline{\alpha}\varphi_v$$

und somit ist hier die Bijektion $V \xrightarrow{\sim} V^*$ semilinear. □

Im Kapitel über Dualräume hatten wir zu jeder linearen Abbildung $f : V \to W$ eine duale lineare Abbildung $f^* : W^* \to V^*$ definiert. Für Euklidische bzw. unitäre Vektorräume können wir diese nun wie folgt interpretieren:

Proposition 6.4. *Sei $f \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ ein Homomorphismus endlich-dimensionaler Euklidischer oder unitärer Vektorräume. Dann gibt es genau ein $g \in \mathrm{Hom}_{\mathbb{K}}(W,V)$ mit*

$$\big\langle w, f(v)\big\rangle_W \;=\; \big\langle g(w), v\big\rangle_V \quad \textit{für alle} \quad v \in V,\ w \in W.$$

Wir schreiben auch $g = f^\dagger$ und bezeichnen dies als die zu f adjungierte *Abbildung.*

Beweis. Lemma 6.1 bzw. 6.3 liefert die semilinearen Isomorphismen φ_V, φ_W in dem folgenden Diagramm:

$$\begin{array}{ccc} W & \xrightarrow[\varphi_W]{\simeq} & W^* \\ {\scriptstyle g}\,\vdots\downarrow & & \downarrow{\scriptstyle f^*} \\ V & \xrightarrow[\varphi_V]{\simeq} & V^* \end{array}$$

Für $w \in W$ gilt per Konstruktion

$$(\varphi_V \circ g)(w) \;=\; \big\langle g(w), -\big\rangle_V$$

$$(f^* \circ \varphi_W)(w) \;=\; \big\langle w, f(-)\big\rangle_W$$

Das Diagramm kommutiert also genau dann, wenn g die in der Proposition genannte Eigenschaft besitzt. Die eindeutige lineare Abbildung $g \in \mathrm{Hom}_{\mathbb{K}}(W,V)$ mit dieser Eigenschaft ist daher $g = \varphi_V^{-1} \circ f^* \circ \varphi_W$. Man beachte, dass es sich hierbei auch im komplexen Fall um eine lineare, nicht um eine semilineare Abbildung handelt! □

Natürlich kann man die abstrakte Charakterisierung der adjungierten Abbildung auch in Matrizensprache konkretisieren:

Lemma 6.5. *Für $i = 1,2$ sei V_i ein Euklidischer oder unitärer Vektorraum und $\mathscr{B}_i$ sei eine Orthonormalbasis desselben. Für $f \in \mathrm{Hom}_{\mathbb{K}}(V_1,V_2)$ ist dann bezüglich der gegebenen Basen die Abbildungsmatrix der adjungierten Abbildung die adjungierte Matrix der Abbildungsmatrix:*

$$M_{\mathscr{B}_2,\mathscr{B}_1}(f^\dagger) \;=\; \big(M_{\mathscr{B}_1,\mathscr{B}_2}(f)\big)^\dagger$$

Beweis. Seien $\mathscr{B}_1 = (u_1,\ldots,u_n)$ und $\mathscr{B}_2 = (v_1,\ldots,v_m)$ Orthonormalbasen. Für die Abbildungsmatrizen

$$M_{\mathscr{B}_1,\mathscr{B}_2}(f) \;=\; (a_{ij}) \;\in\; \mathrm{Mat}(m\times n,\mathbb{K})$$
$$M_{\mathscr{B}_2,\mathscr{B}_1}(f^\dagger) \;=\; (b_{ji}) \;\in\; \mathrm{Mat}(n\times m,\mathbb{K})$$

gilt dann

$$f(u_j) \;=\; \sum_{i=1}^{m} a_{ij}v_i \quad \text{und} \quad f^\dagger(v_i) \;=\; \sum_{j=1}^{n} b_{ji}u_j.$$

Somit gilt

$$\begin{aligned} a_{ij} \;&=\; \langle v_i, f(u_j)\rangle && \text{weil } v_1,\dots,v_m \text{ ein Orthonormalsystem bilden}\\ &=\; \langle f^\dagger(v_i), u_j\rangle && \text{per Definition der adjungierten Abbildung}\\ &=\; \overline{b_{ji}} && \text{weil } u_1,\dots,u_n \text{ ein Orthonormalsystem bilden}\end{aligned}$$

und es folgt die Behauptung. □

Bemerkung 6.6. In Proposition 6.4 steht die adjungierte Abbildung in der ersten Variablen des Skalarproduktes. Da das Skalarprodukt Hermitesch ist, gilt dann aber auch

$$\langle f(v), w\rangle \;=\; \overline{\langle w, f(v)\rangle} \;=\; \overline{\langle f^\dagger(w), v\rangle} \;=\; \langle v, f^\dagger(w)\rangle.$$

Wegen der Eindeutigkeit folgt

$$(f^\dagger)^\dagger \;=\; f.$$

Für die Zusammensetzung von Abbildungen sieht man analog $(g\circ f)^\dagger = f^\dagger \circ g^\dagger$.

Besonders interessant ist der Fall von Endomorphismen. Dann sind f und $f^\dagger$ Endomorphismen desselben Vektorraumes, insbesondere kann man fragen, ob diese beiden Endomorphismen gleich sind:

Definition 6.7. Sei V ein Euklidischer oder unitärer Vektorraum mit $\dim_{\mathbb{K}}(V) < \infty$. Ein Endomorphismus $f \in \mathrm{End}_{\mathbb{K}}(V)$ heißt *selbstadjungiert*, wenn $f^\dagger = f$ ist. Das ist äquivalent zu der Bedingung

$$A^\dagger \;=\; A$$

für die Abbildungsmatrix $A = M_{\mathscr{B}}(f)$ zu einer beliebigen Orthonormalbasis $\mathscr{B}$ des Vektorraumes. Wir halten fest:

a) Für $\mathbb{K} = \mathbb{R}$ ist ein Endomorphismus selbstadjungiert genau dann, wenn er in einer Orthonormalbasis durch eine symmetrische Matrix dargestellt wird.

b) Für $\mathbb{K} = \mathbb{C}$ ist ein Endomorphismus selbstadjungiert genau dann, wenn er in einer Orthonormalbasis durch eine hermitesche Matrix dargestellt wird.

Matrizen $A \in \mathrm{Mat}(n\times n,\mathbb{K})$ mit $A^\dagger = A$ bezeichnet man auch als *selbstadjungiert*.

Wir haben in Lemma 5.10 gesehen, dass die Determinante und Eigenwerte von orthogonalen bzw. unitären Matrizen Betrag 1 haben. Auch für selbstadjungierte Matrizen gibt es eine Einschränkung an die Determinante und Eigenwerte:

Lemma 6.8. *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ selbstadjungiert. Dann gilt:*

a) $\det(A) \in \mathbb{R}$.

b) Alle Eigenwerte von A sind reell.

Beweis. Die erste Eigenschaft haben wir uns im Lema 4.1 überlegt. Die zweite folgt mit ähnlichen Argumenten: Sei $\lambda \in \mathbb{K}$ ein Eigenwert und $v \in \mathbb{K}^n \setminus \{0\}$ ein dazu gehöriger Eigenvektor; dann gilt

$$A \cdot v \;=\; \lambda \cdot v \quad \text{und} \quad \overline{v}^{\mathsf{t}} \cdot A^{\dagger} \;=\; (Av)^{\dagger} \;=\; (\lambda v)^{\dagger} \;=\; \overline{\lambda} \cdot \overline{v}^{\mathsf{t}}$$

und wegen $A = A^{\dagger}$ somit

$$\lambda \cdot \|v\|^2 \;=\; \overline{v} \cdot \lambda v \;=\; \overline{v}^{\mathsf{t}} \cdot (A \cdot v) \;=\; \overline{v}^{\mathsf{t}} \cdot (A^{\dagger} \cdot v) \;=\; (\overline{v}^{\mathsf{t}} \cdot A^{\dagger}) \cdot v \;=\; \overline{\lambda} \cdot \|v\|^2.$$

Indem wir $\|v\|^2 \neq 0$ auf beiden Seiten kürzen, erhalten wir die Behauptung. □

Beim Übergang von abstrakten Endomorphismen zu Abbildungsmatrizen ist zu beachten, dass die Korrespondenz

$$\text{orthogonale/unitäre Endomorphismen} \;\longleftrightarrow\; \text{orthogonale/unitäre Matrizen}$$

$$\text{selbstadjungierte Endomorphismen} \;\longleftrightarrow\; \text{symmetrische/hermitesche Matrizen}$$

nur für Abbildungsmatrizen bezüglich einer *Orthonormalbasis* gilt:

Beispiel 6.9. Es sei $V = \mathbb{R}^2$ mit dem Standardskalarprodukt, und $f \in \mathrm{End}_{\mathbb{R}}(V)$ sei definiert durch

$$f(v) = A \cdot v \quad \text{für die Matrix} \quad A \;:=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Dann ist f ein selbstadjungierter und orthogonaler Endomorphismus. Aber in der nicht orthonormalen Basis $\mathscr{B} = (e_1, e_1 + e_2)$ ist

$$M_{\mathscr{B}}(f) \;=\; \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix},$$

und diese Matrix ist weder symmetrisch noch orthogonal.

Othogonale, unitäre oder selbstadjungierte Endomorphismen sollten wir also möglichst in Orthonormalbasen beschreiben. Als Basiswechsel bleiben dann nur Matrizen $S \in O(n)$ bzw. $S \in U(n)$. Nur für diese Basiswechselmatrizen gilt $S^{\dagger} = S^{-1}$ und somit

$$A \text{ orthogonal bzw. unitär} \;\Longleftrightarrow\; S^{-1}AS \text{ orthogonal bzw. unitär}$$

$$A \text{ selbstadjungiert} \;\Longleftrightarrow\; S^{-1}AS \text{ selbstadjungiert}$$

Dies führt auf die Frage: Wie einfach kann man eine Abbildungsmatrix durch einen orthogonalen bzw. unitären Basiswechsel machen? Wann ist eine Matrix durch einen solchen Basiswechsel diagonalisierbar? Ein notwendiges und hinreichendes Kriterium dafür liefert der im nächsten Abschnitt diskutierte Spektralsatz.

7 Der Spektralsatz

Wir haben zwei wichtige Klassen von Matrizen $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ definiert durch die Bedingung

$$A^\dagger = \begin{cases} A^{-1} & \text{für } A \text{ orthogonal bzw. unitär,} \\ A & \text{für } A \text{ symmetrisch bzw. hermitesch.} \end{cases}$$

Aus geometrischer Sicht sind die orthogonalen bzw. unitären Matrizen genau die Isometrien bezüglich des Standardskalarproduktes, während die symmetrischen bzw. hermiteschen Matrizen die für das Standardskalarprodukt selbstadjungierten Endomorphismen sind. Wir werden den Spektralsatz für beide Typen von Matrizen beweisen und dabei nur die folgende allgemeinere Eigenschaft benötigen:

Definition 7.1. Wir sagen,

a) eine Matrix $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ sei *normal*, wenn $A^\dagger \cdot A = A \cdot A^\dagger$ gilt.

b) ein Endomorphismus $f \in \mathrm{End}_{\mathbb{K}}(V)$ eines endlich-dimensionalen Euklidischen oder unitären Vektorraumes sei *normal*, wenn $f^\dagger \circ f = f \circ f^\dagger$ ist.

Orthogonale, unitäre und selbstadjungierte Matrizen sind trivialerweise normal, es gibt aber viele weitere Beispiele:

Beispiel 7.2. Für Diagonalmatrizen $A = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \in Gl_n(\mathbb{K})$ gilt:

a) A ist orthogonal bzw. unitär genau dann, wenn $|\lambda_i| = 1$ für alle i ist.

b) A ist selbstadjungiert genau dann, wenn $\lambda_i \in \mathbb{R} \setminus \{0\}$ für alle i ist.

c) A ist normal für beliebige Diagonaleinträge $\lambda_1, \ldots, \lambda_n \in \mathbb{K} \setminus \{0\}$.

Die Bedingung $A^\dagger \cdot A = A \cdot A^\dagger$ ist stabil unter Basiswechseln mit orthogonalen bzw. unitären Basiswechselmatrizen, aber nicht unter anderen Basiswechseln: Z.B. ist die Matrix

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

aus dem Beispiel 6.9 normal. Aber der Basiswechsel S aus demselben Beispiel führt zu der Matrix

$$B := S^{-1}AS = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix},$$

und diese ist nicht normal: Man rechnet leicht nach, dass hier $B^{\mathsf{t}} \cdot B \neq B \cdot B^{\mathsf{t}}$ ist.

Proposition 7.3. *Es sei V ein endlich-dimensionaler Euklidischer oder unitärer Vektorraum. Für normale Endomorphismen $f \in \mathrm{End}_{\mathbb{K}}(V)$ gilt:*

a) Für alle $v \in V$ ist $\|f^\dagger(v)\| = \|f(v)\|$.

b) f und $f^\dagger$ haben dieselben Eigenvektoren. Genauer gilt für alle $v \in V$ und $\lambda \in \mathbb{K}$:

$$f(v) \;=\; \lambda \cdot v \quad\Longleftrightarrow\quad f^\dagger(v) \;=\; \overline{\lambda} \cdot v$$

c) Eigenvektoren von f zu verschiedenen EW sind zueinander orthogonal.

Beweis. Für a) berechnet man

$$\begin{aligned}
\|f(v)\|^2 &= \langle f(v), f(v)\rangle && \text{per Definition der Norm}\\
&= \langle f^\dagger(f(v)), v\rangle && \text{per Definition von } f^\dagger\\
&= \langle f(f^\dagger(v)), v\rangle && \text{per Normalität } f^\dagger \circ f = f \circ f^\dagger\\
&= \langle f^\dagger(v), f^\dagger(v)\rangle && \text{wegen } f = (f^\dagger)^\dagger\\
&= \|f^\dagger(v)\|^2 && \text{per Definition der Norm}
\end{aligned}$$

Die Aussage b) folgt dann aus

$$\begin{aligned}
\|f(v) - \lambda v\|^2 &= \langle f(v) - \lambda v, f(v) - \lambda v\rangle\\
&= \|f(v)\|^2 - \lambda\langle f(v), v\rangle - \overline{\lambda}\langle v, f(v)\rangle + |\lambda|^2\|v\|^2\\
&= \|f^\dagger(v)\|^2 - \lambda\langle v, f^\dagger(v)\rangle - \overline{\lambda}\langle f^\dagger(v), v\rangle + |\lambda|^2\|v\|^2 \quad (\text{nach } a)\\
&= \langle f^\dagger(v) - \overline{\lambda} v, f^\dagger(v) - \overline{\lambda} v\rangle\\
&= \|f^\dagger(v) - \overline{\lambda} v\|^2
\end{aligned}$$

Für c) sei $v_i \in V$ ein Eigenvektor von f zu einem Eigenwert $\lambda_i \in \mathbb{K}$ für $i = 1, 2$, dann gilt

$$\lambda_2\langle v_1, v_2\rangle \;=\; \langle v_1, \lambda_2 v_2\rangle \;=\; \langle v_1, f(v_2)\rangle \;=\; \langle f^\dagger(v_1), v_2\rangle \overset{b)}{=} \langle \overline{\lambda}_1 v_1, v_2\rangle \;=\; \lambda_1\langle v_1, v_2\rangle$$

Somit ist $(\lambda_2 - \lambda_1)\cdot\langle v_1, v_2\rangle = 0$, und im Fall $\lambda_2 \neq \lambda_1$ folgt $\langle v_1, v_2\rangle = 0$. □

Korollar 7.4. *Sei V ein Euklidischer oder unitärer Vektorraum mit $\dim_{\mathbb{K}}(V) < \infty$, und sei ein normaler Endomorphismus $f \in \mathrm{End}_{\mathbb{K}}(V)$ gegeben. Dann ist für jeden Eigenvektor $v \in V$ von f das Orthokomplement*

$$U \;:=\; \big\{\, u \in V \mid \langle u, v\rangle = 0 \,\big\} \;\subseteq\; V \quad \textit{ein } f\textit{-invarianter Unterraum.}$$

Beweis. Sei $f(v) = \lambda v$ mit $\lambda \in \mathbb{K}$. Nach Teil b) von Proposition 7.3 ist $f^\dagger(v) = \overline{\lambda} v$. Somit gilt

$$\langle v, f(u)\rangle \;=\; \langle f^\dagger(v), u\rangle \;=\; \langle \overline{\lambda} v, u\rangle \;=\; \lambda\cdot\langle v, u\rangle$$

und aus $\langle v, u\rangle = 0$ folgt daher wie behauptet $\langle v, f(u)\rangle = 0$. □

Dies führt auf den Spektralsatz, das zentrale Resultat dieses Kapitels. Der Name dieses Satzes kommt daher, dass die Menge der Eigenwerte eines Endomorphismus auch sein *Spektrum* genannt wird. Der Spektralsatz gibt eine vollständige Antwort auf die Frage, wann ein Endomorphismus in einer geeigneten Orthonormalbasis durch eine Diagonalmatrix dargestellt werden kann:

Satz 7.5 (Spektralsatz für Endomorphismen). *Sei V ein endlich-dimensionaler Euklidischer oder unitärer Vektorraum. Dann sind die folgenden Bedingungen für Endomorphismen $f \in \mathrm{End}_{\mathbb{K}}(V)$ äquivalent:*

a) Es existiert eine Orthonormalbasis von V aus Eigenvektoren von f.

b) Es ist f normal und das Polynom $\chi_f(t)$ zerfällt in $\mathbb{K}[t]$ in Linearfaktoren.

Beweis. Wenn $a)$ gilt, sei $\mathscr{B} = (v_1, \ldots, v_n)$ eine Orthonormalbasis und $f(v_i) = \lambda_i v_i$ mit $\lambda_i \in \mathbb{K}$. Dann ist

$$M_{\mathscr{B}}(f) \;=\; \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

eine Diagonalmatrix, also nach Beispiel 7.2 eine normale Matrix. Da es sich hier um die Abbildungsmatrix bezüglich einer Orthogonalbasis handelt, ist dann auch der Endomorphismus f normal. Außerdem zerfällt $\chi_f(t) = \prod_{i=1}^{n}(t - \lambda_i)$ komplett in Linearfaktoren. Somit gelten die Bedingungen in $b)$.

Sei nun umgekehrt $b)$ erfüllt. Da das Polynom $\chi_f(t)$ in $\mathbb{K}[t]$ in Linearfaktoren zerfällt, hat es insbesondere eine Nullstelle, d.h. f hat einen Eigenwert $\lambda \in \mathbb{K}$. Sei dann $v \in V \setminus \{0\}$ ein zugehöriger Eigenvektor. Durch Reskalieren können wir die Normierung

$$\|v\| \;=\; 1$$

erreichen. Wir wollen nun per Induktion über die Dimension von V schließen und betrachten das Orthokomplement

$$U \;:=\; \big\{u \in V \mid u \perp v\big\}.$$

Dies ist ein f-invarianter Unterraum nach Korollar 7.4. Durch Einschränken von f erhalten wir somit einen Endomorphismus

$$f_U : \quad U \longrightarrow U, \quad u \mapsto f(u).$$

Wenn wir zeigen können, dass mit f auch f_U die Voraussetzungen $b)$ erfüllt, gibt es per Induktion über die Dimension wegen

$$\dim_{\mathbb{K}}(U) \;=\; \dim_{\mathbb{K}}(V) - 1$$

eine Orthonormalbasis von U bestehend aus Eigenvektoren von f_U. Indem wir zu dieser Basis noch den zu Beginn gewählten normierten Eigenvektor v hinzufügen, erhalten wir eine Orthonormalbasis von V aus Eigenvektoren von f.

Es bleibt also nur zu prüfen, dass der Endomorphismus $f_U \in \mathrm{End}_{\mathbb{K}}(U)$ normal ist und sein charakteristisches Polynom in $\mathbb{K}[t]$ in Linearfaktoren zerfällt. Um dies zu zeigen, wählen wir zunächst eine beliebige Orthonormalbasis $\mathscr{B}_U = (u_2, \ldots, u_n)$ von U. Dann ist

$$\mathscr{B} := (v, u_2, \ldots, u_n)$$

eine Orthonormalbasis von V und die Abbildungsmatrix von f zu dieser Basis hat die Blockform

$$A := M_{\mathscr{B}}(f) = \left(\begin{array}{c|c} \lambda & 0 \\ \hline 0 & A_U \end{array}\right) \quad \text{mit} \quad A_U := M_{\mathscr{B}_U}(f_U).$$

Insbesondere gilt für die charakteristischen Polynome

$$\chi_f(t) = \chi_A(t) = (t-\lambda) \cdot \chi_{A_U}(t) = (t-\lambda) \cdot \chi_{f_U}(t),$$

sodass mit $\chi_f(t)$ auch das Polynom $\chi_{f_U}(t)$ in $\mathbb{K}[t]$ in Linearfaktoren zerfällt. Für dieses Argument hätten wir noch keine Orthonormalbasis benötigt, diese spielt aber für die Normalität eine Rolle: Da wir $\mathscr{B}$ als Orthonormalbasis gewählt haben, ist die Normalität von f gleichbedeutend mit

$$A^\dagger \cdot A = A \cdot A^\dagger$$

Durch Einsetzen der obigen Blockmatrix für A wird dies zu

$$\left(\begin{array}{c|c} |\lambda|^2 & 0 \\ \hline 0 & A_U^\dagger \cdot A_U \end{array}\right) = \left(\begin{array}{c|c} |\lambda|^2 & 0 \\ \hline 0 & A_U \cdot A_U^\dagger \end{array}\right)$$

und damit folgt

$$A_U^\dagger \cdot A_U = A_U \cdot A_U^\dagger$$

Somit ist auch A_U eine normale Matrix. Da es sich hierbei um die Abbildungsmatrix von f_U bezüglich einer Orthonormalbasis handelt, folgt die Normalität von f_U. □

Bemerkung 7.6 (Spektralzerlegung in Orthogonalprojektionen). Dass V eine Orthonormalbasis aus Eigenvektoren von f besitzt, lässt sich basisfrei auch wie folgt formulieren: Seien $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ die paarweise verschiedenen Eigenwerte von f und

$$p_i : \quad V \twoheadrightarrow U_i = \ker(f - \lambda_i \cdot id_V) \subseteq V$$

die Orthogonalprojektion auf die zugehörigen Eigenräume; dann zerlegt sich die Identitätsabbildung als

$$id_V = \sum_{i=1}^{k} \lambda_i \cdot p_i.$$

Diese Formulierung lässt sich gut verallgemeinern auf den Fall $\dim_{\mathbb{K}} V = \infty$, indem man die Summe durch eine in einem geeigneten Sinn konvergente Reihe oder ein Integral ersetzt. Dazu mehr in der Funktionalanalysis.

Der Vollständigkeit halber halten wir auch noch eine explizite Matrixversion des Spektralsatzes fest:

Korollar 7.7 (Spektralsatz für Matrizen). *Für $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ sind äquivalent:*

a) Es ist A mit einem orthogonalen bzw. unitären Basiswechsel diagonalisierbar, d.h.

$$S^{-1}AS \;=\; \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \quad \textit{für ein} \quad \begin{cases} S \in SO(n) & \textit{im Fall } \mathbb{K} = \mathbb{R}, \\ S \in SU(n) & \textit{im Fall } \mathbb{K} = \mathbb{C}. \end{cases}$$

wobei $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ die Eigenwerte der Matrix A bezeichnen.

b) Es gilt:

- *Die Matrix A ist normal, d.h. $A^\dagger \cdot A = A \cdot A^\dagger$*
- *Im Fall $\mathbb{K} = \mathbb{R}$ ist zusätzlich $\chi_A(t) = \prod_{i=1}^n (t - \lambda_i)$ mit $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.*

Beweis. Dies folgt direkt aus dem vorigen Satz, wenn man dort $V = \mathbb{K}^n$ mit dem Standardskalarprodukt wählt. Nach dem Fundamentalsatz der Algebra zerfällt das charakteristische Polynom im Fall $\mathbb{K} = \mathbb{C}$ immer in Linearfaktoren; nur für $\mathbb{K} = \mathbb{R}$ ist das Zerfallen eine echte Bedingung. Der erhaltene Basiswechsel S ist zunächst nur eine orthogonale bzw. unitäre Matrix, aber durch Reskalieren einer Zeile von S mit einem Skalar λ mit $|\lambda| = 1$ können wir $\det(S) = 1$ erreichen. □

Wir sagen kurz, eine Matrix sei *orthogonal bzw. unitär diagonalisierbar*, wenn sie die Bedingung *a)* erfüllt. Die wichtigsten Beispiele normaler Endomorphismen sind selbstadjungierte Endomorphismen und Isometrien. Wir erhalten:

Korollar 7.8. *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{K})$.*

a) Wenn A symmetrisch bzw. hermitesch ist, also $A = A^\dagger$ gilt, dann ist

- *A orthogonal diagonalisierbar im Fall $\mathbb{K} = \mathbb{R}$,*
- *A unitär diagonalisierbar im Fall $\mathbb{K} = \mathbb{C}$.*

b) Wenn A unitär ist, also $A^\dagger = A^{-1}$ gilt, dann ist A unitär diagonalisierbar.

Beweis. In *a)* ist A selbstadjungiert, in *b)* eine Isometrie, in beiden Fällen also eine normale Matrix. Zu zeigen bleibt nach dem Spektralsatz nur noch, dass für jede reelle symmetrische Matrix A das Polynom $\chi_A(t)$ über $\mathbb{R}$ in Linearfaktoren zerfällt; dazu schreiben wir zunächst

$$\chi_A(t) \;=\; \prod_{i=1}^{n} (t - \lambda_i) \quad \text{mit} \quad \lambda_i \in \mathbb{C}$$

nach dem Fundamentalsatz der Algebra. Da jede reelle symmetrische Matrix auch eine komplexe hermitesche Matrix ist, müssen nach Lemma 6.8 alle ihre Eigenwerte reell sein, d.h. es ist $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ und damit zerfällt $\chi_A(t)$ auch in $\mathbb{R}[t]$ komplett in Linearfaktoren. □

Während also jede reelle symmetrische Matrix orthogonal diagonalisierbar ist, hat das Korollar 7.8 *b*) kein reelles Analogon: Nicht jede orthogonale Matrix ist orthogonal diagonalisierbar — man denke an Drehungen! In den Fällen, wo der Spektralsatz anwendbar ist, liefert er aber zugleich einen Algorithmus, um einen passenden Basiswechsel zu finden:

Algorithmus 7.9 (Spektralzerlegung normaler Matrizen). Sei $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ gegeben mit

$$A^\dagger \cdot A \;=\; A \cdot A^\dagger \quad \text{und} \quad \chi_A(t) \;=\; \prod_{i=1}^{k} (t-\lambda_i)^{e_i}$$

für paarweise verschiedene $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$. Für $i = 1, \ldots, k$ berechne man:

- den Eigenraum $U_i := \ker(A - \lambda_i \cdot \mathbf{1})$,
- eine beliebige Orthonormalbasis $(v_{i1}, \ldots, v_{in_i})$ von U_i (z.B. mit Gram-Schmidt).

Dann ist

$$\mathscr{B} \;:=\; (v_{11}, \ldots, v_{1n_1}, v_{21}, \ldots, v_{2n_2}, \ldots, v_{k1}, \ldots, v_{kn_k})$$

eine Orthonormalbasis von $V = \mathbb{K}^n$ bestehend aus Eigenvektoren zu der Matrix A, und für die aus diesen Basisvektoren als Spalten gebildete orthogonale bzw. unitäre Matrix S gilt

$$S^{-1}AS \;=\; S^\dagger AS \;=\; \mathrm{Diag}(\lambda_1, \ldots, \lambda_1, \ldots, \lambda_k, \ldots, \lambda_k)$$

Beweis. Nach dem Spektralsatz ist A diagonalisierbar, also ist $\mathbb{K}^n = U_1 \oplus \cdots \oplus U_k$ die direkte Summe der Eigenräume. Nach Proposition 7.3 *c*) sind diese Eigenräume paarweise orthogonal zueinander, sodass die Vereinigung von Orthonormalbasen der Eigenräume eine Orthonormalbasis von $\mathbb{K}^n$ ergibt; vgl. Bemerkung 7.6. □

Beispiel 7.10. Gegeben sei die reelle symmetrische Matrix

$$A \;=\; \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \;\in\; \mathrm{Mat}(2 \times 2, \mathbb{R}).$$

Nach dem Spektralsatz ist diese diagonalisierbar. Für ihr charakteristisches Polynom berechnet man

$$\chi_A(t) \;=\; t^2 - 4t + 3 \;=\; (t-1)(t-3)$$

Wir erhalten die Eigenräume

$$\begin{aligned} U_1 \;&:=\; \ker(A - \mathbf{1}) = \mathbb{R}u_1, \\ U_2 \;&:=\; \ker(A - 3\mathbf{1}) = \mathbb{R}u_2, \end{aligned}$$

aufgespannt von den Eigenvektoren

$$u_1 \;:=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{und} \quad u_2 \;:=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

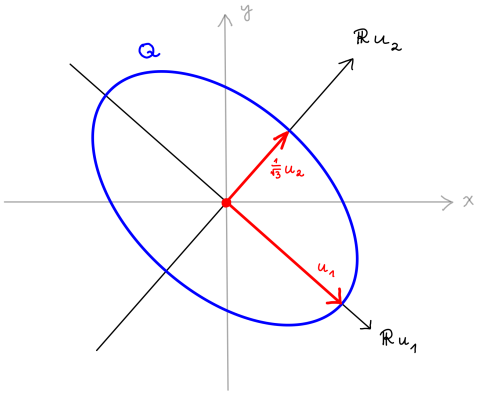
die wir hier auch gleich bezüglich des Standardskalarproduktes normiert haben. Wie erwartet stehen diese beiden Vektoren senkrecht aufeinander, und wir erhalten die Diagonalform

$$S^{-1}AS = S^{\mathrm{t}}AS = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \quad \text{für die Matrix} \quad S := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \in SO(2).$$

Hieraus oder aus dem Hauptminorenkriterium folgt sofort, dass die Matrix A positiv definit ist. Die Menge

$$\begin{aligned} Q &:= \{v \in \mathbb{R}^2 \mid v^{\mathrm{t}} \cdot A \cdot v = 1\} \\ &= \{(x,y)^{\mathrm{t}} \in \mathbb{R}^2 \mid 2x^2 + 2xy + 2y^2 = 1\} \end{aligned}$$

ist eine um $\pi/4$ geneigte Ellipse:



Wir wollen nun allgemeiner solche Lösungsmengen für beliebige symmetrische Matrizen $A \in \mathrm{Mat}(n \times n, \mathbb{R})$ betrachten; die Symmetrie der Matrizen ist dabei keine echte Einschränkung, denn für jede Matrix $B \in \mathrm{Mat}(n \times n, \mathbb{R})$ gilt

$$\begin{aligned} v^{\mathrm{t}} \cdot B \cdot v &= (v^{\mathrm{t}} \cdot B \cdot v)^{\mathrm{t}} && \text{als Transponierte einer } 1 \times 1 \text{ Matrix} \\ &= v^{\mathrm{t}} \cdot B^{\mathrm{t}} \cdot v && \text{wegen } (X \cdot Y \cdot Z)^{\mathrm{t}} = Z^{\mathrm{t}} \cdot Y^{\mathrm{t}} \cdot X^{\mathrm{t}} \end{aligned}$$

und somit $v^{\mathrm{t}} \cdot B \cdot v = v^{\mathrm{t}} \cdot A \cdot v$ für die symmetrische Matrix $A = \frac{1}{2}(B + B^{\mathrm{t}})$.

Korollar 7.11 (Hauptachsentransformation). *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{R})$ symmetrisch und*

$$Q := \{v \in \mathbb{R}^n \mid v^{\mathrm{t}} \cdot A \cdot v = c\}$$

für ein $c \in \mathbb{R}$. Dann gibt es eine Drehung $S \in SO_n(\mathbb{R})$ und Konstanten $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit

$$S \cdot Q = \{(x_1, \ldots, x_n)^{\mathrm{t}} \in \mathbb{R}^n \mid \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 = c\}.$$

Beweis. Der Spektralsatz für symmetrische reelle Matrizen (Korollar 7.8) liefert ein $S \in SO(n)$ mit $S \cdot A \cdot S^t = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$. Mit der Substitution $x = S \cdot v$ und der dazu inversen Substitution $v = S^{-1} \cdot x = S^t \cdot x$ wird dann

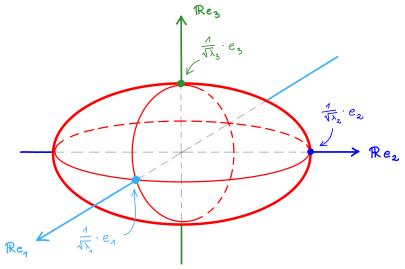
$$\begin{aligned} S \cdot Q \;=\; \{S \cdot v \in \mathbb{R}^n \mid v^t \cdot A \cdot v = c\} \;&=\; \{x \in \mathbb{R}^n \mid (S^{-1}x)^t \cdot A \cdot (S^{-1}x) = c\} \\ &=\; \{x \in \mathbb{R}^n \mid x^t \cdot (S^t \cdot A \cdot S) \cdot x = c\} \\ &=\; \{x \in \mathbb{R}^n \mid x^t \cdot \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \cdot x = c\}. \end{aligned}$$

und es folgt die Behauptung. □

Die Eigenwerte λ_i von A sind bis auf Umordnen eindeutig bestimmt. Die Drehmatrix S muß nicht eindeutig sein, wie man für $A = \mathbf{1}$ sieht. Die von den Spalten von S^t aufgespannten Geraden heißen *Hauptachsen* von Q. Falls $c = 1$ und $\lambda_i > 0$ für alle i ist, erhalten wir ein sogenanntes *Ellipsoid*

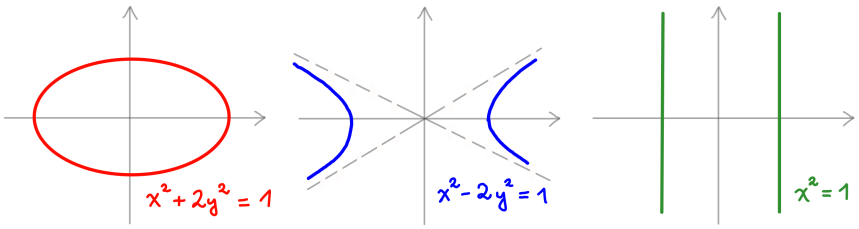
$$\left(\sqrt{\lambda_1} \cdot x_1\right)^2 + \cdots + \left(\sqrt{\lambda_n} \cdot x_n\right)^2 \;=\; 1,$$

mit den Achsenabschnitten $1/\sqrt{\lambda_1}, \ldots, 1/\sqrt{\lambda_n}$ wie in der folgenden Abbildung:



Für $n = 2$ und $c = 1$ gilt:

- Für $\lambda_1, \lambda_2 > 0$ erhalten wir eine Ellipse.
- Für $\lambda_1 > 0 > \lambda_2$ erhalten wir eine Hyperbel.
- Für $\lambda_1 > 0$ und $\lambda_2 = 0$ erhalten wir zwei parallele affine Geraden.
- Für $\lambda_1, \lambda_2 \leq 0$ erhalten wir die leere Menge.



Für die qualitative Unterscheidung der obigen Fälle sind die genauen Eigenwerte nicht wichtig, es geht nur um ihre Vorzeichen. Dies führt auf folgende Klassifikation symmetrischer Bilinearformen im reellen und komplexen Fall:

Satz 7.12 (Trägheitssatz von Sylvester). *Sei V ein $\mathbb{K}$-Vektorraum von endlicher Dimension und*

$$\langle\cdot,\cdot\rangle: \quad V\times V \longrightarrow \mathbb{K}$$

eine hermitesche Sesquilinearform. Dann besitzt V eine Basis $\mathscr{B}$ mit

$$\mathrm{Gram}_{\mathscr{B}}\langle\cdot,\cdot\rangle \;=\; \mathrm{Diag}(\underbrace{1,\ldots,1}_{r},\underbrace{-1,\ldots,-1}_{s},\underbrace{0,\ldots,0}_{t}).$$

Dabei sind r,s,t von der gewählten Basis unabhängig. Es gilt

$$\begin{aligned} r \;&=\; \max\big\{\dim_{\mathbb{K}}(U) \mid U\subseteq V \text{ Unterraum mit } \langle\cdot,\cdot\rangle \text{ positiv definit auf } U\big\} \\ &=\; \text{Anzahl der positiven Eigenwerte (mit Vielfachheiten gezählt)} \\ &\quad\; \text{der Matrix } \mathrm{Gram}_{\mathscr{A}}\langle\cdot,\cdot\rangle \text{ zu einer beliebigen Basis } \mathscr{A} \end{aligned}$$

und analoge Formeln gelten für s, wenn "positiv" durch "negativ" ersetzt wird.

Beweis. Sei $A=\mathrm{Gram}_{\mathscr{A}}\langle\cdot,\cdot\rangle$ für eine zunächst beliebige Basis $\mathscr{A}$. Da $\langle\cdot,\cdot\rangle$ eine hermitesche Form ist, ist die Gram-Matrix hermitesch, also $A^\dagger=A$. Der Spektralsatz für hermitesche Matrizen (Korollar 7.8) liefert daher eine orthogonale bzw. unitäre Matris S mit

$$S^\dagger\cdot A\cdot S \;=\; S^{-1}\cdot A\cdot S \;=\; \mathrm{Diag}(\lambda_1,\ldots,\lambda_n),$$

wobei $\lambda_1,\ldots,\lambda_n$ als Eigenwerte einer hermiteschen Matrix nach Lemma 6.8 reell sind. Aus dem Transformationsverhalten von Gram-Matrizen unter Basiswechsel folgt $\mathrm{Gram}_{\mathscr{C}}\langle\cdot,\cdot\rangle=\mathrm{Diag}(\lambda_1,\ldots,\lambda_n)$ für die Basis $\mathscr{C}=(u_1,\ldots,u_n)$, die aus $\mathscr{A}$ durch Anwenden des Basiswechsels S hervorgeht. Nach Umnumerieren der Basisvektoren finden wir r,s mit

$$\lambda_i \begin{cases} >0 & \text{für } 1\le i\le r, \\ <0 & \text{für } r<i\le r+s, \\ =0 & \text{für } i>r+s. \end{cases}$$

Insbesondere ist r die Zahl der positiven und s die Zahl der negativen Eigenwerte der gegebenen Gram-Matrix. Die Basis $\mathscr{B}=(v_1,\ldots,v_n)$ mit

$$v_i \;:=\; \begin{cases} \frac{1}{|\lambda_i|}\cdot v_i & \text{für } i\le r+s, \\ v_i & \text{für } i>r+s \end{cases}$$

erfüllt $\mathrm{Gram}_{\mathscr{B}}\langle\cdot,\cdot\rangle=\mathrm{Diag}(1,\ldots,1,-1,\ldots,-1,0,\ldots,0)$. Zu zeigen bleibt

$$\begin{aligned} r \;&=\; \max\big\{\dim_{\mathbb{K}}(U) \mid U\subseteq V \text{ Unterraum mit } \langle\cdot,\cdot\rangle \text{ positiv definit auf } U\big\}, \\ s \;&=\; \max\big\{\dim_{\mathbb{K}}(U) \mid U\subseteq V \text{ Unterraum mit } \langle\cdot,\cdot\rangle \text{ negativ definit auf } U\big\}, \end{aligned}$$

denn hieraus folgt zugleich, dass r und s nicht von der Basis $\mathscr{A}$ abhängen. Wir beweisen die Formel für r, die Formel für s zeigt man analog. Per Konstruktion ist die hermitesche Form auf den Unterräumen

$$U_{>0} := \mathbb{K}v_1 \oplus \cdots \oplus \mathbb{K}v_r \quad \text{bzw.} \quad U_{\leq 0} = \mathbb{K}v_{r+1} \oplus \cdots \oplus \mathbb{K}v_n$$

positiv bzw. negativ semidefinit. Sei nun umgekehrt $U \subseteq V$ ein beliebiger Unterraum, auf dem die hermitesche Form positiv definit ist. Wir müssen zeigen, dass dann $\dim_{\mathbb{K}}(U) \geq r$ ist. Zunächst gilt

$$U \cap U_{\leq 0} = \{0\},$$

denn auf einem von Null verschiedenen Vektorraum kann keine hermitesche Form zugleich positiv definit und negativ semidefinit sein. Also ist $U + U_{\leq 0} \subseteq V$ eine direkte Summe. Es folgt

$$n = \dim_{\mathbb{K}}(V) \geq \dim_{\mathbb{K}}(U \oplus U_{\leq 0}) = \dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(U_{\leq 0}) = \dim_{\mathbb{K}}(U) + (n-r),$$

also $\dim_{\mathbb{K}}(U) \leq r$ wie gewünscht. Die Formel für s folgt analog. □

Definition 7.13. Das Tripel (r,s,t) heißt *Index* oder *Signatur* der hermiteschen Form. Falls $t = 0$ ist, heißt die hermitesche Form *nichtausgeartet*; dies ist der Fall genau dann, wenn ihre Gram-Matrix zu einer beliebigen Basis invertierbar ist. Wir nennen dann auch das Paar (r,s) die Signatur der hermiteschen Form.

Korollar 7.14. *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ mit $A^\dagger = A$. Dann gibt es ein $S \in \mathrm{GL}_n(\mathbb{K})$ mit*

$$S^\dagger \cdot A \cdot S = \mathrm{Diag}(\underbrace{1,\ldots,1}_{r},\underbrace{-1,\ldots,-1}_{s},\underbrace{0,\ldots,0}_{t}).$$

Dabei ist

$$r = \text{Anzahl der Eigenwerte } \lambda > 0 \text{ von } A \text{ (mit Vielfachheiten gezählt)},$$

$$s = \text{Anzahl der Eigenwerte } \lambda < 0 \text{ von } A \text{ (mit Vielfachheiten gezählt)},$$

und $t = \dim_{\mathbb{K}} \ker(A)$. Wir nennen $sgn(A) := (r,s,t)$ die Signatur *der Matrix A.*

Beweis. Satz 7.12 für $V = \mathbb{K}^n$ mit der hermiteschen Form $(v,w) \mapsto \bar{v}^{\mathsf{t}} \cdot A \cdot w$. □

Die Matrix S ist in der Regel *nicht* orthogonal bzw. unitär: Ihre Spalten bilden per Konstruktion ein Orthogonalsystem bzgl. der durch A definierten hermiteschen Form, nicht bzgl. des Standardskalarproduktes. Die Matrizen $S^\dagger \cdot A \cdot S$ und A können daher verschiedene Eigenwerte haben. Der Satz von Sylvester besagt jedoch, dass die Eigenwerte von A und von $S^\dagger \cdot A \cdot S$ die gleichen Vorzeichen haben.

Korollar 7.15. *Sei $A \in \mathrm{Mat}(n \times n, \mathbb{K})$ mit $A^\dagger = A$, und es bezeichne $\mathscr{S}(A) \subset \mathbb{R}$ die Menge ihrer Eigenwerte. Dann gilt:*

$$\begin{aligned}
A \text{ positiv definit} &\iff \mathscr{S}(A) \subset \mathbb{R}_{>0} \iff sgn(A) = (n,0,0)\\
A \text{ negativ definit} &\iff \mathscr{S}(A) \subset \mathbb{R}_{<0} \iff sgn(A) = (0,n,0)\\
A \text{ positiv semidefinit} &\iff \mathscr{S}(A) \subset \mathbb{R}_{\geq 0} \iff sgn(A) = (n-t,0,t)\\
A \text{ negativ semidefinit} &\iff \mathscr{S}(A) \subset \mathbb{R}_{\leq 0} \iff sgn(A) = (0,n-t,t)
\end{aligned}$$

Beweis. Sei $S \in \mathrm{GL}_n(\mathbb{K})$ mit $S^\dagger \cdot A \cdot S = \mathrm{Diag}(1,\ldots,1,-1,\ldots,-1,0,\ldots,0)$. Die Diagonaleinträge haben nach dem Trägheitssatz die gleichen Vorzeichen wie die Eigenwerte von A. Nach der Transformationsformel für Sesquilinearformen unter Basiswechsel beschreibt die Matrix $S^\dagger \cdot A \cdot S$ dieselbe Sesquilinearform wie A, nur in einer anderen Basis. Also ist A positiv definit genau dann, wenn $S^\dagger \cdot A \cdot S$ es ist, und analog für die anderen Definitheitseigenschaften. □

Zum Schluß dieses Kapitels wollen wir eine Anwendung des Spektralsatzes für nicht notwendig quadratische Matrizen betrachten:

Satz 7.16 (Singulärwertzerlegung). *Seien $m,n \in \mathbb{N}$. Für jedes $A \in \mathrm{Mat}(m \times n, \mathbb{K})$ gibt es*

a) positive reelle Zahlen $\lambda_1,\ldots,\lambda_r > 0$,

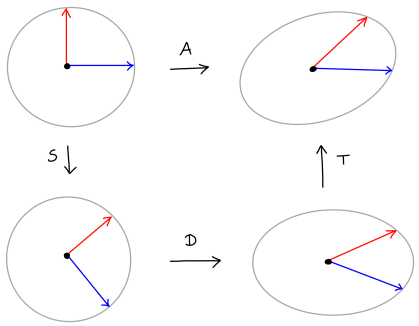
b) orthogonale bzw. unitäre Matrizen

$$S \in \begin{cases} O(m) \\ U(m) \end{cases} \quad \text{und} \quad T \in \begin{cases} O(n) \\ U(n) \end{cases} \quad \text{im Fall} \quad \mathbb{K} = \begin{cases} \mathbb{R} \\ \mathbb{C} \end{cases}$$

sodass gilt:

$$A = S \cdot D \cdot T \quad \text{für die Diagonalmatrix} \quad D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_r \end{pmatrix} \in \mathrm{Mat}(m \times n, \mathbb{K}).$$

Dabei ist $r = \mathrm{rk}(A)$. Die Zahlen $\lambda_1,\ldots,\lambda_r$ sind bis auf die Reihenfolge eindeutig bestimmt und werden als die Singulärwerte *der Matrix A bezeichnet.*



Beweis. Wir beginnen mit der Eindeutigkeit. Wenn eine solche Zerlegung existiert, ist offenbar $r = \mathrm{rk}(D) = \mathrm{rk}(A)$. Um die Eindeutigkeit der Singulärwerte $\lambda_1, \ldots, \lambda_r$ zu zeigen, beachte man, dass es sich hierbei um positive reelle Zahlen handelt; es genügt daher, die Eindeutigkeit ihrer Quadrate $\lambda_1^2, \ldots, \lambda_r^2$ zu zeigen. Diese Quadrate sind aber genau die von Null verschiedenen Eigenwerte der Diagonalmatrix

$$D^\dagger \cdot D \;=\; D^\dagger \cdot S^\dagger \cdot S \cdot D$$

und diese stimmen überein mit den von Null verschiedenen Eigenwerten der hierzu ähnlichen Matrix

$$T^{-1} \cdot D^\dagger \cdot D \cdot T \;=\; T^\dagger \cdot D^\dagger \cdot S^\dagger \cdot S \cdot D \cdot T \;=\; (SDT)^\dagger \cdot (SDT) \;=\; A^\dagger \cdot A.$$

Da die Matrix auf der rechten Seite nicht von der Singulärwertzerlegung, sondern nur von der gegebenen Matrix A abhängt, gilt dasselbe auch für ihre Eigenwerte.

Zu zeigen bleibt die Existenz der Singulärwertzerlegung. Dazu lesen wir das obige Argument rückwärts und betrachten zunächst die Matrix $B := A^\dagger \cdot A$. Diese ist hermitesch wegen

$$B^\dagger = (A^\dagger \cdot A)^\dagger = A^\dagger \cdot (A^\dagger)^\dagger = A^\dagger \cdot A = B.$$

Nach dem Spektralsatz für symmetrische bzw. hermitesche Matrizen (Korollar 7.8) existiert somit eine orthogonale bzw. unitäre Matrix T mit

$$T \cdot B \cdot T^\dagger = \mathrm{Diag}(d_1, \ldots, d_n) \quad \text{für geeignete} \quad d_1, \ldots, d_n \in \mathbb{K}.$$

Da die Matrix B hermitesch ist, sind ihre Eigenwerte d_i reell nach Lemma 6.8. Nach Korollar 7.15 ist zudem $d_i \geq 0$, denn B ist positiv semidefinit wegen

$$\overline{v}^{\mathrm{t}} \cdot B \cdot v \;=\; \overline{v}^{\mathrm{t}} \cdot A^\dagger \cdot A \cdot v \;=\; (Av)^\dagger \cdot (Av) \;=\; \|Av\|^2 \;\geq\; 0 \quad \text{für alle} \quad v \in V.$$

Durch Umnumerieren dürfen wir $d_1, \ldots, d_r > 0$ und $d_i = 0$ für alle $i > r$ annehmen. Wir setzen $\lambda_i := \sqrt{d_i}$ für $i = 1, \ldots, r$ und versuchen es mit der Diagonalmatrix

$$D \;:=\; \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_r \\ & & \end{pmatrix} \;\in\; \mathrm{Mat}(m \times n, \mathbb{K}).$$

Per Konstruktion ist dann $D^\dagger \cdot D = T \cdot B \cdot T^\dagger = T \cdot A^\dagger \cdot A \cdot T^\dagger = (AT^\dagger)^\dagger \cdot (AT^\dagger)$. Für die Spaltenvektoren

$$v_i \;:=\; A \cdot T^\dagger \cdot e_i$$

gilt somit

$$\overline{v}_i^{\mathrm{t}} \cdot v_j \;:=\; \begin{cases} \lambda_i^2 & \text{falls } i = j \text{ ist} \\ 0 & \text{falls } i \neq j \text{ oder } i = j > r \text{ ist.} \end{cases}$$

Wenn wir $u_i := \lambda_i^{-1} v_i$ für $i \leq r$ setzen, folgt:

- Es ist $v_{r+1} = \cdots = v_n = 0$.
- Die Vektoren $u_1, \ldots, u_r$ mit $u_i := \lambda_i^{-1} \cdot v_i$ bilden ein Orthonormalsystem.

Wir ergänzen dieses Orthonormalsystem zu einer Orthonormalbasis $(u_1, \ldots, u_m)$ und erhalten

$$A \cdot T^\dagger \;=\; \begin{pmatrix} | & & | \\ v_1 & \cdots & v_m \\ | & & | \end{pmatrix} \;=\; \begin{pmatrix} | & & | & | & | \\ \lambda_1 u_1 & \cdots & \lambda_r u_r & 0 & \cdots\ 0 \\ | & & | & | & | \end{pmatrix} \;=\; S \cdot D$$

für die Matrix

$$S \;:=\; \begin{pmatrix} | & & | \\ u_1 & \cdots & u_m \\ | & & | \end{pmatrix} \;\in\; \mathrm{Mat}(m \times m, \mathbb{K}).$$

Die Matrix S ist orthogonal bzw. unitär, da ihre Spalten ein Orthonormalsystem bilden, und aus der Identität $A \cdot T^\dagger = S \cdot D$ folgt $A = SDT^\dagger$ wie gewünscht. □

Bemerkung 7.17. Die Singulärwertzerlegung liefert eine praktische Methode, um Matrizen von kleinem Rang effizient zu speichern: Um das Produkt $S \cdot D \cdot T^\dagger$ zu berechnen, müssen wir nur

- die ersten r Spalten von $S \in \mathrm{Mat}(m \times m, \mathbb{K})$,
- die ersten r Zeilen von $T \in \mathrm{Mat}(n \times n, \mathbb{K})$, und
- die Singulärwerte $\lambda_1, \ldots, \lambda_r \in \mathbb{R}_{>0}$

kennen, insgesamt also

$$mr + r + rn \;=\; r \cdot (m + n + 1)$$

reelle Zahlen. Für Matrizen vom Rang $r \ll \min\{m,n\}$ sind das deutlich weniger als die $m \cdot n$ Einträge der Matrix A. Solche Matrizen lassen sich also mithilfe ihrer Singulärwertzerlegung verlustfrei in sehr kompakter Form speichern! Für Matrizen von großem Rang kann man dieselbe Idee zur verlustbehafteten Komprimierung verwenden: Dazu ordnet man die Singulärwerte von $A = SDT$ mit $\mathrm{rk}(A) = r$ der Größe nach als

$$\lambda_1 \geq \cdots \geq \lambda_r > 0$$

an. Wenn ein $s \ll r$ existiert, sodass die ersten s Singulärwerte deutlich größer als die übrigen sind, dann wird A sehr gut approximiert durch

$$A' \;=\; SD'T \quad \text{mit} \quad D' = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_s \\ & & \end{pmatrix}.$$

Man kommt so mit $s \cdot (m + n + 1) \ll m \cdot n$ Zahlen aus. Dies wird z.B. benutzt zur Bildkompression, wobei jeder Matrixeintrag die Farbe eines Pixels speichert.

Kapitel III
Multilineare Algebra

Zusammenfassung Das Skalarprodukt auf einem Euklidischen Vektorraum ist ein Beispiel für eine symmetrische Bilinearform, die Determinante einer Matrix eine alternierende Multilinearform. In diesem Kapitel werden wir allgemeiner beliebige multilineare Abbildungen mittels Tensorprodukten beschreiben. Im symmetrischen bzw. alternierenden Fall führt dies auf symmetrische und äußere Algebren: Erstere kann man als Polynomringe in mehreren Variablen verstehen, letztere liefern einen Kalkül für Untervektorräume, Determinanten und Differentialformen, der sich in der Analysis und Geometrie als sehr nützlich erweisen wird.

Kapitel IV
Moduln über Hauptidealringen

Zusammenfassung In diesem Kapitel studieren wir die Struktur von Moduln über Hauptidealringen, eine wichtige Verallgemeinerung von Vektorräumen über Körpern. Die Klassifikation solcher Moduln liefert als Spezialfälle den Haupsatz für endlich erzeugte abelsche Gruppen und eine Verallgemeinerung der Jordan-Normalform für nicht trigonalisierbare Matrizen.

1 Moduln über Ringen

Die Definition von Moduln über einem Ring sieht formal genauso aus wie die von Vektorräumen über einem Körper:

Definition 1.1. Sei R ein Ring. Ein *Modul über R* oder *R-Modul* ist eine abelsche Gruppe $(V,+)$ mit einer Abbildung

$$\cdot : \quad R \times V \longrightarrow V, \quad (\alpha, v) \mapsto \alpha \cdot v,$$

der Skalarmultiplikation, sodass für alle $\alpha, \beta \in R$, $v, w \in V$ gilt:

a) Assoziativität: $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$.

b) Distributivität: $(\alpha+\beta) \cdot v = \alpha \cdot v + \beta \cdot v$
$\alpha \cdot (v+w) = \alpha \cdot v + \alpha \cdot w$.

c) Kompatibilität mit der Eins: $1 \cdot v = v$.

Beispiel 1.2. Es gilt:

a) Moduln über Körpern $R = K$ sind dasselbe wie K-Vektorräume.

b) Moduln über dem Ring $R = \mathbb{Z}$ sind dasselbe wie abelsche Gruppen.

c) Jeder Ring R ist ein Modul über sich selbst via Linksmultiplikation.

Beweis. Teil $a)$ gilt per Definition. Für Teil $b)$ beachte man, dass für $\mathbb{Z}$-Moduln die Skalarmultiplikation bereits eindeutig festgelegt ist durch die zugrundeliegende Gruppe $(V,+)$: Für $n \in \mathbb{N}$ und $v \in V$ gilt wegen Distributivität und Kompatibilität mit der Eins

$$n \cdot v \;=\; (1+\cdots+1)\cdot v \;=\; 1\cdot v+\cdots+1\cdot v \;=\; v+\cdots+v$$

und für die Skalarmultiplikation mit negativen ganzen Zahlen ist $(-n)\cdot v = -(n\cdot v)$ wegen

$$(-n)\cdot v + n\cdot v \;=\; ((-n)+n))\cdot v \;=\; 0\cdot v \;=\; 0.$$

Umgekehrt definieren diese Gleichungen auf jeder abelschen Gruppe $(V,+)$ die Struktur eines $\mathbb{Z}$-Moduls. Man beachte, dass die Gruppe *abelsch* sein muß, damit die Distributivität

$$\begin{aligned} n\cdot(v+w) \;&=\; (v+w)+\cdots+(v+w) \\ &=\; (v+\cdots+v)+(w+\cdots+w) \;=\; n\cdot v + n\cdot w \end{aligned}$$

erfüllt ist. Für Teil $c)$ versehen wir die additive Gruppe $V = (R,+)$ mit der durch Multiplikation in dem Ring R gegebenen Skalarmultiplikation. Die Modulaxiome folgen dabei sofort aus den Axiomen für Ringe. □

Viele unserer bisherigen Definitionen für Vektorräume übertragen sich direkt auf den allgemeineren Fall von R-Moduln:

Definition 1.3. Ein *Untermodul* eines R-Moduls V ist eine Teilmenge $U \subseteq V$ mit den folgenden beiden Eigenschaften:

a) $(U,+) \subseteq (V,+)$ ist eine additive Untergruppe.

b) Es gilt $\alpha \cdot u \in U$ für alle $u \in U$ und alle $\alpha \in K$.

Beispiel 1.4. Untermoduln von...

a) Vektorräumen sind dasselbe wie Untervektorräume.

b) abelschen Gruppen (d.h. $\mathbb{Z}$-Moduln) sind dasselbe wie Untergruppen.

Der Begriff eines Homomorphismus von Vektorräumen oder von abelschen Gruppen verallgemeinert sich wie folgt:

Definition 1.5. Ein *Modulhomomorphismus* ist eine Abbildung $\varphi : V \longrightarrow W$ von einem R-Modul V in einen R-Modul W mit

$$\varphi(\alpha_1\cdot v_1 + \alpha_2 \cdot v_2) \;=\; \alpha_1\cdot\varphi(v_1) + \alpha_2\cdot\varphi(v_2) \quad \text{für alle} \quad \alpha_1,\alpha_2 \in R, v_1, v_2 \in V.$$

Wir bezeichnen mit $\mathrm{Hom}_R(V,W)$ die Menge aller solcher Homomorphismen. Ein bijektiver Modulhomomorphismus heißt ein *Isomorphismus von R-Moduln*.

Beispiel 1.6. Sei R ein *kommutativer* Ring und V ein R-Modul. Dann ist für jedes feste $r \in R$ die Abbildung

$$\varphi_r : \quad V \longrightarrow V, \quad v \mapsto r \cdot v$$

ein Homomorphismus von R-Moduln, denn für alle $v_1, v_2 \in V$ und $r_1, r_2 \in R$ gilt

$$\begin{aligned}
\varphi_r(r_1 \cdot v_1 + r_2 \cdot v_2) &= r \cdot (r_1 \cdot v_1 + r_2 \cdot v_2) && \text{per Definition} \\
&= (r \cdot r_1) \cdot v_1 + (r \cdot r_2) \cdot v_2 && \text{nach den Modulaxiomen} \\
&= (r_1 \cdot r) \cdot v_1 + (r_2 \cdot r) \cdot v_2 && \text{weil } R \text{ kommutativ ist} \\
&= r_1 \cdot (r \cdot v_1) + r_2 \cdot (r \cdot v_2) && \text{nach den Modulaxiomen} \\
&= r_1 \cdot \varphi_r(v_1) + r_2 \cdot \varphi(v_2) && \text{per Definition}
\end{aligned}$$

Bemerkung 1.7. Seien V, W Moduln über einem Ring R. Wie für abelsche Gruppen und Vektorräume sieht man, dass für jeden Homomorphismus $\varphi \in \mathrm{Hom}_R(V,W)$ der *Kern* und das *Bild*

$$\begin{aligned}
\ker(\varphi) &:= \{v \in V \mid \varphi(v) = 0\} \subseteq V \\
\mathrm{im}(\varphi) &:= \{f(v) \in W \mid v \in V\} \subseteq W
\end{aligned}$$

Untermoduln sind. Umgekehrt kann man jeden Untermodul $U \subseteq V$ eines R-Moduls als Kern eines Homomorphismus von Moduln schreiben: Wir definieren dazu auf der Quotientengruppe $(W,+) := (V/U,+)$ eine Skalarmultiplikation durch

$$R \times W \longrightarrow W, \quad r \cdot [v] \mapsto [r \cdot v].$$

Wie im Fall von Vektorräumen sieht man, dass diese wohldefiniert ist und $W = V/U$ zu einem R-Modul macht, sodass

$$p : \quad V \twoheadrightarrow W = V/U, \quad v \mapsto [v]$$

ein Modulhomomorphismus mit $\ker(p) = U$ ist.

Beispiel 1.8. Falls R ein *kommutativer* Ring ist, dann ist für jedes feste $r \in R$ die Abbildung $\varphi_r : V \longrightarrow V, v \mapsto r \cdot v$ ein Modulhomomorphismus. Im Gegensatz zur Situation für Vektorräume muß dieser für $r \neq 0$ nicht injektiv sein, da in Ringen keine Kürzungsregel gilt! Untermoduln der Form

$$\ker(\varphi_r) = \{v \in V \mid r \cdot v = 0\} \subseteq V$$

sagen viel über die Struktur von Moduln aus: Für $R = \mathbb{Z}$ und $V = \mathbb{Z}/6\mathbb{Z}$ ist z.B.

$$\begin{aligned}
\ker(\varphi_2) &= \{[0],[3]\} \simeq \mathbb{Z}/2\mathbb{Z}, \\
\ker(\varphi_3) &= \{[0],[2],[4]\} \simeq \mathbb{Z}/3\mathbb{Z},
\end{aligned}$$

und es gilt $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (als Produkt abelscher Gruppen).

Das Pendant zum Produkt abelscher Gruppen ist im Fall von Vektorräumen die direkte Summe. Beide sind Spezialfälle der folgenden Konstruktion:

Definition 1.9. Die *externe direkte Summe* von R-Moduln $V_1, \dots, V_n$ ist definiert als das mengentheoretische Produkt

$$V_1 \oplus \cdots \oplus V_n \;:=\; V_1 \times \cdots \times V_n$$

mit der komponentenweisen Addition und Skalarmultiplikation

$$\begin{aligned}(v_1, \dots, v_n) + (w_1, \dots, w_n) \;&:=\; (v_1 + w_1, \dots, v_n + w_n),\\ \alpha \cdot (v_1, \dots, v_n) \;&:=\; (\alpha v_1, \dots, \alpha v_n).\end{aligned}$$

Auch hier gibt es ein analoges Konzept einer internen Summe:

Definition 1.10. Sei V ein R-Modul. Für Untermoduln $U_1, \dots, U_n \subseteq V$ haben wir einen Modulhomomorphismus

$$\varphi: \quad U_1 \oplus \cdots \oplus U_n \;\longrightarrow\; V, \quad (u_1, \dots, u_n) \;\mapsto\; u_1 + \cdots + u_n$$

Wir nennen V die *interne direkte Summe* der gegebenen Untermoduln, wenn φ ein Isomorphismus ist. In diesem Fall schreiben wir auch

$$V \;=\; U_1 \oplus \cdots \oplus U_n$$

und sparen uns die Unterscheidung zwischen interner und externer direkter Summe.

Definition 1.11. Sei V ein R-Modul. Der von $v_1, \dots, v_n \in V$ *erzeugte Untermodul* ist

$$Rv_1 + \cdots + Rv_n \;:=\; \big\{\, r_1 v_1 + \cdots + r_n v_n \in V \mid r_1, \dots, r_n \in R \big\} \;\subseteq\; V.$$

Dieser Untermodul ist das Bild des Homomorphismus

$$\varphi: \quad R^n \;=\; R \oplus \cdots \oplus R \;\longrightarrow\; V, \quad (r_1, \dots, r_n) \;\mapsto\; r_1 v_1 + \cdots + r_n v_n,$$

und wir nennen

a) $(v_1, \dots, v_n)$ ein *Erzeugendensystem* des Moduls, wenn φ surjektiv ist,

b) $(v_1, \dots, v_n)$ eine *Basis* des Moduls, wenn φ ein Isomorphismus ist,

Ein R-Modul heißt

a) *endlich erzeugt*, wenn er ein endliches Erzeugendensystem hat,

b) *endlich erzeugter freier Modul*, wenn er eine endliche Basis hat.

An dieser Stelle wird es für Moduln über Ringen interessanter:

Beispiel 1.12. Der $\mathbb{Z}$-Modul $V = \mathbb{Z}/2\mathbb{Z}$ ist endlich erzeugt, aber hat keine Basis!

Um dies in den Griff zu bekommen, müssen wir etwas mehr über Ringe wissen.

2 Ideale und Hauptidealringe

Die Frage nach den möglichen Quotienten des R-Moduls $V = R$ ist äquivalent zu der Frage nach seinen Untermoduln. Diese haben einen eigenen Namen:

Definition 2.1. Ein *Linksideal* eines Ringes R ist ein Untermodul von $V = R$, also eine additive Untergruppe $I \subseteq (R,+)$ mit

$$ra \in I \quad \text{für alle } r \in R \text{ und } a \in I.$$

Man beachte, dass wir gemäß unserer Konventionen für Vektorräume und Moduln die Skalarmultiplikation immer von links schreiben!

Wir werden es in diesem Kapitel nur mit kommutativen Ringen zu tun haben, für diese ist jedes Linksideal sogar ein Ideal in dem folgenden stärkeren Sinne:

Definition 2.2. Ein *Ideal* eines Ringes R ist eine additive Untergruppe $I \subseteq (R,+)$ mit

$$ra \in I \quad \text{und} \quad ar \in I \quad \text{für alle } r \in R \text{ und } a \in I.$$

In diesem Fall ist R/I nicht nur ein R-Modul, sondern zugleich ein Ring:

Bemerkung 2.3. Sei R ein Ring und $I \subseteq R$ ein Ideal, dann ist der Quotient R/I ein Ring mit der repräsentantenweisen Addition und Multiplikation:

$$\begin{aligned} [a]+[b] &:= [a+b], \\ [a]\cdot[b] &:= [a\cdot b]. \end{aligned}$$

Beweis. Wie für abelsche Gruppen. Wir prüfen hier nur die Wohldefiniertheit der Multiplikation: Für $a,a',b \in R$ gilt

$$\begin{aligned} [a]=[a'] &\implies a-a' \in I && \text{(per Definition)} \\ &\implies (a-a')\cdot b \in I && \text{(weil } I \text{ Ideal ist)} \\ &\implies ab-a'b \in I && \text{(Distributivität)} \\ &\implies [ab]=[a'b] && \text{(per Definition)} \end{aligned}$$

Analog erhält man auch $[ba]=[ba']$. □

Beispiel 2.4. Für $R = \mathbb{Z}$ erhalten wir die Quotientenringe $\mathbb{Z}/n\mathbb{Z}$, die wir bereits aus dem ersten Kapitel kennen. Allgemeiner ist für beliebige kommutative Ringe R und jedes $a \in R$ die Teilmenge

$$aR := \{ar \in R \mid r \in R\} \subseteq R$$

ein Ideal. Es heißt das von dem Element d erzeugte *Hauptideal*.

Für $R = \mathbb{Z}$ hatten wir mittels des Euklidischen Algorithmus gesehen, dass jede additive Untergruppe und damit – was hier dasselbe ist – jedes Ideal die Form $I = n\mathbb{Z}$ mit $n \in \mathbb{Z}$ hat, also ein Hauptideal ist. Diese Eigenschaft wird im Folgenden eine zentrale Rolle spielen und verdient einen Namen:

Definition 2.5. Ein *Hauptidealring* ist ein Integritätsring R, in dem jedes Ideal ein Hauptideal $aR \subseteq R$ ist.

Eine wichtige Klasse von Beispielen sind Euklidische Ringe. Wir erinnern kurz an die Definition: Ein *Euklidischer Ring* ist ein Integritätsring R, für den es eine Funktion

$$\delta\colon \quad R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

gibt, sodass für alle $a \in R$, $b \in R \setminus \{0\}$ Elemente $q, r \in R$ existieren mit

a) $a = qb + r$, und

b) $\delta(r) < \delta(b)$ im Fall $r \neq 0$.

Wir nennen dann δ eine *Gradfunktion* des Euklidischen Ringes R.

Beispiel 2.6. Folgende Ringe R sind Euklidisch mit der Gradfunktion δ:

a) $R = \mathbb{Z}$ mit dem Absolutbetrag $\delta(a) := |a|$.

b) $R = K[x]$ für einen Körper K, mit dem Grad von Polynomen $\delta(f) := \deg(f)$.

Es gilt:

Satz 2.7. *Jeder Euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R Euklidisch mit Gradfunktion $\delta : R \setminus \{0\} \to \mathbb{N}$. Sei $I \subseteq R$ ein Ideal, wobei wir oBdA $I \neq \{0\}$ annehmen dürfen. Wähle ein Element $a \in I$, sodass $\delta(a)$ minimal ist. Wegen $a \in I$ ist dann jedenfalls $aR \subseteq I$. Wir wollen zeigen, dass hier sogar Gleichheit gilt. Sei dazu $b \in I$ vorgegeben. Dann gibt es $q, r \in R$ mit

$$b \;=\; aq + r \quad \text{und} \quad \delta(r) < \delta(a) \quad \text{im Fall} \quad r \neq 0.$$

Aber $r = b - aq \in I$, weil I ein Ideal ist. Die Minimalität von $\delta(a)$ erzwingt $r = 0$ und wir erhalten somit $b = aq \in aR$. Also ist $I = aR$. □

Man beachte: Polynomringe in mehreren Variablen sind keine Hauptidealringe, ebensowenig wie der Ring

$$\mathbb{Z}[t] \;:=\; \left\{ a_n t^n + \cdots + a_1 t + a_0 \mid n \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{Z} \right\}$$

der Polynome in einer Variablen mit ganzzahligen Koeffizienten (Übungsaufgabe)!

3 Teilbarkeit in Hauptidealringen

Bekanntlich hat jede von Null verschiedene ganze Zahl $a \in \mathbb{Z} \setminus \{0\}$ eine eindeutige Primfaktorzerlegung

$$a \;=\; c \cdot \prod_{i=1}^{n} p_i^{e_i}$$

mit $c = \pm 1$, Exponenten $e_i \in \mathbb{N}$ und paarweise verschiedenen Primzahlen p_i. Wir wollen eine analoge Aussage in beliebigen Hauptidealringen zeigen, mit Blick auf den Hauptidealring $K[t]$ über einem Körper K. Wenn K algebraisch abgeschlossen ist, lässt sich dies besonders einfach formulieren: Dann hat jedes $f \in K[t] \setminus \{0\}$ eine eindeutige Zerlegung

$$f(t) \;=\; c \cdot \prod_{i=1}^{n} (t - \lambda_i)^{e_i}$$

mit einer Konstante $c \in K^\times$, Exponenten $e_i \in \mathbb{N}$ und paarweise verschiedenen $\lambda_i \in K$, die Rolle von Primzahlen übernehmen hier also die Polynome vom Grad 1.

Über nicht algebraisch abgeschlossenen Körpern stellt sich die Frage, welche Polynome die Rolle von Primzahlen übernehmen sollen. Primzahlen $p > 1$ kann man durch jede der folgenden äquivalenten Eigenschaften charakterisieren:

1) Aus $p \mid ab$ für $a, b \in \mathbb{Z}$ folgt $p \mid a$ oder $p \mid b$.
2) Aus $p = ab$ mit $a, b \in \mathbb{Z}$ folgt $a = \pm 1$ oder $b = \pm 1$.

Die Vorzeichen in der zweiten Charakterisierung werden benötigt für die trivialen Faktorisierungen $p = c \cdot (p/c)$ für alle $c \in \mathbb{Z}^\times = \{\pm 1\}$. Dies führt auf folgende Definition:

Definition 3.1. Sei R ein Integritätsring. Ein Element $p \in R$ heißt

- *assoziiert zu* $a \in R$, wenn $a = pc$ für ein $c \in R^\times$ ist. Wir schreiben dann $p \sim a$.
- ein *Teiler von* $a \in R$, wenn $a = pc$ für ein $c \in R$ ist. Wir schreiben dann $p \mid a$.
- ein *Primelement*, wenn $p \notin R^\times \cup \{0\}$ ist und für alle $a, b \in R$ gilt:

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ oder } p \mid b.$$

- ein *irreduzibles Element*, wenn $p \notin R^\times \cup \{0\}$ ist und für alle $a, b \in R$ gilt:

$$p \mid ab \quad \Longrightarrow \quad a \in R^\times \text{ oder } b \in R^\times.$$

- *reduzibel*, wenn es nicht irreduzibel ist.

Beispiel 3.2. a) Das Polynom

$$p(t) \;=\; t^2 + 1 \quad \text{ist} \quad \begin{cases} \text{irreduzibel im Ring } R = \mathbb{R}[t], \\ \text{reduzibel in } R = \mathbb{C}[t]. \end{cases}$$

b) Jedes Polynom $p \in K[t]$ mit $\deg(p) = 1$ ist irreduzibel:

$$\begin{aligned} p = ab &\implies \deg(a) + \deg(b) = 1 \\ &\implies \deg(a) = 0 \textit{ oder } \deg(b) = 0 \\ &\implies a \in K^\times \textit{ oder } b \in K^\times \end{aligned}$$

c) Über algebraisch abgeschlossenen Körpern K gilt auch die Umkehrung von b).

Ein Polynom heißt *normiert*, wenn sein Leitkoeffizient gleich Eins ist. Es gilt:

Lemma 3.3. *Die normierten irreduziblen reellen Polynome $f \in \mathbb{R}[t]$ sind genau die Polynome der Form*

- $f(t) = x - a$ *mit* $a \in \mathbb{R}$,
- $f(t) = x^2 + bx + c$ *mit* $b, c \in \mathbb{R}$ *und* $b^2 < 4c$.

Beweis. Sei $f \in \mathbb{R}[t]$ irreduzibel. Nach dem Fundamentalsatz der Algebra hat f eine Nullstelle $a \in \mathbb{C}$, also ist $f(t) = (t-a) \cdot g(t)$ für ein $g(t)\mathbb{C}[t]$. Falls $a \in \mathbb{R}$ ist, muß dabei $g(t) \in \mathbb{R}[t]$ sein. Da f ein normiertes und irreduzibles Polynom in $\mathbb{R}[t]$ ist, folgt dann notwendigerweise $f(t) = t - a$. Falls $a \in \mathbb{C} \setminus \mathbb{R}$ ist, ist das komplex Konjugierte $\overline{a} \neq a$. Da f reelle Koeffizienten hat, gilt aber

$$f(\overline{a}) \;=\; \overline{f(a)} \;=\; \overline{0} \;=\; 0.$$

Aus $f(t) = (t-a) \cdot g(t)$ folgt also $g(\overline{a}) = 0$ und damit

$$\begin{aligned} g(t) \;&=\; (t - \overline{a}) \cdot h(t) \\ \implies f(t) \;&=\; (t-a)(t-\overline{a}) \cdot h(t) \quad \text{für ein } h(t) \in \mathbb{C}[t]. \end{aligned}$$

Dabei ist $(t-a)(t-\overline{a}) \in \mathbb{R}[t]$. Es folgt $f(t) = (t-a)(t-\overline{a})$, also $\deg(f) = 2$. □

Wir haben zwei Begriffe eingeführt, irreduzible Elemente und Primelemente. Die Eindeutigkeit von Primfaktorzerlegungen beruht auf beiden:

Lemma 3.4 (Eindeutigkeit von Faktorisierungen). *Sei R ein Integritätsring, und es gelte*

$$p_1 \cdots p_m \;\sim\; q_1 \cdots q_n$$

mit Primelementen $p_1, \ldots, p_m \in R$ und irreduziblen Elementen $q_1, \ldots, q_n \in R$. Dann ist $m = n$, und nach Umnumerieren der Faktoren gilt $q_i \sim p_i$ für $i = 1, 2, \ldots, n$.

Beweis. OBdA ist $m, n \geq 1$. Da p_1 prim ist und $q_1 \cdots q_n$ teilt, gilt $p_1 \mid q_i$ für ein i. Nach Umnumerieren dürfen wir $i = 1$ annehmen. Da q_1 irreduzibel ist und $p_1 \notin R^\times$ ist, folgt $q_1 = c \cdot p_1$ für eine Einheit $c \in R^\times$. Da R Integritätsring ist, folgt aus der Assoziiertheit $p_1 \ldots p_n \sim q_1 \cdots q_n$ durch Kürzen

$$p_2 \cdots p_m \;\sim\; c \cdot q_2 \cdots q_n.$$

Die Behauptung folgt dann per Induktion. □

Somit kann sich jedes Element auf höchstens eine Weise in ein Produkt von Primelementen zerlegen, denn:

Lemma 3.5. *Primelemente sind irreduzibel.*

Beweis. Sei $p \in R$ ein Primelement. Aus $p = ab$ folgt insbesondere $p \mid ab$. Weil p prim ist, folgt $p \mid a$ oder $p \mid b$. Sei etwa $p \mid a$, also $a = pc$ für ein $c \in R$. Es folgt

$$0 \;=\; p - ab \;=\; p - pcb \;=\; p \cdot (1 - cb).$$

Also ist $cb = 1$, da R ein Integritätsring und $p \neq 0$ ist. Damit ist $b \in R^\times$. □

Umgekehrt müssen irreduzible Elemente nicht unbedingt prim sein und es muß keine Faktorisierung in Primelemente geben, selbst wenn es eine Faktorisierung in irreduzible Elemente gibt. Beispielsweise hat man die zwei Faktorisierungen

$$2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) \quad \text{in} \quad R := \left\{ a + bi\sqrt{5} \in \mathbb{C} \mid a, b \in \mathbb{Z} \right\}.$$

Man kann zeigen, dass in diesem Ring alle vier auftretenden Faktoren irreduzibel sind und dass keine zwei der Faktoren assoziiert zueinander sind. Nach Lemma 3.3 kann $6 \in R$ also kein Produkt von Primelementen sein. Mehr dazu lernen Sie in der algebraischen Zahlentheorie! Wir müssen uns darum hier keine Sorgen machen:

Proposition 3.6. *Sei R ein Hauptidealring. Dann ist in R ein Element genau dann ein Primelement, wenn es irreduzibel ist.*

Beweis. Sei $p \in R$ irreduzibel und $p \mid ab$ für $a, b \in R$. Wir wollen zeigen, dass $p \mid a$ oder $p \mid b$ gilt. Da R ein Hauptidealring ist, ist das Ideal

$$aR + pR := \{ ar_1 + pr_2 \mid r_1, r_2 \in R \} \subseteq R$$

ein Hauptideal, also gleich dR für ein $d \in R$. Insbesondere ist $p \in dR$, also $p = cd$ für ein $c \in R$. Da p irreduzibel ist, folgt $c \in R^\times$ oder $d \in R^\times$. Wir haben also

$$aR + pR \;=\; dR \quad \text{und} \quad p \;=\; cd,$$

wobei einer der folgenden zwei Fälle eintritt:

- Für $c \in R^\times$ ist $d = p \cdot c^{-1} \in pR$, also

$$pR \;=\; dR \;=\; aR + pR \;\ni\; a \quad \Longrightarrow \quad p \mid a.$$

- Für $d \in R^\times$ ist $1 = d \cdot d^{-1} \in dR = aR + pR$, also

$$\begin{aligned} & \exists r_1, r_2 \in R: \quad 1 = ar_1 + pr_2 \\ \Longrightarrow\; & b \;=\; 1 \cdot b \;=\; ab \cdot r_1 + p \cdot br_2 \\ \Longrightarrow\; & p \mid b \quad \text{wegen} \quad p \mid ab. \end{aligned}$$

□

Satz 3.7 (Primfaktorzerlegung in Hauptidealringen). *In Hauptidealringen R hat jedes Element $a \in R$ mit $a \notin R^\times \cup \{0\}$ eine Faktorisierung*

$$a \;=\; p_1 \cdots p_n$$

mit irreduziblen $p_i \in R$. Dabei sind die Primfaktoren p_i bis auf Multiplikation mit Einheiten und Umnumerieren eindeutig.

Beweis. In jedem Integritätsring sind Zerlegungen in Primelemente eindeutig, und in Hauptidealringen sind irreduzible Elemente prim. Zu zeigen bleibt daher nur, dass in Hauptidealringen jedes Element ein Produkt von irreduziblen Elementen ist.

Angenommen, es wäre etwa $a_1 \in R$ nicht als Produkt endlich vieler irreduzibler Elemente darstellbar. Dann ist insbesondere a_1 nicht irreduzibel, also

$$a_1 \;=\; a_2 b_2 \quad \text{mit} \quad a_2, b_2 \;\in\; R \setminus R^\times \cup \{0\}.$$

Mindestens einer der beiden Faktoren, sagen wir a_2, ist kein Produkt endlich vieler irreduzibler Elemente. Induktiv fortfahrend könnten wir so eine unendliche Folge von Elementen $a_1, a_2, a_3, \cdots \in R \setminus R^\times \cup \{0\}$ finden, sodass a_{i+1} ein echter Teiler von a_i ist für alle i. Wir erhalten dann eine echt aufsteigende Kette von Idealen

$$a_1 R \;\subsetneq\; a_2 R \;\subsetneq\; a_3 R \;\subsetneq\; \cdots \;\subseteq\; R.$$

Für aufsteigende Ketten von Idealen ist die Vereinigung wieder ein Ideal

$$I \;:=\; \bigcup_{n=1}^{\infty} a_n R \;\subseteq\; R$$

Da R ein Hauptidealring ist, handelt es sich hierbei um ein Hauptideal, also $I = dR$ für ein $d \in R$. Aus $d \in I$ folgt per Definition $d \in a_n R$ für ein $n \in \mathbb{N}$. Aber dann ist $I = a_n R = a_{n+1} R = \cdots$ im Widerspruch dazu, dass wir eine echt aufsteigende Kette von Idealen konstruiert hatten. □

Korollar 3.8 (Faktorisierung in irreduzible Polynome). *Sei K ein Körper. Für jedes $f \in K[t] \setminus \{0\}$ existiert eine bis auf die Reihenfolge der Faktoren eindeutige Zerlegung*

$$f(t) \;=\; c \cdot \prod_{i=1}^{n} \big(p_i(t)\big)^{e_i}$$

mit paarweise verschiedenen irreduziblen normierten Polynomen $p_i(t) \in K[t]$, einer Konstanten $c \in K^\times$ und Exponenten $e_i \in \mathbb{N}$.

Allgemeiner sei R ein Hauptidealring und $\mathscr{P} \subset R$ ein Repräsentantensystem für die Menge der Primelemente modulo Assoziiertheit, z.B.

$$\mathscr{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\} \subset R = \mathbb{Z},$$
$$\mathscr{P} = \{\text{normierte irreduzible Polynome}\} \subset R = K[t]$$

etc. Jedes $a \in R \setminus \{0\}$ hat dann eine eindeutige Zerlegung der Form

$$a \;=\; c \cdot \prod_{p \in \mathscr{P}} p^{e_p(a)}$$

mit $c \in R^\times$ und Exponenten $e_p(a) \in \mathbb{N}_0$ (fast alle Null).

Definition 3.9. Für $a_1, \ldots, a_n \in R \setminus \{0\}$ definieren wir

- den *größten gemeinsamen Teiler*

$$\mathrm{ggT}(a_1, \ldots, a_n) \;:=\; \prod_{p \in \mathscr{P}} p^{e_p} \quad \text{mit} \quad e_p \;:=\; \min\bigl\{e_p(a_i) \mid i = 1, \ldots, n\bigr\}.$$

- das *kleinste gemeinsame Vielfache*

$$\mathrm{kgV}(a_1, \ldots, a_n) \;:=\; \prod_{p \in \mathscr{P}} p^{f_p} \quad \text{mit} \quad f_p \;:=\; \max\bigl\{e_p(a_i) \mid i = 1, \ldots, n\bigr\}.$$

Die Elemente $a_1, \ldots, a_n$ heißen *teilerfremd*, falls $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ ist.

Bemerkung 3.10. Bei anderer Wahl des Systems $\mathscr{P} \subseteq R$ von Primelementen ändern sich der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache nur um eine Einheit. Das von ihnen erzeugte Hauptideal ist davon unabhängig, genauer sieht man leicht

$$\mathrm{kgV}(a,b) \cdot R \;=\; aR \cap bR \quad \text{und} \quad \mathrm{ggT}(a,b) \cdot R \;=\; aR + bR,$$

wobei wir $aR + bR := \bigl\{ax + by \in R \mid x, y \in R\bigr\}$ setzen. Insbesondere gilt in R die sog. *Bézout-Identität*

$$\mathrm{ggT}(a,b) \;=\; ax + by \quad \text{für geeignete} \quad x, y \;\in\; R.$$

Als einfache Anwendung wollen wir den Chinesischen Restsatz betrachten, eine elementare Aussage über die Lösbarkeit simultaner Kongruenzen, die ihren Namen der folgenden Frage verdankt:

Problem (Sun-Tzu, 3. Jh.). *Gegeben sei eine unbekannte Zahl von Objekten. Wenn man sie*

- *in Dreiergruppen zusammenfasst, bleiben zwei übrig,*
- *in Fünfergruppen zusammenfasst, bleiben drei übrig,*
- *in Siebenergruppen zusammenfasst, bleiben zwei übrig.*

Um wieviele Objekte handelt es sich?

In moderner Sprache lässt sich dieses Problem formulieren als die Suche nach einer Lösung $x \in \mathbb{Z}$ des Systems von Kongruenzen

$$\begin{aligned} x &\equiv 2 \mod 3, \\ x &\equiv 3 \mod 5, \\ x &\equiv 2 \mod 7. \end{aligned}$$

Die kleinste positive Lösung ist $x = 23$, und jede weitere Lösung erhält man hieraus durch Addition eines ganzzahligen Vielfachen von $3 \cdot 5 \cdot 7 = 105$. Tatsächlich ist die natürliche Abbildung

$$\begin{aligned} \mathbb{Z}/105\mathbb{Z} &\xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \\ a \bmod 105 &\mapsto (a \bmod 3,\ a \bmod 5,\ a \bmod 7) \end{aligned}$$

ein Isomorphismus von Ringen. Allgemein gilt:

Satz 3.11 (Chinesischer Restsatz). *Sei R ein Hauptidealring und $a = a_1 \cdots a_n$ das Produkt von paarweise teilerfremden Elementen $a_1, \ldots, a_n \in R$, d.h.* $\mathrm{ggT}(a_i, a_j) = 1$ *für alle $i \neq j$. Dann gibt es einen Isomorphismus von Ringen*

$$R/aR \xrightarrow{\sim} R/a_1R \times \cdots \times R/a_nR.$$

Beweis. Durch Reduktion modulo der Ideale $I_k = a_kR$ für $1 \leq k \leq n$ erhalten wir einen Ringhomomorphismus

$$\varphi\colon \quad R \longrightarrow \prod_{k=1}^{n} R/I_k, \quad r \mapsto \big(r \bmod I_1, \ldots, r \bmod I_n\big).$$

Es gilt $\ker(\varphi) = \{r \in R \mid \forall k\colon\ r \in I_k\} = I_1 \cap \cdots \cap I_n = aR$, wir erhalten also einen injektiven Homomorphismus

$$\overline{\varphi}\colon \quad R/I_1 \cap \cdots \cap I_n \hookrightarrow \prod_{k=1}^{n} R/I_k.$$

Zu zeigen bleibt die Surjektivität. Es genügt, für jedes $i \in \{1, \ldots, n\}$ ein $e_i \in R$ zu konstruieren mit

$$\varphi(e_i) = (0, \ldots, 0, 1, 0, \ldots, 0) \in \prod_{k=1}^{n} R/I_k$$

mit '1' an der i-ten Stelle: Für beliebige $r_1, \ldots, r_n \in R$ folgt dann

$$\varphi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} \varphi(r_i)\varphi(e_i) = (r_1 \bmod I_1, \ldots, r_n \bmod I_n).$$

Zur Konstruktion von e_i benutzen wir, dass $a_1,\dots,a_n$ paarweise teilerfremd sind. Es gilt somit

$$1 \in I_i + I_j \quad \text{für alle} \quad j \neq i.$$

Sei nun i fest gewählt. Für jedes $j \neq i$ haben wir

$$1 = a_j + b_j \quad \text{mit} \quad a_j \in I_i \quad \text{und} \quad b_j \in I_j.$$

Dann ist $b_j \equiv 1 \mod I_i$ und $b_j \equiv 0 \mod I_j$. Es folgt

$$e_i := \prod_{j\neq i} b_j \equiv \begin{cases} 1 \mod I_k & \text{für } k = i, \\ 0 \mod I_k & \text{für } k \neq i. \end{cases}$$

□

Beispiel 3.12. Für $n = p_1^{e_1}\cdots p_n^{e_n} \in \mathbb{N}$ mit paarweise verschiedenen Primzahlen p_i ist

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}.$$

Die Teilerfremdheit der Faktoren ist essentiell: Z.B. gilt $\mathbb{Z}/p^2\mathbb{Z} \not\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Beispiel 3.13. Für Polynome

$$f(t) = (t-a_1)\cdots(t-a_n) \in K[t]$$

mit paarweise verschiedenen Nullstellen $a_1,\dots,a_n \in K$ ist

$$K[t]/f(t)\cdot K[t] \xrightarrow{\sim} K^n \quad \text{via} \quad [g(t)] \mapsto (g(a_1),\dots,g(a_n)).$$

Der chinesische Restsatz liefert hier Polynome $e_i(t) \in K[t]$ mit

$$e_i(a_j) = \begin{cases} 1 & \textit{für } j = i, \\ 0 & \textit{für } j \neq i. \end{cases}$$

Explizit kann man

$$e_i(t) := \prod_{j\neq i} \frac{t-a_j}{a_i-a_j} \in K[t]$$

wählen. Damit haben wir ein Interpolationsproblem gelöst: Seien $c_1,\dots,c_n \in K$, dann gilt:

- Das Polynom $g(t) := c_1e_1(t) + \cdots + c_ne_n(t)$ erfüllt $g(a_i) = c_i$ für $i = 1,\dots,n$.
- Jedes andere Polynom mit dieser Eigenschaft erhält man hieraus durch Addition eines polynomialen Vielfaches von $f(t) = \prod_{i=1}^n (t-a_i)$.

4 Der Elementarteilersatz

Nach diesem Exkurs in die Ringtheorie kommen wir nun zurück zu Moduln. Wir werden im nächsten Abschnitt zeigen, dass jeder endlich erzeugte Modul M über einem Hauptidealring R von der Form

$$M \simeq R^n \oplus R/a_1R \oplus \cdots \oplus R/a_kR$$

für ein $n \in \mathbb{N}_0$ und $a_i \in R \setminus \{0\}$ ist. Um das zu sehen, benötigen wir ein Version des Gauß-Algorithmus über Hauptidealringen. Genauer müssen wir die Aussage verallgemeinern, dass sich jede Matrix $A \in \mathrm{Mat}(m \times n, K)$ über einem Körper K durch geeignete $S \in \mathrm{GL}_m(K), T \in \mathrm{GL}_n(K)$ transformieren lässt zu einer Matrix

$$S \cdot A \cdot T = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & \end{pmatrix}$$

Um solche Basiswechsel zu finden, hatten wir eine Version des Gauß-Algorithmus auf die Zeilen und Spalten der gegebenen Matrix angewandt, wobei gilt:

- S ist das Produkt der vorgenommenen Zeilentransformationen,
- T ist das Produkt der vorgenommenen Spaltentransformationen.

Wenn wir statt Vektorräumen allgemeiner freie Moduln über einem kommutativen Ring betrachten wollen, steht uns im Gauß-Algorithmus keine Division mehr zur Verfügung. Wir müssen vorsichtiger vorgehen:

Beispiel 4.1. Sei $R = \mathbb{Z}$ und

$$A = \begin{pmatrix} 10 & * & \cdots & * \\ 14 & * & \cdots & * \end{pmatrix} \in \mathrm{Mat}(2 \times n, R).$$

Über den rationalen Zahlen würden wir im ersten Schritt des Gauß-Algorithmus die erste Zeile durch 10 teilen. Das ist in $R = \mathbb{Z}$ nicht möglich. Stattdessen gehen wir wie folgt vor:

$$\begin{pmatrix} 10 & * & \cdots & * \\ 14 & * & \cdots & * \end{pmatrix} \xrightarrow{II \mapsto II - I} \begin{pmatrix} 10 & * & \cdots & * \\ 4 & * & \cdots & * \end{pmatrix} \xrightarrow{I \mapsto I - 2 \cdot II} \begin{pmatrix} 2 & * & \cdots & * \\ 4 & * & \cdots & * \end{pmatrix}$$

$$\xrightarrow{II \mapsto II - 2 \cdot I} \begin{pmatrix} 2 & * & \cdots & * \\ 0 & * & \cdots & * \end{pmatrix}$$

Besser geht's nicht, denn jede ganzzahlige Linearkombination von 10 und 14 muß eine gerade Zahl sein. Wir können die obigen drei Schritte zusammenfassen in der Linksmultiplikation mit der Matrix

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix}$$

Effektiv haben wir hier den Euklidischen Algorithmus ablaufen lassen: Die erste Zeile der Matrix auf der rechten Seite enthält die Koeffizienten 3 und -2 aus der Bézout-Identität

$$\mathrm{ggT}(10,14) = 2 = 3 \cdot 10 + (-2) \cdot 14.$$

Man beachte, dass alle vorgenommenen Zeilentransformationen invertierbar über $\mathbb{Z}$ waren. Es ist

$$\det \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} = 3 \cdot 3 + (-4) \cdot (-2) = 1.$$

Die letzte Gleichung kann man auch als Bézout-Identität für $\mathrm{ggT}(3,-2) = 1$ lesen!

Die Bézout-Identität gilt in jedem Hauptidealring, siehe Bemerkung 3.10. Ab jetzt sei also R ein beliebiger Hauptidealring. Invertierbare Zeilentransformationen über R sind gegeben durch Linksmultiplikation mit Elementen der Gruppe

$$\mathrm{GL}_m(R) := \left\{ S \in \mathrm{Mat}(m \times m, R) \mid \exists S' \in \mathrm{Mat}(m \times m, R) : SS' = S'S = \mathbf{1} \right\}.$$

Das obige Beispiel verallgemeinert sich zu:

Lemma 4.2. *Seien $a_1, a_2 \in R$, und sei $a_1R + a_2R = dR$. Dann gibt es ein $S \in \mathrm{GL}_2(R)$, sodass gilt:*

$$S \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Beweis. Seien $b_1, b_2 \in R$ mit $a_1b_1 + a_2b_2 = d$. Da d ein größter gemeinsamer Teiler von a_1 und a_2 war, sind dann notwendigerweise die Elemente b_1 und b_2 zueinander teilerfremd. Somit ist $b_1c_1 + b_2c_2 = 1$ für geeignete Elemente $c_1, c_2 \in R$. Für die Matrix

$$S_1 := \begin{pmatrix} b_1 & b_2 \\ -c_2 & c_1 \end{pmatrix} \in \mathrm{Mat}(2 \times 2, R)$$

gilt dann $\det(S_1) = 1$ und somit ist nach der Cramer'schen Formel $S_1 \in \mathrm{GL}_2(R)$. Es gilt nun

$$S_1 \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} d \\ e \end{pmatrix} \quad \text{mit} \quad e \in a_1R + a_2R = dR.$$

Sei $f \in R$ mit $e = df$, dann ist

$$S_2 \cdot \begin{pmatrix} d \\ e \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix} \quad \text{für} \quad S_2 := \begin{pmatrix} 1 & 0 \\ -f & 1 \end{pmatrix} \in \mathrm{GL}_2(R)$$

und die Matrix $S := S_2 \cdot S_1$ leistet das Gewünschte. □

Wir können den Struktursatz für lineare Abbildungen von Vektorräumen nun wie folgt verallgemeinern:

Satz 4.3 (Elementarteilersatz für Matrizen). *Sei R ein Hauptidealring.*

a) Für jede Matrix $A \in \mathrm{Mat}(m \times n, R)$ existieren Matrizen $S \in \mathrm{GL}_n(R)$, $T \in \mathrm{GL}_m(R)$ mit

$$S \cdot A \cdot T \;=\; \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \\ & & \end{pmatrix}$$

wobei $r \leq \min\{m,n\}$ ist, $d_1, \ldots, d_r \in R \setminus \{0\}$ sind und $d_i \mid d_{i+1}$ für alle i gilt.

b) Dabei sind die d_i bis auf Multiplikation mit Einheiten des Ringes R eindeutig bestimmt. Wir bezeichnen sie als die Elementarteiler *von A.*

Beweis. *a*) Nach Satz 3.7 besitzt jedes von Null verschiedene Element von R eine Primfaktorzerlegung $a = \varepsilon \cdot p_1^{e_1} \cdots p_k^{e_k}$ mit Primfaktoren $p_i \in R$, einer Einheit $\varepsilon \in R^\times$ und Exponenten $e_i \in \mathbb{N}$. Wir bezeichnen die mit Vielfachheiten gezählte Anzahl der Faktoren mit $\delta(a) := e_1 + \cdots + e_k \in \mathbb{N}_0$. Für Matrizen $A = (a_{ij}) \in \mathrm{Mat}(m \times n, R)$ setzen wir

$$\delta(A) \;:=\; \min\bigl\{\delta(a_{ij}) \mid a_{ij} \neq 0\bigr\} \;\in\; \mathbb{N}_0.$$

Wir gehen nun nach dem folgenden Algorithmus vor:

I. Wende Zeilen- und Spaltenvertauschungen an, sodass $\delta(A) = \delta(a_{11})$ wird.

II. Wenn ein Element a_{i1} der ersten Spalte nicht durch das Element a_{11} teilbar ist, schreibe

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_{11} \\ a_{i1} \end{pmatrix} \;=\; \begin{pmatrix} d \\ 0 \end{pmatrix} \quad \text{für eine Matrix} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\in\; \mathrm{GL}_2(R)$$

nach Lemma 4.2 für einen größten gemeinsamen Teiler $d = \mathrm{ggT}(a_{11}, a_{i1})$. Wir wenden nun die entsprechende Zeilentransformation auf die erste und die i-te Zeile an, wobei wir alle übrigen Zeilen der Matrix unverändert lassen: Durch Multiplikation mit

$$S \;=\; \begin{pmatrix} a & & & c & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ b & & & d & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \;\in\; \mathrm{GL}_m(R)$$

erhalten wir eine neue Matrix $A' = S \cdot A$ mit dem linken oberen Eintrag $a'_{11} = d$, dabei gilt

$$\delta(A') \leq \delta(a'_{11}) = \delta(d) < \delta(a_{11}) = \delta(A).$$

Ersetze nun A durch die neue Matrix A' und gehe zurück zu Schritt I.

III. Wenn ein Element a_{1j} der ersten Zeile nicht durch das Element a_{11} teilbar ist, verfahren wir analog mit Spaltentransformationen und erhalten ein $T \in \mathrm{GL}_n(K)$ mit $\delta(A') < \delta(A)$ für die Matrix $A' = A \cdot T$. Ersetze dann A durch diese neue Matrix und gehe zurück zu Schritt I.

IV. Wenn alle Einträge der ersten Zeile und der ersten Spalte durch a_{11} teilbar sind, ziehe Vielfache der ersten Zeile von den übrigen Zeilen ab und verfahre analog mit den Spalten, um eine Blockmatrix

$$A' = \left(\begin{array}{c|c} a_{11} & 0 \cdots 0 \\ \hline 0 & \\ \vdots & B \\ 0 & \end{array}\right)$$

zu erhalten. Man beachte, dass noch immer $\delta(A') \leq \delta(a_{11}) \leq \delta(A)$ gilt. Wenn der Matrixblock B einen Eintrag enthält, welcher nicht durch das Element a_{11} teilbar ist, so addiere man die entsprechende Spalte zur ersten Spalte und gehe mit der so erhaltenen Matrix zurück zu Schritt II.

Da in jedem der Schritte II und III die ganzzahlige Invariante $\delta(A) \geq 0$ echt kleiner wird, muß das Verfahren nach endlich vielen Schritten abbrechen bei einer Matrix in der Blockform aus Schritt IV mit der Eigenschaft, dass alle Einträge der Matrix B durch das Element $d_1 := a_{11}$ teilbar sind. Die Behauptung folgt dann per Induktion über die Zeilenzahl der Matrizen, indem wir dasselbe Verfahren auf B anwenden.

b) Die Eindeutigkeitsaussage wird später in Satz 5.1 klar werden, wenn wir unser Resultat in die intrinsische Sprache von Moduln übersetzt haben; natürlich werden wir dabei aufpassen, dass wir die Eindeutigkeit vorher nirgends benutzen. □

Wir haben invertierbare Matrizen bereits als Basiswechsel betrachtet. Allgemein sind die Homomorphismen zwischen Standard-R-Moduln $\varphi : R^m \longrightarrow R^n$ genau die Abbildungen

$$\varphi : \quad R^m \longrightarrow R^n, \quad v \mapsto A \cdot v$$

die man durch Linksmultiplikation mit Matrizen $A \in \mathrm{Mat}(m \times n, R)$ erhält. Als eine erste Anwendung erhalten wir:

Korollar 4.4. *Sei M ein endlich erzeugter freier R-Modul. Dann bestehen je zwei Basen des Moduls aus gleich vielen Elementen.*

Beweis. Der Basiswechsel zwischen zwei Basen der Länge n bzw. m liefert einen Isomorphismus $\varphi : R^n \longrightarrow R^m$. Als Isomorphismus von Standardmoduln ist dieser

gegeben durch die Multiplikation mit einer Matrix $A \in \mathrm{Mat}(m \times n, K)$. Nach Satz 4.3 gibt es $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$, sodass

$$D := S \cdot A \cdot T^{-1} \in \mathrm{Mat}(m \times n, K)$$

eine Matrix ist, bei der alle Einträge außerhalb der Diagonalem verschwinden. Die Multiplikation mit einer solchen Matrix ist aber für $n > m$ nicht injektiv, für $m > n$ nicht surjektiv. Also muß $m = n$ sein. □

Als nächstes wollen wir den Elementarteilersatz für Matrizen in eine Aussage über Untermoduln von freien Moduln übersetzen. Dazu schauen wir uns zunächst einige einfache Beispiele an:

Beispiel 4.5. Für Vektorräume über Körpern gibt es zu jedem Untervektorraum ein Komplement. Dies ist für Moduln über Ringen im Allgemeinen nicht der Fall: Der freie $\mathbb{Z}$-Modul $V = \mathbb{Z}$ enthält den freien Untermodul

$$U = 2\mathbb{Z} \hookrightarrow V = \mathbb{Z},$$

aber keine Basis von U lässt sich zu einer Basis von V ergänzen. Hier erhalten wir immerhin noch eine Basis des Untermoduls, wenn wir den Basisvektor einer Basis des umgebenden Moduls verdoppeln. Geht so etwas allgemein?

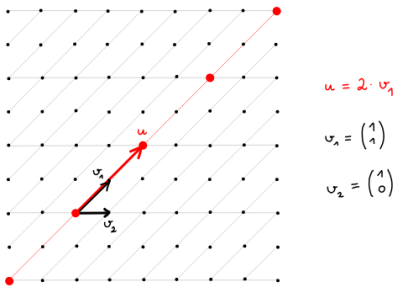
Beispiel 4.6. Für den freien Untermodul

$$U = \mathbb{Z} \cdot u \hookrightarrow V = \mathbb{Z}^2 \quad \text{mit} \quad u = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$

liefert Lemma 4.2 ein $S \in \mathrm{GL}_2(\mathbb{Z})$ mit

$$S \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix} \quad \text{für} \quad d = \mathrm{ggT}(a_1, a_2).$$

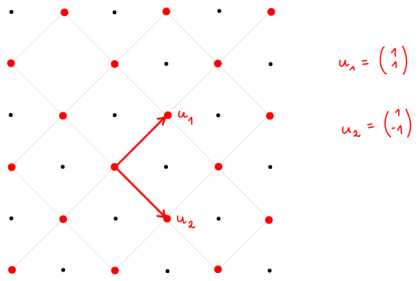
Wenn wir von der Standardbasis (e_1, e_2) des freien Moduls $V = \mathbb{Z}^2$ übergehen zu der Basis (v_1, v_2) mit $v_i = S^{-1} e_i$ wie in der folgenden Abbildung, ist der Basisvektor von U ein Vielfaches $u = d \cdot v_1$:



Beispiel 4.7. Als nächstes betrachten wir den freien Untermodul

$$U = \mathbb{Z}\cdot u_1 \oplus \mathbb{Z}\cdot u_2 \subseteq V = \mathbb{Z}^2 \quad \text{mit} \quad u_1 = \begin{pmatrix}1\\1\end{pmatrix} \quad u_2 = \begin{pmatrix}1\\-1\end{pmatrix}.$$

Die folgende Abbildung skizziert diesen in der reellen Ebene:



Hier lässt sich aus u_1, u_2 durch Reskalieren keine Basis von V gewinnen, da die u_i keine echten Vielfachen anderer ganzzahliger Vektoren sind. Aber wenn wir für V die Basis aus $v_1 = e_1$ und $v_2 = u_1$ wählen, bilden $\tilde{u}_1 = 2v_1$ und $\tilde{u}_2 = v_2$ eine Basis von U. Um Basen eines Untermoduls mit Basen des umgebenden Moduls in Bezug zu setzen, müssen wir also *beide* Basen geeignet wählen!

Wenn wir den Elementarteilersatz für Matrizen über Ringen interpretieren als Aussage über Untermoduln, wird daraus allgemein:

Satz 4.8 (Elementarteilersatz für Untermoduln). *Sei R ein Hauptidealring.*

a) Für endlich erzeugte freie R-Modul V ist auch jeder Untermodul $U \subseteq V$ endlich erzeugt und frei. Genauer existieren

- *eine Basis $v_1, \dots, v_m$ von V*
- *Elemente $d_1, \dots, d_r \in R \setminus \{0\}$ für ein $r \leq m$,*

sodass $d_1 v_1, \dots, d_r v_r$ eine Basis von U bilden und $d_i \mid d_{i+1}$ für alle i ist.

b) Dabei sind die d_i bis auf Multiplikation mit Einheiten des Ringes R eindeutig bestimmt, wir nennen sie die Elementarteiler *des Untermoduls.*

Beweis. Für die Existenzaussage $a)$ genügt es, den Fall $V = R^m$ zu behandeln; den allgemeinen Fall reduziert man hierauf durch Wahl einer Basis. Wir zeigen zunächst per vollständiger Induktion über $m \in \mathbb{N}$, dass jeder Untermodul $U \subseteq V = R^m$ endlich erzeugt ist. Für den Induktionsanfang $m = 1$ ist nichts zu zeigen: Die Untermoduln von R sind genau die Ideale des Ringes R, und per Definition von Hauptidealringen wird jedes solche Ideal sogar von einem Element erzeugt. Für den Induktionsschritt betrachten wir die Sequenz

$$0 \longrightarrow R^{m-1} \xrightarrow{\iota} R^m \xrightarrow{\pi} R \longrightarrow 0$$

von R-Moduln, mit $\iota(a_1,\dots,a_{m-1}) := (a_1,\dots,a_{m-1},0)$, $\pi(a_1,\dots,a_m) := a_m$. Dabei gilt

$$\iota \text{ ist injektiv, } \pi \text{ ist surjektiv, und } \ker(\pi) = \operatorname{im}(\iota).$$

Man sagt auch, die Sequenz sei exakt. Wir wissen aus dem Induktionsanfang $m = 1$, dass der Untermodul $\pi(U) \subseteq R$ von einem Element erzeugt wird; wir wählen einen beliebigen solchen Erzeuger und schreiben diesen in der Form $\bar{u}_1 = \pi(u_1)$ für ein $u_1 \in U$. Per Induktion ist zudem der Schnitt $U \cap \operatorname{im}(\iota)$ als Untermodul eines freien Moduls vom Rang $m-1$ ein endlich erzeugter Modul, sei etwa $U \cap \operatorname{im}(\iota) = Ru_2 + \cdots + Ru_n$. Wir erhalten dann:

$$\begin{aligned}
u \in U &\implies \exists r_1 \in R: \quad \pi(u) = r \cdot \bar{u}_1 \\
&\implies \exists r_1 \in R: \quad \pi(u - ru_1) = 0 \\
&\implies \exists r_1 \in R: \quad u - ru_1 \in U \cap \ker(\pi) = U \cap \operatorname{im}(\iota) \\
&\qquad\qquad\qquad\qquad = Ru_2 + \cdots + Ru_n \\
&\implies \exists r_1,\dots,r_n \in R: \quad u - r_1u_1 = r_2u_2 + \cdots + r_nu_n \\
&\implies \exists r_1,\dots,r_n \in R: \quad u = r_1u_1 + \cdots + r_nu_n \\
&\implies u \in Ru_1 + Ru_2 + \cdots + Ru_n.
\end{aligned}$$

Damit ist der Untermodul $U \subseteq V = R^m$ endlich erzeugt und gleich dem Bild des Modulhomomorphismus

$$\varphi: \quad R^n \longrightarrow R^m, \quad (r_1,\dots,r_n) \mapsto r_1u_1 + \cdots r_nu_n.$$

In den Standardbasen wird dieser Modulhomomorphismus dargestellt durch eine Matrix

$$A \in \operatorname{Mat}(m \times n, R) = \operatorname{Hom}_R(R^n, R^m).$$

Der Elementarteilersatz 4.3 liefert Basiswechselmatrizen $S \in \mathrm{GL}_m(R), T \in \mathrm{GL}_n(R)$ mit

$$S \cdot A \cdot T = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \\ & & \\ & & \end{pmatrix}$$

und $d_i \mid d_{i+1}$ für alle i. Dann bilden

- die Vektoren $v_i := S^{-1} \cdot e_i$ für $i = 1,\dots,m$ eine Basis von $V = R^m$,
- die Vektoren $d_i \cdot v_i$ für $i = 1,\dots,r$ eine Basis von $U = \operatorname{im}(A) = S^{-1} \cdot \operatorname{im}(S \cdot A \cdot T)$,

und somit ist die Existenzaussage $a)$ des Satzes bewiesen.

Die Eindeutigkeitsaussage $b)$ werden wir am Ende des nächsten Abschnitts durch Betrachten von V/U folgern. Natürlich werden wir bis dahin nur die Aussage $a)$ verwenden, sodass kein Zirkelschluß vorliegt. □

5 Moduln über Hauptidealringen

Die Eindeutigkeitsaussage im obigen Elementarteilersatz versteht man am besten als Aussage über Quotientenmoduln. Das Ziel dieses Abschnittes ist der Beweis des folgenden Satzes, der eine vollständige Beschreibung aller endlich erzeugten Moduln über Hauptidealringen gibt:

Satz 5.1 (Strukturssatz für endlich erzeugte Moduln über Hauptidealringen).

a) Sei R ein Hauptidealring. Dann besitzt jeder endlich erzeugter R-Modul M die Form

$$M \simeq R^r \oplus R/d_1R \oplus \cdots \oplus R/d_kR$$

für ein $r \in \mathbb{N}_0$ und $d_1, \ldots, d_k \in R \setminus (R^\times \cup \{0\})$ mit $d_i \mid d_{i+1}$ für alle i.

b) Dabei sind r und die d_i durch die obigen Eigenschaften eindeutig bestimmt. Wir nennen

- $r = \mathrm{rk}(M)$ *den* Rang *des Moduls M,*
- $d_1, \ldots, d_k$ *die* Elementarteiler *von M.*

Beweis (der Existenzaussage a)). Per Definition von endlicher Erzeugtheit existiert eine Darstellung

$$M = Rw_1 + \cdots + Rw_m \quad \text{für geeignete} \quad w_1, \ldots, w_m \in M.$$

Eine solche Darstellung ist natürlich nicht eindeutig. Wir wählen sie beliebig und erhalten einen surjektiven Homomorphismus

$$\varphi: \quad V := R^m \twoheadrightarrow M, \quad (a_1, \ldots, a_m) \mapsto a_1w_1 + \cdots + a_mw_m$$

Nach dem Elementarteilersatz 4.8 ist sein Kern $\ker(\varphi) \subseteq V$ als Untermodul eines endlich erzeugten freien R-Moduls ebenfalls endlich erzeugt und frei, genauer liefert der Satz einen Isomorphismus

$$f: \quad V \xrightarrow{\sim} R^m \quad \text{mit} \quad f\big(\ker(\varphi)\big) = \bigoplus_{i=1}^{m} d_iR \subseteq \bigoplus_{i=1}^{m} R = f(V),$$

wobei $d_1, \ldots, d_k$ die Elementarteiler des Untermoduls $\ker(\varphi) \subseteq V$ seien und wir zur Vereinfachung der Notation $d_{k+1} = \cdots = d_m = 0$ schreiben. Wir erhalten somit Isomorphismen

$$\begin{aligned} M &\simeq V/\ker(\varphi) \\ &\simeq (R \oplus \cdots \oplus R)/(d_1R \oplus \cdots \oplus d_mR) \\ &\simeq \bigoplus_{i=1}^{m} R/d_iR. \end{aligned}$$

Dabei haben wir im ersten Schritt den Homomorphiesatz für φ, im zweiten Schritt den Isomorphismus f und zuletzt die Verträglichkeit von direkten Summen mit Quotienten benutzt. Somit folgt die Existenzaussage $a)$ des Satzes. □

Es bleibt die Eindeutigkeitsaussage $b)$ zu zeigen. Hierzu benötigen wir einige allgemeine Konstruktionen:

Definition 5.2. Der *Torsionsanteil* eines R-Moduls M ist

$$M_{tors} := \{ m \in M \mid \exists a \in R \setminus \{0\} : a \cdot m = 0 \} \subseteq M.$$

Man sieht leicht, dass es sich hierbei um einen Untermodul handelt. Wir definieren den *torsionsfreien Anteil* von M als

$$M_{frei} := M/M_{tors}.$$

Man sieht sofort anhand der Definition, dass für jeden Homomorphismus $\varphi : M \to N$ von R-Moduln gilt:

$$\varphi(M_{tors}) \subseteq N_{tors}$$

Wir erhalten somit Homomorphismen

$$\begin{aligned} \varphi_{tors} : \quad & M_{tors} \longrightarrow N_{tors}, \quad m \mapsto \varphi(m), \\ \varphi_{frei} : \quad & M_{frei} \longrightarrow N_{frei}, \quad [m] \mapsto [\varphi(m)]. \end{aligned}$$

Wenn φ ein Isomorphismus ist, dann trivialerweise auch φ_{tors} und φ_{frei}.

Bemerkung 5.3. Im Gegensatz zum Torsionsanteil ist der torsionsfreie Anteil eines Moduls im Allgemeinen kein Untermodul, sondern nur ein Quotient. Satz 5.1 $a)$ zeigt zwar, dass über Hauptidealringen R jeder endlich erzeugte Modul isomorph ist zu einer direkten Summe

$$M \simeq M_{tors} \oplus M_{frei} \quad \text{mit} \quad \begin{cases} M_{frei} \simeq R^r \\ M_{tors} \simeq R/d_1R \oplus \cdots \oplus R/d_kR, \end{cases}$$

aber die Einbettung $M_{frei} \hookrightarrow M$ ist dabei willkürlich und es gibt keine Wahl, die mit beliebigen Modulhomomorphismen kompatibel wäre. Z.B. ist für $M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ die Abbildung

$$\varphi : \quad M \xrightarrow{\sim} M, \quad \big(a, [b]\big) \mapsto \big(a, [a+b]\big)$$

ein Isomorphismus von Moduln, aber sie bildet den freien Untermodul $\mathbb{Z} \oplus \{0\} \subseteq M$ nicht auf sich ab, und daran ändert sich auch nichts, wenn wir diesen freien Modul auf andere Weise einbetten (die Situation ist analog zur Wahl eines Komplementes für einen gegebenen Untervektorraum eines Vektorraumes; auch dort gab es keine kanonische Wahl und man sollte besser den Quotientenvektorraum betrachten). Im

Gegensatz zur willkürlichen Zerlegung als direkte Summe hängt jedoch die exakte Sequenz

$$0 \longrightarrow M_{tors} \longrightarrow M \longrightarrow M_{frei} \longrightarrow 0$$

nur von dem gegebenen Modul ab, und das wird für unsere Zwecke genügen.

Die obige Diskussion reduziert den Beweis der Eindeutigkeit im Struktursatz 5.1 im Wesentlichen auf den Fall freier Moduln und den Fall von Torsionsmoduln. Um Torsionsmoduln zu behandeln, benötigen wir etwas Vorarbeit.

Beispiel 5.4. Sei R ein Hauptidealring. Für beliebige Elemente $a \in R \setminus (R^\times \cup \{0\})$ gilt dann

$$R/aR \;\not\cong\; R/aR \oplus R/aR.$$

Dies folgt z.B.

a) im Fall $R = \mathbb{Z}$ durch Zählen der Elemente dieser endlichen Gruppen.

b) im Fall $R = K[t]$ durch Betrachten der Vektorraumdimension über K.

Um dasselbe über beliebigen Hauptidealringen R zu beweisen, verallgemeinern wir die Vektorraumdimension:

Definition 5.5. Die *Länge* eines R-Moduls M ist das Supremum der Längen aller echt aufsteigenden Ketten von Untermoduln:

$$\ell(M) \;:=\; \sup\{\ell \in \mathbb{N}_0 \mid \exists \text{Untermoduln } 0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M\} \;\in\; \mathbb{N}_0 \cup \{\infty\}.$$

Für Vektorräume über Körpern stimmt die Länge mit der Dimension überein. Für uns interessanter ist das Beispiel $M = R/aR$ mit $a \in R \setminus \{0\}$. Wir betrachten dazu die Primfaktorzerlegung

$$a \;=\; \varepsilon \cdot p_1^{e_1} \cdots p_n^{e_n}$$

mit Primfaktoren $p_i \in R$, einer Einheit $\varepsilon \in R^\times$ und Exponenten $e_i \in \mathbb{N}$. Wie im Beweis des Elementarteilersatzes 4.3 bezeichnen wir die Anzahl der auftretenden Primfaktoren inclusive Vielfachheiten mit $\delta(a) := e_1 + \cdots + e_n$.

Lemma 5.6. *Sei R ein Hauptidealring und $a \in R \setminus \{0\}$. Der R-Modul $M = R/aR$ besitzt dann die Länge*

$$\ell(M) \;=\; \delta(a).$$

Beweis. Für jedes Ideal $I \subseteq R$ mit $aR \subseteq I$ ist sein Bild unter $\pi : R \twoheadrightarrow R/aR$ ein Untermodul

$$\pi(I) \;\subseteq\; R/aR \;=\; M,$$

und umgekehrt ist für jeden Untermodul $U \subseteq M$ das Urbild $I = \pi^{-1}(U) \subseteq R$ ein Ideal. Die Länge von M ist also das Supremum der Längen aller echt aufsteigenden Ketten

$$aR \;=\; I_0 \;\subsetneq\; I_1 \;\subsetneq\; I_2 \;\subsetneq\; \cdots \;\subsetneq\; I_\ell \;=\; R$$

von Idealen. Da R ein Hauptidealring ist, können wir dabei $I_k = a_k R$ mit $a_k \in R$ schreiben und die gesuchte Länge wird damit zum Supremum aller Längen von Folgen $a_0, \ldots, a_\ell \in R$, sodass gilt:

- $a_0 = a$, und
- a_{i+1} ist ein echter Teiler von a_i für alle i.

Die maximale Länge wird offenbar erreicht, wenn wir $a_{i+1} = a_i/p_i$ wählen für einen Primfaktor $p_i \mid a_i$, solange es einen solchen Primfaktor gibt, solange also $\delta(a_i) > 0$ ist. Dann wird in jedem Schritt $\delta(a_{i+1}) = \delta(a_i) - 1$. □

Um das Argument in Beispiel 5.4 zu vervollständigen, müssen wir noch zeigen, dass die Länge von Moduln additiv bezüglich direkter Summen ist. Das gilt nicht nur für direkte Summen $M = M' \oplus M''$ von R-Moduln, sondern sogar für beliebige exakte Sequenzen:

Lemma 5.7 (Additivität der Länge von Moduln). *Sei*

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{\pi} M'' \longrightarrow 0$$

eine exakte Sequenz von R-Moduln, dann gilt $\ell(M) = \ell(M') + \ell(M'')$.

Beweis. Für jede Kette von Untermoduln $U_1 \subseteq U_2 \subseteq \cdots \subseteq M$ erhalten wir Ketten von Untermoduln

$$U_1 \cap M' \subseteq U_2 \cap M' \subseteq \cdots \subseteq M' \quad \text{und} \quad \pi(U_1) \subseteq \pi(U_2) \subseteq \cdots \subseteq M''$$

und wegen $M' = \ker(\pi)$ gilt dabei:

$$U_i = U_{i+1} \quad \Longleftrightarrow \quad U_i \cap M' = U_{i+1} \cap M' \text{ und } \pi(U_i) = \pi(U_{i+1})$$

Jede echte Inklusion in einer aufsteigenden Kette von Untermoduln liefert somit eine echte Inklusion in der induzierten Kette in M' oder M'' und für das Supremum der Längen folgt $\ell(M) \leq \ell(M') + \ell(M'')$. Für die umgekehrte Ungleichung seien beliebige Ketten

$$\begin{aligned} U'_1 \subseteq U'_2 \subseteq \cdots \subseteq U'_r \subseteq M' \\ U''_1 \subseteq U''_2 \subseteq \cdots \subseteq U''_s \subseteq M'' \end{aligned}$$

von Untermoduln gegeben. Wir setzen dann

$$U_i := \begin{cases} U'_i & \text{für } 1 \leq i \leq r, \\ \pi^{-1}(U''_{i-r}) & \text{für } r < i \leq r+s. \end{cases}$$

und erhalten eine aufsteigende Kette von Untermoduln $U_1 \subseteq U_2 \subseteq \cdots \subseteq M$. Jede strikte Inklusion in einer der beiden vorgegebenen Ketten gibt eine strikte Inklusion in der zusammengesetzten Kette. Für das Supremum der Längen solcher Ketten folgt somit $\ell(M) \geq \ell(M') + \ell(M'')$ wie gewünscht. □

Beispiel 5.8. In der in Beispiel 5.4 betrachteten Situation ist $R/aR \oplus R/aR \not\simeq R/aR$, denn

$$\ell(R/aR \oplus R/aR) \;=\; \ell(R/aR) + \ell(R/aR) \;>\; \ell(R/aR)$$

für jedes $a \in R \setminus (R^\times \cup \{0\})$. Wir haben hierbei benutzt, dass isomorphe Moduln die gleiche Länge besitzen müssen. Die Umkehrung dieser letzten Aussage ist nicht richtig: Die Moduln

$$M \;=\; R/aR \oplus R/aR \quad \text{und} \quad N \;=\; R/a^2R$$

besitzen die gleiche Länge, sind aber nicht zueinander isomorph. Die letzte Aussage folgt z.B. aus $a \cdot m = 0$ für alle $m \in M$ und $a \cdot n \neq 0$ für das Element $n = [1] \in N$.

Um derartige Argumente zur Unterscheidung von Moduln zu verallgemeinern, betrachten wir für R-Moduln M und $a \in R$ den Untermodul

$$a \cdot M \;:=\; \{a \cdot m \mid m \in M\} \;\subseteq\; M.$$

Die folgende Beobachtung erlaubt es, per Induktion über die Zahl der auftretenden Primfaktoren zu argumentieren:

Proposition 5.9. *Sei R ein Hauptidealring, und sei $p \in R$ prim. Für $a \in R \setminus \{0\}$ gilt dann*

$$p \cdot (R/aR) \;\simeq\; R/bR \quad \textit{mit} \quad b \;=\; \begin{cases} a & \textit{für } p \nmid a, \\ a/p & \textit{für } p \mid a. \end{cases}$$

Beweis. Der Modulhomomorphismus $\varphi : R \twoheadrightarrow p \cdot (R/aR), m \mapsto p \cdot [m]$ ist surjektiv mit Kern

$$\begin{aligned} \ker(\varphi) \;&=\; \big\{\, c \in R \mid pc \in aR \,\big\} \\ &=\; \big\{\, c \in R \mid \exists d \in R :\; pc = ad \,\big\} \\ &=\; \big\{\, c \in R \mid \exists d' \in R :\; c = bd' \,\big\} \;=\; bR, \end{aligned}$$

wobei wir im vorletzten Schritt zwei Fälle unterscheiden:

- Im Fall $p \nmid a$ bedeutet $pc = ad$, dass $p \mid d$ ist, also $c = bd'$ mit $b = a$ und $d' = d/p$.
- Im Fall $p \mid a$ bedeutet $pc = ad$, dass $c = bd'$ ist mit $b = a/p$ und $d' = d$.

Nach dem Homomorphiesatz ist $\mathrm{im}(\varphi) \simeq R/\ker(\varphi)$, also sind wir fertig. □

Wir können nun die Eindeutigkeit im Struktursatz 5.1 beweisen. Aus praktischen Gründen numerieren wir die Elementarteiler um und lassen jetzt auch Einheiten zu, wobei für $d_i \in R^\times$ der Summand $R/d_iR = \{0\}$ trivial ist; damit können wir am Ende der Liste von Elementarteilern beliebige Einheiten ergänzen:

Satz 5.10 (Eindeutigkeitssatz). *Sei R ein Hauptidealring, und es gelte $M \simeq N$ für zwei Moduln der Form*

$$M \;=\; R^r \oplus R/d_1R \oplus \cdots \oplus R/d_kR \qquad \textit{mit } r \in \mathbb{N}_0,\ d_i \in R\setminus\{0\} \textit{ und } d_{i+1} \mid d_i \textit{ für alle } i,$$

$$N \;=\; R^s \oplus R/e_1R \oplus \cdots \oplus R/e_lR \qquad \textit{mit } s \in \mathbb{N}_0,\ e_i \in R\setminus\{0\} \textit{ und } e_{i+1} \mid e_i \textit{ für alle } i.$$

Dann ist $r = s$, und indem wir formal $d_i = 1$ für $i > r$ und $e_i = 1$ für $i > l$ setzen, erhalten wir

$$d_iR \;=\; e_iR \quad \textit{für alle } i.$$

Beweis. Sei $\varphi : M \xrightarrow{\sim} N$ ein Isomorphismus. Wir erhalten dann insbesondere einen Isomorphismus

$$\varphi_{frei}: \quad M_{frei} \xrightarrow{\sim} N_{frei}.$$

Es folgt $r = s$, da nach Korollar 4.4 der Rang eines endlich erzeugten freien Moduls eindeutig bestimmt ist. Es bleibt nur der Torsionsteil zu behandeln. Dazu betrachten wir

$$\varphi_{tors}: \quad M_{tors} \;=\; R/d_1R \oplus \cdots \oplus R/d_kR \;\xrightarrow{\sim}\; N_{tors} \;=\; R/e_1R \oplus \cdots \oplus R/e_lR.$$

Nach Lemma 5.6 und 5.7 gilt

$$\begin{aligned} \ell(M_{tors}) \;&=\; \delta(d_1) + \cdots + \delta(d_k), \\ \ell(N_{tors}) \;&=\; \delta(e_1) + \cdots + \delta(e_l). \end{aligned}$$

Da isomorphe Moduln gleiche Länge haben, müssen diese beiden Längen gleich sein. Wir wollen nun per Induktion über die Länge schließen. Der Fall der Länge Null ist trivial, wir dürfen also annehmen, dass ein Primelement $p \in R$ mit $p \mid d_1$ existiert. Wir betrachten dann den Isomorphismus

$$\varphi_{tors}: \quad pM_{tors} \xrightarrow{\sim} pN_{tors}$$

Für $a \in R\setminus\{0\}$ schreiben wir kurz

$$a' \;:=\; \begin{cases} a & \text{falls } p \nmid a, \\ a/p & \text{falls } p \mid a, \end{cases}$$

dann gilt nach Proposition 5.9:

$$\begin{aligned} pM_{tors} \;&=\; R/d_1'R \oplus \cdots \oplus R/d_k'R, \\ pN_{tors} \;&=\; R/e_1'R \oplus \cdots \oplus R/e_l'R. \end{aligned}$$

Es gilt noch immer $d_{i+1}' \mid d_i'$ und $e_{i+1}' \mid e_i'$, auch wenn für die neu erhaltene Liste von Elementarteilern eventuell einige Einheiten am Ende der Liste hinzukommen. Wir setzen

$$\begin{aligned} k_0 \;&:=\; \max\{i:\ p \mid d_i\}, \\ l_0 \;&:=\; \max\{i:\ p \mid e_i\} \cup \{0\} \end{aligned}$$

dann gilt für die Längen der Moduln:

$$\begin{aligned} \ell(pM_{tors}) &= \ell(M_{tors}) - k_0, \\ \ell(pN_{tors}) &= \ell(N_{tors}) - l_0. \end{aligned}$$

Da isomorphe Moduln gleiche Länge haben, erhalten wir $k_0 = l_0$. Per Induktion über die Länge folgt zudem $d'_i \cdot R = e'_i \cdot R$ für alle $i \geq 0$ und damit die Behauptung des Satzes, wobei wir die Listen der Elementarteiler zur Vereinfachung der Notation formal fortsetzen durch $d'_{k+1} = d'_{k+2} = \cdots = e'_{l+1} = e'_{l+2} = \cdots = 1$. □

Korollar 5.11. *Sei R ein Hauptidealring. Dann sind für Matrizen $A \in \mathrm{Mat}(m \times n, R)$ und ebenso für Untermoduln $U \subseteq V = R^m$ die Elementarteiler in Satz 4.3 bzw. 4.8 bis auf Multiplikation mit Einheiten eindeutig bestimmt.*

Beweis. Jeder Untermodul $U \subseteq R^m$ eines endlich erzeugten freien Moduls hat die Form

$$U = \left\{ A \cdot v \in V \mid v \in R^n \right\} \quad \text{für eine Matrix} \quad A \in \mathrm{Mat}(m \times n, R),$$

und umgekehrt erzeugen die Spalten jeder solchen Matrix einen Untermodul. Die nicht-Einheiten unter den Elementarteilern von $U \subseteq V$ bzw. von A sind genau die Elementarteiler des Moduls $M = V/U$ und somit sind sie nach Satz 5.10 eindeutig bestimmt bis auf Multiplikation mit Einheiten. Es bleibt daher nur noch zu zeigen, dass die Gesamtzahl der unter den Elementarteilern von $U \subseteq V$ bzw. A auftretenden Einheiten ebenfalls eindeutig bestimmt ist. Dazu reicht es zu zeigen, dass die Anzahl der Elementarteiler von $U \subseteq V$ eindeutig ist; aber diese Anzahl ist gleich der Länge einer Basis des Untermoduls und als solche eindeutig nach Korollar 4.4. □

Die im Struktursatz 5.1 auftretenden direkten Summanden der Form R/dR lassen sich mittels des chinesischen Restsatzes weiter zerlegen. Dazu benötigen wir eine weitere Definition, die den Begriff des Torsionsuntermoduls verfeinert:

Definition 5.12. Sei M ein R-Modul und $p \in R$ ein Primelement. Dann bezeichnen wir

$$M(p) := \left\{ m \in M \mid \exists n \in \mathbb{N} : \; p^n \cdot m = 0 \right\} \subseteq M$$

als den *p-Torsionsteil* von M. Offenbar ist dieser ein Untermodul von M_{tors}.

Wir wollen uns überlegen, dass im Fall von endlich erzeugten Moduln über Hauptidealringen der gesamte Torsionsuntermodul M_{tors} zerfällt als eine endliche direkte Summe seiner p-Torsionsteile und dass sich diese weiter zerlegen lassen in direkte Summen von Moduln der Form R/p^eR für geeignete $e \in \mathbb{N}$:

Satz 5.13 (Verfeinerter Struktursatz). *Sei R ein Hauptidealring,*

a) Sei M ein endlich erzeugter R-Modul. Dann ist

$$M \simeq R^r \oplus M(p_1) \oplus \cdots \oplus M(p_n)$$

für eindeutige $r,n \in \mathbb{N}_0$ und paarweise nicht-assoziierte, bis auf Umordnen und Multiplikation mit Einheiten eindeutige Primelemente $p_1,\ldots,p_n \in R$.

b) Dabei gilt

$$M(p_i) \simeq \bigoplus_{j=1}^{m_i} R/p_i^{e_{ij}}R \quad \textit{für eindeutige} \quad e_{ij} \in \mathbb{N} \quad \textit{mit} \quad e_{i1} \le e_{i2} \le \cdots \le e_{im_i}.$$

Beweis. Wir beginnen mit der Existenz einer solchen Zerlegung. Da die direkte Summe von je endlich vielen Moduln der angegebenen Form offenbar wieder eine solche Form besitzt, genügt es nach dem Struktursatz 5.1, den Spezialfall $M = R/dR$ mit $d \in R \setminus \{0\}$ zu behandeln. In diesem Fall folgt die Existenz der Zerlegung aus dem Chinesischen Restsatz in Kapitel **??**, Korollar **??**: Genauer liefert dieser einen Isomorphismus von Ringen

$$R/dR \simeq \bigoplus_{i=1}^{n} R/p_i^{e_i}R \quad \text{für die Primfaktorzerlegung} \quad d = u \cdot p_1^{e_1} \cdots p_n^{e_n}$$

mit Primfaktoren $p_i \in R$, einer Einheit $u \in R^\times$ und Exponenten $e_i \in \mathbb{N}$. Dieser ist insbesondere ein Isomorphismus von R-Moduln, da die Modulstruktur auf beiden Seiten von der Ringstruktur induziert ist.

Es bleibt die Eindeutigkeitsaussage zu zeigen. Die Primelemente $p_1,\ldots,p_n$ sind bis auf Assoziiertheit eindeutig bestimmt, denn für beliebige Primelemente $p \in R$ gilt:

$$M(p) \neq \{0\} \quad \Longleftrightarrow \quad p \sim p_i \text{ für ein } i \in \{1,\ldots,n\},$$

wobei $\sim$ Assoziiertheit bedeutet. In der Tat:

- Wenn $p \sim p_i$ ist, gilt offenbar $M(p) = M(p_i) \neq 0$.
- Wenn $p \not\sim p_i$ ist, gilt für jedes $e \in \mathbb{N}$ nach Bézout $a_e p + b_e p_i^e = 1$ mit $a_e, b_e \in R$. Dann ist
$$M(p_i) \longrightarrow M(p_i), \quad m \mapsto p \cdot m$$
ein Isomorphismus, und wenn dies für alle direkten Summanden $M(p_i) \subseteq M$ in der Summe $M_{tors} \simeq M(p_1) \oplus \cdots \oplus M(p_n)$ gilt, ist $M_{tors} \to M_{tors}, m \mapsto p \cdot m$ ein Isomorphismus. In diesem Fall ist also $M(p) = \{0\}$.

Es bleibt zu zeigen, dass für jedes der Primelemente p_i die Exponenten $e_{ij} \in \mathbb{N}$ in der Zerlegung von $M(p_i)$ eindeutig bestimmt sind. Dies folgt aus der Eindeutigkeit im Struktursatz 5.10, angewandt auf den Modul $M(p_i)$. □

Die so gefundene Zerlegung ist optimal in dem Sinne, dass sie sich nicht weiter verfeinern lässt. Hierzu machen wir folgende

Definition 5.14. Ein R-Modul M heißt *unzerlegbar*, wenn es keine Zerlegung der Form

$$M \simeq M' \oplus M''$$

mit zwei von Null verschiedenen R-Moduln $M' \neq \{0\}$ und $M'' \neq \{0\}$ gibt.

Die im Satz 5.13 erhaltenen Summanden lassen sich nicht weiter zerlegen, unser Resultat ist also bestmöglich:

Korollar 5.15. *Sei R ein Hauptidealring, $p \in R$ ein Primelement und $e \in \mathbb{N}$. Dann ist der Modul*

$$M := R/p^e R \quad \textit{unzerlegbar}.$$

Beweis. Sei eine Zerlegung als direkte Summe $M \simeq M' \oplus M''$ gegeben. Nach dem verfeinerten Struktursatz 5.13 gilt

$$\begin{aligned} M' &\simeq R^r \oplus R/p_1^{e_1}R \oplus \cdots \oplus R/p_a^{e_a}R \\ M'' &\simeq R^s \oplus R/p_{a+1}^{e_{a+1}}R \oplus \cdots \oplus R/p_b^{e_b}R \end{aligned}$$

mit geeigneten $r,s \in \mathbb{N}_0$, $e_i \in \mathbb{N}$, $b \geq a$ und Primelementen $p_i \in R$, wobei wir zur Vereinfachung der Notation Mehrfachnennungen von Primelementen erlauben. Es folgt

$$R/p^e R = M \simeq M' \oplus M'' \simeq R^{r+s} \oplus R/p_1^{e_1}R \oplus \cdots \oplus R/p_b^{e_b}R$$

und somit $r = s = 0$ und $b = 1$ wegen der Eindeutigkeit in Satz 5.13. Insbesondere erhalten wir daher wie gewünscht $M' = \{0\}$ oder $M'' = \{0\}$. □

Wir haben in Bemerkung 5.3 gesehen, dass der freie Anteil eines Moduls sich im Allgemeinen auf verschiedene Weise als Untermodul einbetten lässt. Auch die feinere Zerlegung von $M(p_i)$ in unzerlegbare Teile in Satz 5.13(b) ist nur eindeutig bis auf Isomorphie. Im Gegensatz dazu sind die p-Torsionsuntermoduln $M(p_i) \subset M$ eindeutig festgelegt und sehr einfach zu berechnen:

Korollar 5.16. *Sei M ein endlich erzeugter Modul über einem Hauptidealring R, dann gilt:*

a) Es ist $\mathrm{Ann}(M_{tors}) := \{a \in R \mid a \cdot M_{tors} = \{0\}\} = dR$ *für ein* $d \in R \setminus \{0\}$.

b) Für Primelemente $p \in R$ gilt $M(p) \neq \{0\}$ genau dann, wenn $p \mid d$ ist, und in diesem Fall hat man

$$M(p) = \ker(M \xrightarrow{p^e} M) = q \cdot M_{tors} \quad \textit{für } d = p^e q \textit{ mit } e \in \mathbb{N} \textit{ und } p \nmid q.$$

Beweis. Nach Satz 5.13 dürfen wir annehmen, dass $M_{tors} = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} R/p_i^{e_{ij}}R$ mit paarweise nicht-assoziierten Primelementen $p_i \in R$ und Exponenten $e_{ij} \in \mathbb{N}$ ist, und dann gilt

$$\operatorname{Ann}(M_{tors}) \;=\; \bigcap_{i,j} \operatorname{Ann}(R/p_i^{e_{ij}}R) \;=\; dR \quad \text{für} \quad d \;=\; p_1^{e_1}\cdots p_n^{e_n}$$

wobei die Exponenten gegeben sind durch $e_i := \max\{e_{ij} \mid j = 1,2,\dots\}$. Ist $a \in R$ ein von Null verschiedenes Ringelement, so wissen wir aus dem Beweis von Satz 5.13, dass die Abbildung

$$R/p_i^{e_{ij}}R \;\longrightarrow\; R/p_i^{e_{ij}}R, \quad [x] \;\mapsto\; [ax]$$

im Fall $p_i \nmid a$ ein Isomorphismus ist. Wählen wir hier speziell $a = p$ prim, so sehen wir erneut, dass $M(p) \neq \{0\}$ nur dann gelten kann, wenn $p \sim p_i$ für ein $i \in \{1,\dots,n\}$ ist. In diesem Fall ist

$$d \;=\; p^e \cdot q \quad \text{mit} \quad \begin{cases} p \;=\; p_i \\ e \;=\; e_i \\ q \;\sim\; \prod_{k\neq i} p_k^{e_k} \end{cases}$$

In der Zerlegung

$$M_{tors} \;=\; M_i \oplus M_i' \quad \text{mit} \quad M_i \;:=\; \bigoplus_{j=1}^{m_i} R/p_i^{e_{ij}}R \quad \text{und} \quad M_i' \;:=\; \bigoplus_{k\neq i}\bigoplus_{j=1}^{m_k} R/p_k^{e_{kj}}R$$

operiert somit

- p^e durch Null auf M_i und durch einen Isomorphismus auf M_i',
- q durch Null auf M_i' und durch einen Isomorphismus auf M_i.

Damit folgt die Behauptung. □

Zum Abschluß wollen wir die Resultate dieses Abschnitts im Fall $R = \mathbb{Z}$ kurz zusammenfassen. Wir erhalten in diesem Fall eine Klassifikation von allen endlich erzeugten abelschen Gruppen:

Korollar 5.17 (Hauptsatz über endlich erzeugte abelsche Gruppen). *Sei G eine endlich erzeugte abelsche Gruppe. Dann ist*

$$G \;\simeq\; \mathbb{Z}^r \times G_1 \times \cdots \times G_n \quad \textit{mit} \quad G_i \;:=\; \mathbb{Z}/p_i^{e_{i1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i^{e_{im_i}}\mathbb{Z}$$

für

- *ein eindeutiges $r \in \mathbb{N}_0$,*
- *paarweise verschiedene, bis auf Umnumerieren eindeutige Primzahlen p_i,*
- *eindeutige $m_i \in \mathbb{N}$ und eindeutige Exponenten $e_{ij} \in \mathbb{N}$ mit $1 \leq e_{i1} \leq \cdots \leq e_{im_i}$.*

Beweis. Dies folgt direkt aus dem Fall $R = \mathbb{Z}$ des vorigen Satzes: Eine endliche direkte Summe von $\mathbb{Z}$-Moduln ist nichts anderes als ein endliches Produkt abelscher Gruppen. □

Beispiel 5.18. Sei p eine Primzahl. Jede endliche abelsche Gruppen der Ordnung p^2 ist isomorph zu

$$\mathbb{Z}/p^2\mathbb{Z} \quad \text{oder} \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},$$

und diese beiden Gruppen sind nicht isomorph zueinander. Andererseits gibt es für jede Primzahl $q \neq p$ bis auf Isomorphie genau eine endliche abelsche Gruppe der Ordnung pq, nämlich

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Beispiel 5.19. Für endliche Gruppen wissen wir aus dem Satz von Lagrange, dass die Ordnung jeden Gruppenelementes ein Teiler der Gruppenordnung ist. Analog zum Minimalpolynom eines Endomorphismus definieren wir den *Exponent* einer multiplikativ geschriebenen endlichen Gruppe G durch

$$e(G) := \min\{n \in \mathbb{N} \mid \forall g \in G : \, g^n = 1\}.$$

Der Exponent ist immer ein Teiler der Gruppenordnung. Für additiv geschriebene abelsche Gruppen

$$G \simeq G_1 \times \cdots \times G_n \quad \text{mit} \quad G_i = \mathbb{Z}/p_i^{e_{i1}}\mathbb{Z} \times \cdots \mathbb{Z}/p_i^{e_{im_i}}\mathbb{Z}$$

sind die Ordnung und der Exponent gegeben durch

$$\begin{aligned} |G| &= \prod_{i=1}^{n} \prod_{j=1}^{m_i} p_i^{e_{ij}} = p_1^{e_1} \cdots p_n^{e_n} \qquad \text{mit} \quad e_i = e_{i1} + \cdots + e_{im_i}, \\ e(G) &= \operatorname{kgV}\left\{p_i^{e_{ij}}\right\} = p_1^{d_1} \cdots p_n^{d_n} \qquad \text{mit} \quad d_i = \max\{e_{i1}, \ldots, e_{im_i}\}. \end{aligned}$$

Beispielsweise ist die Gruppe G zyklisch genau dann, wenn $|G| = e(G)$ ist.