Lineare Algebra für Informatiker

Matthias Künzer

Universität Ulm

Inhalt

Vorwort

Das vorliegende Skript wurde begleitend zu einer Vorlesung Lineare Algebra für Informatiker erstellt, gehalten in Ulm im Wintersemester 2002/03. Inhaltlich lehnt es sich an die Vorlesung Gerhard Baurs aus dem Vorjahr an [**1**]. Hinzugefügt wurden zusätzliche Beispiele endlicher Körper. Ferner wurde die Jordansche Normalform vollends vollständig abgehandelt. Dafür wurde die Behandlung der ebenen Quadriken aus Zeitgründen weggelassen.

Endliche Körpererweiterungen von $\mathbf{F}_p$ sind im Hinblick auf die Anwendungen in der Informatik, und insbesondere in der Codierungstheorie, mit aufgenommen worden. Nach Erläuterung des allgemeinen Konstruktionsprinzips für Körpererweiterungen mittels irreduzibler Polynome beschränken wir uns jedoch pars pro toto auf $\mathbf{F}_4$, $\mathbf{F}_8$ und $\mathbf{F}_9$.

Der Algorithmus zur Berechnung der Jordanschen Normalform ist für nicht diagonalisierbare Matrizen etwas aufwendiger. Man erhält so aber ein vollständiges Repräsentantensystem der Konjugationsklassen quadratischer Matrizen über einem algebraisch abgeschlossenen Körper. Insbesondere kennt man auf diese Weise jeden Endomorphismus eines endlichdimensionalen Vektorraums über einem solchen Körper.

Im abschließenden Abschnitt werden normale und also insbesondere hermitesche Matrizen unitär diagonalisiert. Wir hoffen, daß sich der Leser die zur Behandlung von Quadriken notwendige geometrische Interpretation als Hauptachsentransformation bei Bedarf selbst aneignen kann.

Ich möchte mich bei meinen Übungsleitern Marc Meister und Norbert Renz für zahlreiche kritische Anmerkungen bedanken. Desweiteren erhielt ich aus den Reihen der Studenten, der Korrektoren und der Tutoren viele Hinweise auf Fehler, auch dafür meinen Dank.

Ulm, den 18.02.2003

Matthias Künzer

In die aktualisierte Version wurden der Beweis des Fundamentalsatzes der Algebra nach Derksen [**2**] und die Jordanform nach Frobenius und Böge (cf. [**10,** p. 144–146]) als *fakultative* Abschnitte mit aufgenommen. Ferner wurden zahlreiche Korrekturen und Umstellungen vorgenommen. So z.B. wird die direkte Summe mehrerer Unterräume nun unmittelbar nach der direkten Summe zweier Unterräume eingeführt. Ein Dank geht an Andreas Martin, der mich von einer ökonomischeren Darlegungsweise des Nilpotenzlemmas überzeugte. Ein weiterer Dank geht an Leonhard Grünschloß für eine sorgfältige Durchsicht des ganzen Manuskripts.

Ulm, den 26.08.2004

Matthias Künzer

Ein Abschnitt zur vereinfachten Berechnung des charakteristischen Polynoms wurde mit aufgenommen. Die verwandte Methode kenne ich von Max Neunhöffer.

Aachen, den 11.10.2006

Matthias Künzer

Kapitel 1

Mengen, Gruppen, Ringe, Körper

Die Mengentheorie ist die Sprache der Mathematik. Gruppen werden uns in der Form von symmetrischen Gruppen bei den Determinanten begegnen. Sie werden auch als Bestandteil der Definitition von Ringen auftreten. Als Ringe werden wir etwa Polynomringe kennenlernen, oder aber eben Körper, wie etwa die reellen Zahlen $\mathbf{R}$, die komplexen Zahlen $\mathbf{C}$ und die ganzen Zahlen modulo einer Primzahl p, geschrieben $\mathbf{F}_p$. Körper sind als die zugrundegelegten Skalarbereiche von Vektorräumen der Ausgangspunkt der Linearen Algebra.

1.1 Mengen

1.1.1 Allgemeines

Seien X und Y Mengen.

Beispiele. Mit $\mathbf{N}$ werde die Menge der natürlichen Zahlen bezeichnet (einschließlich 0), mit $\mathbf{Z}$ die der ganzen Zahlen, mit $\mathbf{Q}$ die der rationalen Zahlen und mit $\mathbf{R}$ die der reellen Zahlen. Die leere Menge schreibt sich $\emptyset$. Sind $a, b \in \mathbf{Z}$, so schreiben wir

$$[a, b] \ := \ \{z \in \mathbf{Z} \mid a \leqslant z \leqslant b\} \ \subseteq \ \mathbf{Z}$$

für das ganzzahlige Intervall von a bis b.

Definition. Mit $X \times Y := \{(x, y) \mid x \in X, \ y \in Y\}$ bezeichnen wir das *cartesische Produkt* der Mengen X und Y, d.h. die Menge der geordneten Paare von Elementen aus X in erster und aus Y in zweiter Stelle. Analog ist $X \times Y \times Z$ die Menge der geordneten Tripel mit Einträgen aus X, Y und Z. Usf.

Definition. Die *Potenzmenge* $\mathfrak{P}(X) := \{U \mid U \subseteq X\}$ ist die Menge der Teilmengen von X, d.h. $U \in \mathfrak{P}(X) \iff U \subseteq X$.

Definition. Ist X eine *endliche* Menge, so bezeichnet $\#X$ die Anzahl ihrer Elemente.

Definition. Sind U_i für $i \in I$ Teilmengen von X, so heißt ihre Vereinigung $V := \bigcup_{i \in I} U_i \subseteq X$ *disjunkt,* falls es für jedes Element $x \in X$ höchstens ein $i \in I$ gibt mit $x \in U_i$. Diesenfalls schreiben wir auch $V = \bigsqcup_{i \in I} U_i$.

1.1.2 Abbildungen

Definition. Seien X, Y und Z Mengen.

Eine *Abbildung* $f : X \longrightarrow Y$ (oder $X \xrightarrow{f} Y$) ist eine Zuordnung, die jedem Element $x \in X$ genau ein Element $f(x) \in Y$ zuweist. Für die Zuordnung eines einzelnen Elementes schreiben wir auch $x \longmapsto f(x)$.

Sind zwei Abbildungen $X \xrightarrow{f} Y \xrightarrow{g} Z$ gegeben, so bezeichne $g \circ f : X \longrightarrow Z$ deren *Komposition,* d.h. $(g \circ f)(x) := g(f(x))$ für alle $x \in X$.

Die identische Abbildung wird $X \xrightarrow{1_X} X : x \longmapsto x$ geschrieben, oder auch id_X, falls Verwechslungsgefahr besteht.

Seien $U \subseteq X$ und $V \subseteq Y$ Teilmengen. Wir schreiben $f(U) = \{f(x) \in Y \mid x \in U\} \subseteq Y$ und $f^{-1}(V) = \{x \in X \mid f(x) \in V\} \subseteq X$.

Sind $X \xrightarrow{f} Y$ und $X' \xrightarrow{f'} Y'$ Abbildungen, so schreiben wir $f \times f' : X \times X' \longrightarrow Y \times Y' : (x, x') \longmapsto (f(x), f'(x'))$ für deren cartesisches Produkt.

Die Abbildung f heißt *surjektiv,* falls $f(X) = Y$, d.h. falls $\#f^{-1}(\{y\}) \geqslant 1$ für alle $y \in Y$.

Sie heißt *injektiv,* falls für $x, x' \in X$ aus $f(x) = f(x')$ stets $x = x'$ geschlossen werden kann. D.h. falls $\#f^{-1}(\{y\}) \leqslant 1$ für alle $y \in Y$.

Sie heißt *bijektiv,* falls sie injektiv und surjektiv ist, d.h. falls $\#f^{-1}(\{y\}) = 1$ für alle $y \in Y$. Symbolisch schreiben wir $f : X \xrightarrow{\sim} Y$.

Lemma. *Die Abbildung $X \xrightarrow{f} Y$ ist genau dann bijektiv, wenn es eine Abbildung $Y \xrightarrow{g} X$ so gibt, daß $g \circ f = 1_X$ und $f \circ g = 1_Y$. Die Abbildung g ist eindeutig bestimmt, und wir schreiben auch $f^{-1} := g$.*

Beweis. Sei ein solches g als existent angenommen. Dann ist f surjektiv wegen $y = f(g(y))$ für alle $y \in Y$. Zeigen wir die Injektivität. Seien $x, x' \in X$ mit $f(x) = f(x')$ gegeben. Es folgt $x = g(f(x)) = g(f(x')) = x'$. Insgesamt ist f also bijektiv.

Sei nun f als bijektiv angenommen. Sei $y \in Y$ vorgegeben. Da f surjektiv ist, gibt es ein x mit $f(x) = y$, und da f injektiv ist, existiert höchstens ein solches x. Wir dürfen also $g(y) := x$ setzen, und sehen, daß nach Konstruktion $f(g(y)) = y$ gilt, d.h. $f \circ g = 1_Y$. Bleibt zu zeigen, daß $g \circ f = 1_X$, d.h. daß $g(f(x)) = x$ für alle $x \in X$. Nun ist aber $f(g(f(x))) = f(x)$, und die behauptete Gleichung folgt aus der Injektivität von f.

Damit ist die Äquivalenz der beiden Aussagen nachgewiesen. In der Praxis ist es oft ratsam, anstatt Injektivität und Surjektivität zu zeigen, besser die Umkehrabbildung hinzuschreiben.

Bleibt noch die Eindeutigkeit von g zu zeigen. Sei noch eine Abbildung $Y \xrightarrow{\tilde{g}} X$ gegeben mit $f \circ \tilde{g} = 1_Y$ (das genügt bereits als Annahme). Dann ist $g = g \circ f \circ \tilde{g} = \tilde{g}$. □

Vorsicht. Das Urbild $f^{-1}(V)$ einer Teilmenge existiert für alle Abbildungen f, nicht nur für die bijektiven. Ist f bijektiv, so stimmen die beiden Bedeutungen von $f^{-1}(V)$ – "Urbild unter f" und "Bild unter f^{-1}" – überein. Für ein einzelnes Element $y \in Y$ ist $f^{-1}(\{y\}) = \{f^{-1}(y)\}$.

1.1.3 Äquivalenzrelationen

Seien X und Y Mengen.

Definition. Eine *Relation* zwischen X und Y ist eine Teilmenge $R \subseteq X \times Y$. Für $(x, y) \in R$ schreiben wir auch $x\,R\,y$, d.h. x ist in Relation zu y.

Etwa ist einer Abbildung $f : X \longrightarrow Y$ als Relation ihr *Graph*

$$\Gamma_f \;:=\; \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$$

zugeordnet.

Man kann über die Graphenkonstruktion umgekehrt Abbildungen auch als spezielle Relationen Γ definieren – für $x \in X$ wird verlangt, daß es genau ein $y \in Y$ so gibt, daß $x\Gamma y$ gilt; man setzt dann $f_\Gamma(x) := y$. Dies nur als Bemerkung.

Definition. Eine Relation $(\sim) \subseteq X \times X$ (d.h. *auf* X) heißt *Äquivalenzrelation,* falls (A 1, 2, 3) gelten.

(A 1) Für alle $x \in X$ ist $x \sim x$ (Reflexivität).

(A 2) Für alle $x, y \in X$ ist $x \sim y \iff y \sim x$ (Symmetrie).

(A 3) Für alle $x, y, z \in X$ impliziert $x \sim y$ und $y \sim z$, daß $x \sim z$ (Transitivität).

Sei nun $(\sim)$ eine Äquivalenzrelation auf einer Menge X.

Definition. Die *Äquivalenzklasse* von $x \in X$ ist gegeben durch

$$\bar{x} \;:=\; \{y \in X \mid y \sim x\} \;\subseteq\; X\ .$$

Jedes Element von $\bar{x}$ heißt *Repräsentant* von $\bar{x}$. Wegen (A 1) ist x Repräsentant von $\bar{x}$.

Beispiel. Sei $X = \{1, 12, 7, 74, 3\}$, und sei $x \sim y$ genau dann, wenn die Ziffernzahlen von x und y übereinstimmen. Dann gibt es die Äquivalenzklassen

$$\begin{array}{rcl} \overline{1} = \overline{3} = \overline{7} & = & \{1, 3, 7\}\ , \\ \overline{12} = \overline{74} & = & \{12, 74\}\ . \end{array}$$

Lemma. *Es ist $\bar{x} = \bar{y}$ genau dann, wenn $x \sim y$.*

Beweis. Ist $\bar{x} = \bar{y}$, so ist insbesondere $x \in \bar{y}$, was gerade $x \sim y$ bedeutet.

Ist umgekehrt $x \sim y$, so wollen wir zunächst $\bar{x} \subseteq \bar{y}$ zeigen. Ist $u \in \bar{x}$, so ist wegen $u \sim x \sim y$ mit (A 3) auch $u \in \bar{y}$. Zeigen wir nun $\bar{y} \subseteq \bar{x}$. Ist $v \in \bar{y}$, so ist wegen $v \sim y \sim x$, wofür wir (A 2) verwandt haben, mit (A 3) auch $v \in \bar{x}$. ▫

Lemma.

(i) *Für $x, y \in X$ gilt entweder $\bar{x} = \bar{y}$ oder $\bar{x} \cap \bar{y} = \emptyset$.*

(ii) *Es gibt (mindestens) eine Teilmenge $S \subseteq X$ so, daß*

$$X = \bigsqcup_{s \in S} \bar{s} .$$

Eine solche Teilmenge S heißt auch Repräsentantensystem *von $(\sim)$.*

(iii) *Bezeichnet $X/\!\sim\ := \{\bar{x} \mid x \in X\} \subseteq \mathfrak{P}(X)$ die Menge der Äquivalenzklassen (die Aufzählung über $x \in X$ ist i.a. redundant!), so ist die Abbildung $S \longrightarrow X/\!\sim\ :\ s \longmapsto \bar{s}$ bijektiv.*

Beweis. Zu (i). Seien $x, y \in X$ mit $\bar{x} \cap \bar{y} \neq \emptyset$ gegeben. Wir fixieren ein Element $z \in \bar{x} \cap \bar{y}$ und haben $\bar{x} = \bar{y}$ zu zeigen.

Wir zeigen $\bar{x} \subseteq \bar{y}$. Sei $u \in \bar{x}$. Mit (A 2) wird $u \sim x \sim z \sim y$, also mit (A 3) auch $u \sim y$, was nach Definition gerade $u \in \bar{y}$ heißt.

Die Inklusion $\bar{x} \supseteq \bar{y}$ zeigt man genauso. Also ist in der Tat $\bar{x} = \bar{y}$.

Zu (ii). Wir wählen nun aus jeder Äquivalenzklasse genau ein Element und sammeln die ausgewählten Elemente in einer Menge S ([1]).

Wir zeigen zunächst, daß für jedes Element $x \in X$ wenigstens ein $s \in S$ existiert mit $x \in \bar{s}$, d.h. daß $X = \bigcup_{s \in S} \bar{s}$ (gewöhnliche Vereinigung). Sei $x \in X$, und sei $s \in \bar{x} \cap S$ – diese Schnittmenge enthält nach Konstruktion S genau ein Element. Dann ist $x \in \bar{s} \subseteq \bigcup_{s \in S} \bar{s}$.

Nun zeigen wir, daß die Vereinigung disjunkt ist, d.h. daß für jedes Element $x \in X$ höchstens ein $s \in S$ existiert mit $x \in \bar{s}$. Sei $x \in \bar{s}$ und $x \in \bar{s}'$ mit $s, s' \in S$. Dann ist $s \sim x \sim s'$, es liegen also s und s' in $\bar{x}$. Da aber jede Äquivalenzklasse nach Konstruktion genau ein Element von S enthält, folgt $s = s'$.

Zu (iii). Da es zu jeder Äquivalenzklasse einen Repräsentanten in S gibt, ist die Abbildung surjektiv. Da es sogar genau einen solchen gibt, ist die Abbildung auch injektiv. ▫

Beispiel. Sei $X = \mathbf{Z}$, und sei $x \sim y$ genau dann, wenn $x - y \in 3\mathbf{Z} := \{3z \mid z \in \mathbf{Z}\}$, geschrieben $x \equiv_3 y$, gesprochen x kongruent zu y modulo 3. (A 1, 2) sind klar. Für (A 3) argumentieren wir wie folgt. Sei $x \sim y \sim z$, genauer, sei $x - y = 3a$ und $y - z = 3b$ mit $a, b \in \mathbf{Z}$. Dann ist $x - z = (x - y) + (y - z) = 3(a + b) \in 3\mathbf{Z}$, und mithin $x \sim z$.

[1] Dieser intuitiv einleuchtende Schritt benötigt strenggenommen das sogenannte *Auswahlaxiom.*

Es ist $\mathbf{Z} = \bar{0} \sqcup \bar{1} \sqcup \bar{2}$, d.h. es ist $S = \{0, 1, 2\}$ ein Repräsentantensystem. Alternativ ist aber auch $S' = \{3, -5, 8\}$ ein Repräsentantensystem.

Bemerkung. Sei $P(X) := \{T \subseteq \mathfrak{P}(X) \mid \bigsqcup_{B \in T} B = X\}$ die Menge der *Partitionen* von X, und sei $A(X) := \{(\sim) \subseteq X \times X \mid (\sim) \text{ ist Äquivalenzrelation}\}$ die Menge der Äquivalenzrelationen auf X. Es gibt eine Bijektion

$$
\begin{array}{rcl}
P(X) & \xrightarrow{\sim} & A(X) \\
T & \longmapsto & (\sim_T)\,, \quad \text{wobei } x \sim_T y \Longleftrightarrow \text{es gibt ein } B \in T \text{ mit } \{x, y\} \subseteq B \\
\{\bar{x} \mid x \in X\} & \longleftarrow\!\shortmid & (\sim)\,,
\end{array}
$$

wobei in der dritten Zeile die Äquivalenzklasse $\bar{x}$ bezüglich $(\sim)$ zu bilden ist.

1.2 Gruppen

Definition. Sei G eine Menge, und sei $(\cdot) : G \times G \longrightarrow G : (x, y) \longmapsto x \cdot y$ eine Abbildung, genannt *Verknüpfung* oder *Operation.* Betrachte folgende Bedingungen.

(G 1) Für alle $x, y, z \in G$ ist $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Assoziativität).

(G 2) Es existiert ein Element $e \in G$ so, daß $x \cdot e = e \cdot x = x$ für alle $x \in G$ (neutrales Element).

(G 3) Für alle $x \in G$ existiert ein $y \in G$ mit $x \cdot y = y \cdot x = e$ (inverses Element).
(Das Element e aus (G 2) ist eindeutig, s.u.)

(G 4) Für alle $x, y \in G$ ist $x \cdot y = y \cdot x$ (Kommutativität).

Das Paar $(G, \cdot)$ (oder kurz auch nur G) heißt *Monoid,* falls (G 1, 2) gelten. Wegen (G 1) schreibt man bei iterierten Produkten in einem Monoid meist keine Klammern.

G heißt *abelsches Monoid,* falls (G 1, 2, 4) gelten.

G heißt *Gruppe,* falls (G 1, 2, 3) gelten.

G heißt *abelsche Gruppe,* falls (G 1, 2, 3, 4) gelten.

Sei G ein Monoid. Sind e und e' neutrale Elemente von G im Sinne von (G 2), so ist $e = e \cdot e' = e'$. Das neutrale Element ist also eindeutig bestimmt. Man schreibt auch $1 := e$.

Sei G nun eine Gruppe. Sind y und y' Inverse von $x \in G$ im Sinne von (G 3), so ist wegen $y = y \cdot e = y \cdot x \cdot y' = e \cdot y' = y'$. Auch das Inverse ist damit eindeutig. Man schreibt daher auch $x^{-1} := y$. Beachte, daß insbesondere $(x^{-1})^{-1} = x$ und $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Wir schreiben auch $x^n := \underbrace{x \cdot x \cdots x}_{n \text{ Faktoren}}$ und $x^{-n} := \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n \text{ Faktoren}}$ für $n \geqslant 1$ und $x^0 = 1$.

Damit sind $x^{m+n} = x^m \cdot x^n$ und $(x^m)^n = x^{mn}$ für $m, n \in \mathbf{Z}$.

Ist die Gruppe abelsch und ist die Verknüpfung mit dem Symbol $+$ bezeichnet, so schreibt man jedoch in der Regel $0 := e$ und $-x := y$. Auch schreibt man $x + (-x') = x - x'$ für $x, x' \in G$, sowie $nx := \underbrace{x + x + \cdots + x}_{n \text{ Summanden}}$ und $(-n)x := \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ Summanden}}$ für $n \geqslant 1$, und $0 \cdot x := 0$.

Beispiele. $(\mathbf{N}, +)$ und $(\mathbf{N}, \cdot)$ sind abelsche Monoide. $(\mathbf{Z}, +)$ ist eine abelsche Gruppe, $(\mathbf{Z}, \cdot)$ ist ein abelsches Monoid. $(\mathbf{Q}, +)$ ist eine abelsche Gruppe, $(\mathbf{Q}, \cdot)$ ist ein abelsches Monoid, $(\mathbf{Q} \smallsetminus \{0\}, \cdot)$ ist eine abelsche Gruppe. Dito mit $\mathbf{R}$ statt $\mathbf{Q}$.

Definition. Eine nichtleere Teilmenge U einer Gruppe G heißt *Untergruppe,* falls für alle $x, y \in U$ auch $x \cdot y^{-1} \in U$. Wir schreiben $U \leqslant G$.

Lemma. *Ist $U \leqslant G$, dann ist auch $(U, \cdot)$ (eingeschränkte Verknüpfung) eine Gruppe.*

Beweis. Es gibt in $U \neq \emptyset$ ein Element $x \in U$. Somit ist auch $x \cdot x^{-1} = 1 \in U$. Liegen x und y in U, so auch $y^{-1} = 1 \cdot y^{-1}$, und mithin auch $x \cdot (y^{-1})^{-1} = x \cdot y$. Damit ist die Operation $U \times U \xrightarrow{(\cdot)} U$ definiert. Die Eigenschaften (G 1, 2, 3) vererben sich aus G. ▫

Definition. Seien G und H Gruppen. Eine Abbildung $G \xrightarrow{f} H$ heißt *Gruppenmorphismus,* falls für alle $x, y \in G$ gilt, daß $f(x \cdot y) = f(x) \cdot f(y)$. Hierbei bezeichnet $x \cdot y$ das Produkt in G, und $f(x) \cdot f(y)$ das Produkt in H.

Es wird

$$f(1) \;=\; f(1) \cdot f(1) \cdot f(1)^{-1} \;=\; f(1 \cdot 1) \cdot f(1)^{-1} \;=\; f(1) \cdot f(1)^{-1} \;=\; 1\;.$$

Ferner gilt für alle $x \in G$

$$f(x^{-1}) \;=\; f(x^{-1}) \cdot f(x) \cdot f(x)^{-1} \;=\; f(x^{-1} \cdot x) \cdot f(x)^{-1} \;=\; f(1) \cdot f(x)^{-1} \;=\; 1 \cdot f(x)^{-1} \;=\; f(x)^{-1}\;.$$

Definition. Der *Kern* des Gruppenmorphismus $G \xrightarrow{f} H$ ist gegeben durch

$$\mathrm{Kern}\, f \;:=\; f^{-1}(\{1\}) \;=\; \{x \in G \mid f(x) = 1\}\;.$$

Der Kern ist eine Untergruppe, $\mathrm{Kern}\, f \leqslant G$.

Lemma. *Ein Gruppenmorphismus $G \xrightarrow{f} H$ ist injektiv genau dann, wenn* $\mathrm{Kern}\, f = \{1\}$.

Beweis. Ist f injektiv, so folgt aus $f(x) = 1 = f(1)$, daß $x = 1$.

Ist umgekehrt $\mathrm{Kern}\, f = \{1\}$, so folgt aus $f(x) = f(y)$ zunächst $f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1} = f(y) \cdot f(y)^{-1} = 1$, und also $x \cdot y^{-1} = 1$, d.h. $x = x \cdot y^{-1} \cdot y = y$. Somit ist f injektiv. ▫

Der minimale Exponent $m \geqslant 1$, für welchen $x^m = 1$ ist, heißt – sofern existent – die *Ordnung* von x. Ist $\#G$ endlich, so hat jedes Element x von G eine Ordnung. In der Tat, es muß unter den Potenzen von x wenigstens zwei übereinstimmende geben, sagen wir $x^a = x^b$ mit $a, b \in \mathbf{Z}$, $a < b$. Dann ist $x^{b-a} = 1$.

Lemma (Lagrange). *Ist G eine endliche Gruppe und U eine Untergruppe von G, so ist $\#U$ ein Teiler von $\#G$. Insbesondere teilt die Ordnung jedes Elements x von G die Anzahl $\#G$ der Elemente von G.*

Beweis. Sei auf G eine Relation dadurch erklärt, daß $x \sim y$ genau dann gelte, wenn es ein $u \in U$ gibt mit $y = xu$, wobei $x, y \in G$. Da U eine Untergruppe ist, ist dies eine Äquivalenzrelation. Die Äquivalenzklasse von $x \in G$ wird vermittels $y \longmapsto x^{-1}y$ bijektiv auf U abgebildet. Die Äquivalenzklassen enthalten also alle $\#U$ Elemente, und die erste Behauptung folgt mit der disjunkten Zerlegung von G in Äquivalenzklassen.

Für die zweite Behauptung betrachten wir die Untergruppe $\langle x\rangle := \{x^m \mid m \in \mathbf{Z}\} \leqslant G$. Bezeichnet n die Ordnung von x, so ist $\langle x\rangle = \{x^t \mid t \in [0, n-1]\}$. In der Tat kann man jedes $m \in \mathbf{Z}$ schreiben als $m = ns + t$ mit $s \in \mathbf{Z}$ und $t \in [0, n-1]$, und es wird $x^m = x^{ns+t} = x^{ns}x^t = x^t$. Außerdem ist $x^t \neq x^{t'}$ für $t, t' \in [0, n-1]$ mit $t \neq t'$. Wäre nämlich $x^t = x^{t'}$, und wäre $t < t'$, so wäre $x^{t'-t} = 1$ und $t' - t \in [1, n-1]$, was der Minimalität von $n \geqslant 1$ mit $x^n = 1$ widerspräche. Also teilt $n = \#\langle x\rangle$ die Anzahl $\#G$. ▫

1.3 Die symmetrische Gruppe

1.3.1 Permutationen und Zykel

Symmetrische Gruppe. *Sei $n \geqslant 1$, und sei $\mathcal{S}_n$ die Menge der Bijektionen von $[1, n]$ nach $[1, n]$. Zusammen mit der Komposition $\mathcal{S}_n \times \mathcal{S}_n \longrightarrow \mathcal{S}_n : (\sigma, \rho) \longmapsto \sigma \circ \rho$ bildet $(\mathcal{S}_n, \circ)$ eine Gruppe, genannt die* symmetrische Gruppe (auf n Elementen). *Die Elemente von $\mathcal{S}_n$ heißen auch* Permutationen.

Beweis. Wir haben die Gruppeneigenschaften nachzuweisen. Sind $\sigma : [1, n] \xrightarrow{\sim} [1, n]$ und $\rho : [1, n] \xrightarrow{\sim} [1, n]$ bijektiv, so auch $\rho \circ \sigma : [1, n] \xrightarrow{\sim} [1, n]$. Damit gibt die Komposition eine Abbildung $(\circ) : \mathcal{S}_n \times \mathcal{S}_n \longrightarrow \mathcal{S}_n$. Die Komposition ist assoziativ, es gilt also (G 1). Es ist $1_{[1,n]} \circ \sigma = \sigma \circ 1_{[1,n]} = \sigma$, und dieses neutrale Element $1_{\mathcal{S}_n} = 1_{[1,n]}$ zeigt (G 2). Schließlich sind Bijektionen invertierbar, woraus (G 3) folgt.

Wir schreiben ein Element $\sigma \in \mathcal{S}_n$ als

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

Vorsicht. $\mathcal{S}_n$ ist im allgemeinen nicht abelsch. In $\mathcal{S}_3$ erhalten wir z.B. $\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$, während $\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$.

Zykelschreibweise. Eine etwas handlichere Bezeichnungsweise geht wie folgt.

Sei $n \geqslant 1$ und sei uns ein $\sigma \in \mathcal{S}_n$ gegeben. Wir definieren eine Äquivalenzrelation auf $[1, n]$ durch $a \sim b$ genau dann, wenn es ein $m \in \mathbf{Z}$ gibt mit $b = \sigma^m(a)$. Die Äquivalenzklassen sind von der Form $\bar{a} = \{\sigma^m(a) \mid m \in \mathbf{Z}\}$. Sei $S = \{s_1, \ldots, s_k\}$ ein Repräsentantensystem.

Sei $i_j = \#\bar{s}_j$ für $j \in [1, k]$. Nicht redundant aufgezählt ist

$$\bar{s}_j = \{\sigma^0(s_j), \sigma^1(s_j), \ldots, \sigma^{i_j - 1}(s_j)\}.$$

In der Tat, da $[1,n]$ endlich ist, gibt es Exponenten $u,v \geqslant 0$, $u < v$ mit $\sigma^u(s_j) = \sigma^v(s_j)$, mithin $\sigma^{v-u}(s_j) = s_j$. Sei $m \geqslant 1$ minimal mit $\sigma^m(s_j) = s_j$. Dann sind $\sigma^0(s_j)$, $\sigma^1(s_j)$, $\dots$, $\sigma^{m-1}(s_j)$ paarweise verschieden, da ansonsten mit $u < v$ wie eben, nur dazuhin $u,v \in [0,m-1]$, wegen $v-u \in [1,m-1]$ ein Widerspruch zur Minimalität von m entstünde. Damit ist $i_j \geqslant m$. Ferner können wir $k \in \mathbf{Z}$ schreiben als $k = c + dm$ mit $c \in [0,m-1]$ und $d \in \mathbf{Z}$, und erhalten $\sigma^k(s_j) = \sigma^{c+dm}(s_j) = \sigma^c(s_j)$. Damit ist $i_j = m$, da die angegebene Aufzählung genau alle Elemente von $\bar{s}_j$ umfaßt.

Wir schreiben nun auch

$$\sigma \;=\; (\sigma^0(s_1),\sigma^1(s_1),\dots,\sigma^{i_1-1}(s_1))(\sigma^0(s_2),\sigma^1(s_2),\dots,\sigma^{i_2-1}(s_2))\cdots(\sigma^0(s_k),\sigma^1(s_k),\dots,\sigma^{i_k-1}(s_k))\ .$$

Ein Ausdruck der Form $(\sigma^0(s_j),\sigma^1(s_j),\dots,\sigma^{i_j-1}(s_j))$ heißt *Zykel* von σ. Zykel der Länge 1 werden auch gerne weggelassen. Für die Identität – die so zum leeren Ausdruck würde – schreiben wir jedoch weiterhin $1 \in \mathcal{S}_n$. Beachte noch, daß

$$\begin{array}{rcl}\sigma &=& (\sigma^0(s_1),\sigma^1(s_1),\dots,\sigma^{i_1-1}(s_1)) \;\;\cdots\;\; (\sigma^0(s_k),\sigma^1(s_k),\dots,\sigma^{i_k-1}(s_k)) \\ &=& (\sigma^0(s_1),\sigma^1(s_1),\dots,\sigma^{i_1-1}(s_1)) \circ\cdots\circ (\sigma^0(s_k),\sigma^1(s_k),\dots,\sigma^{i_k-1}(s_k))\ .\end{array}$$

Beispiel. Etwa ist

$$\left(\begin{smallmatrix}1&2&3&4&5&6\\2&5&6&4&1&3\end{smallmatrix}\right) \;=\; (1,2,5)(3,6)(4) \;=\; (1,2,5)(3,6)\ .$$

Dies berechnet sich wie folgt. Wähle z.B. den Repräsentanten 1. Bilde dessen Äquivalenzklasse $\{\sigma^0(1) = 1,\ \sigma^1(1) = 2,\ \sigma^2(1) = 5\}$ (beachte $\sigma^3(1) = 1$). Wähle als nächsten Repräsentanten ein Element in $[1,6] \smallsetminus \bar{1}$, z.B. das kleinste solche Element 3. Bilde dessen Äquivalenzklasse $\{\sigma^0(3) = 3,\ \sigma^1(3) = 6\}$ (beachte $\sigma^2(3) = 3$). Wähle als nächsten Repräsentanten ein Element in $[1,6] \smallsetminus (\bar{1} \cup \bar{3})$, z.B. das kleinste (und bereits einzige) solche Element 4. Bilde dessen Äquivalenzklasse $\{\sigma^0(4) = 4\}$ (beachte $\sigma^1(4) = 4$). Die disjunkte Vereinigung der gefundenen Äquivalenzklassen $\{1,2,5\} \sqcup \{3,6\} \sqcup \{4\}$ ergibt nun bereits $[1,6]$, so daß $S = \{1,3,4\}$ ein Repräsentantensystem darstellt. Bleibt uns, die gefundenen Zykel aneinanderzureihen.

Beispiel. Es ist $\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) = (1,2)(3) = (1,2)$ und $\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = (1,2,3)$. Die Rechnungen in obigem Beispiel lesen sich nun $(1,2)\circ(1,2,3) = (2,3)$ und $(1,2,3)\circ(1,2) = (1,3)$.

Beispiel.

$$\begin{array}{rcccl} ((1,2,5)(3,4))^6 &=& (1,2,5)^6 \circ (3,4)^6 &=& 1\ , \\ ((1,2,3,4)(5,6,7))^{-1} &=& (4,3,2,1)(7,6,5) &=& (1,4,3,2)(5,7,6)\ , \\ (1,2)\circ(2,3)\circ(3,4) &=& (1,2,3,4)\ , && \end{array}$$

alles jeweils in einer geeignet großen symmetrischen Gruppe.

Definition. Eine Permutation der Form (i,j) mit $i \neq j$ heißt auch *Transposition.*

1.3.2 Das Signum

Sei $n \geqslant 1$. Wir wollen einen Gruppenmorphismus von $\mathcal{S}_n$ in die Gruppe $(\{-1,+1\},\cdot)$ definieren.

Sei $X := \{(i,j) \in [1,n] \times [1,n] \mid i \neq j\}$ das cartesische Produkt $[1,n] \times [1,n]$ ohne die Diagonale. Wir definieren eine Äquivalenzrelation auf X durch $(i,j) \sim (i',j')$ genau dann, wenn $\{i,j\} = \{i',j'\}$ (z.B. $(1,2) \sim (2,1)$). Die Äquivalenzklassen sind alle von der Form $\{(i,j),(j,i)\}$.

Sei S ein Repräsentantensystem. Für $\sigma \in \mathcal{S}_n$ ist dann auch $(\sigma \times \sigma)(S)$ ein Repräsentantensystem. In der Tat, ist $(i,j) \in X$ vorgegeben, so ist entweder $(\sigma^{-1}(i), \sigma^{-1}(j))$ oder $(\sigma^{-1}(j), \sigma^{-1}(i))$ in S, und also entweder $(i,j) = (\sigma \times \sigma)(\sigma^{-1}(i), \sigma^{-1}(j))$ oder $(j,i) = (\sigma \times \sigma)(\sigma^{-1}(j), \sigma^{-1}(i))$ in $(\sigma \times \sigma)(S)$. Jede Äquivalenzklasse $\{(i,j),(j,i)\}$ hat also genau einen Repräsentanten in $(\sigma \times \sigma)(S)$.

Die Signumsabbildung ist definiert als

$$\begin{array}{rcl} \mathcal{S}_n & \longrightarrow & \{-1,+1\} \\ \sigma & \longmapsto & \varepsilon_\sigma \ := \ \prod_{(i,j)\in S} \frac{\sigma(j)-\sigma(i)}{j-i} \ , \end{array}$$

wobei $\prod_{(i,j)\in S}$ das über S indizierte Produkt bezeichne. Da jede Äquivalenzklasse von der Form $\{(i,j),(j,i)\}$ ist, ist diese Definition unabhängig von der Wahl des Repräsentantensystems S – das Produkt bleibt bei einem Wechsel des Repräsentantensystems Faktor für Faktor dasselbe.

Wir können auch als Repräsentantensystem $S_0 = \{(i,j) \in X \mid i < j\}$ auszeichnen und

$$(*) \qquad \varepsilon_\sigma \ := \ \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

schreiben. Um in der Praxis ein Signum auszurechnen, ist es jedoch streng untersagt, diese Formel zu verwenden – siehe untenstehenden Satz 1.

Wegen

$$\begin{array}{rcl} \prod_{(i,j)\in S} \frac{\sigma(j)-\sigma(i)}{j-i} & = & \left(\prod_{(i,j)\in S} (\sigma(j) - \sigma(i))\right) \Big/ \left(\prod_{(i,j)\in S} (j-i)\right) \\ & = & \left(\prod_{(i',j')\in(\sigma\times\sigma)(S)} (j'-i')\right) \Big/ \left(\prod_{(i,j)\in S} (j-i)\right) \\ & = & \pm \left(\prod_{(i,j)\in S} (j-i)\right) \Big/ \left(\prod_{(i,j)\in S} (j-i)\right) \\ & = & \pm 1 \end{array}$$

ist in der Tat $\varepsilon_\sigma \in \{-1,+1\}$.

Die Signumsabbildung $\sigma \longmapsto \varepsilon_\sigma$ ist nun wegen

$$\begin{aligned}
\varepsilon_{\sigma\circ\rho} &= \prod_{(i,j)\in S} \frac{\sigma(\rho(j))-\sigma(\rho(i))}{j-i} \\
&= \left(\prod_{(i,j)\in S} \frac{\sigma(\rho(j))-\sigma(\rho(i))}{\rho(j)-\rho(i)}\right)\cdot\left(\prod_{(i,j)\in S}\frac{\rho(j)-\rho(i)}{j-i}\right) \\
&= \left(\prod_{(i',j')\in(\rho\times\rho)(S)} \frac{\sigma(j')-\sigma(i')}{j'-i'}\right)\cdot\left(\prod_{(i,j)\in S}\frac{\rho(j)-\rho(i)}{j-i}\right) \\
&= \varepsilon_\sigma\cdot\varepsilon_\rho
\end{aligned}$$

für $\sigma,\rho\in\mathcal{S}_n$ ein Gruppenmorphismus von $(\mathcal{S}_n,\circ)$ nach $(\{-1,+1\},\cdot)$.

Satz 1 *Sei eine Permutation*

$$\sigma = (\sigma^0(s_1),\sigma^1(s_1),\ldots,\sigma^{i_1-1}(s_1))\cdots(\sigma^0(s_k),\sigma^1(s_k),\ldots,\sigma^{i_k-1}(s_k)) \;\in\; \mathcal{S}_n$$

gegeben. Es ist

$$\varepsilon_\sigma \;=\; (-1)^{\sum_{j\in[1,k]}(i_j-1)}\ .$$

Beachte, daß auch hierfür Zykel der Länge 1 *unterschlagen werden können.*

Beweis. Da die Signumsabbildung ein Gruppenmorphismus ist, dürfen wir annehmen, daß σ selbst ein Zykel ist, also von der Form $\sigma = (a_1,a_2,\ldots,a_l)$, und haben $\varepsilon_\sigma = (-1)^{l-1}$ zu zeigen. Denn sobald dies gezeigt sein wird, können wir das Signum des Produkts der Zykel als das Produkt der Signen der Zykel bilden, und erhalten gerade die gewünschte Summe im Exponenten auf der rechten Seite.

Schreiben wir

$$(a_1,a_2,\ldots,a_l) \;=\; (a_1,a_2)\circ(a_2,a_3)\circ\cdots\circ(a_{l-1},a_l)$$

als Produkt von $l-1$ Transpositionen, so sehen wir wieder mit der Eigenschaft des Gruppenmorphismus, daß wir uns darauf beschränken können, nachzuweisen, daß das Signum einer Transposition (a,b) gleich -1 ist. Denn aus $\varepsilon_{(a_i,a_{i+1})} = -1$ wird $\varepsilon_{(a_1,\ldots,a_l)} = (-1)^{l-1}$ folgen.

Wir dürfen $a<b$ annehmen. Ist $a+1<b$, so wird

$$(a,b) \;=\; (a+1,b)\circ(a,a+1)\circ(a+1,b)\ .$$

Unter abermaliger Verwendung der Eigenschaft des Gruppenmorphismus sind wir also darauf reduziert, $\varepsilon_{(a,a+1)} = -1$ für $a\in[1,n-1]$ zu zeigen. Denn aus $\varepsilon_{(a,a+1)} = -1$ wird $\varepsilon_{(a,b)} = \varepsilon_{(a+1,b)}\varepsilon_{(a,a+1)}\varepsilon_{(a+1,b)} = -1\cdot\varepsilon^2_{(a+1,b)} = -1$ folgen.

Es gibt nun aber im definierenden Produktausdruck $(*)$ für $\varepsilon_{(a,a+1)}$ genau einen negativen Faktor, nämlich $\frac{a-(a+1)}{(a+1)-a}$. Also ist $\varepsilon_{(a,a+1)}$ negativ, d.h. $\varepsilon_{(a,a+1)} = -1$. $\square$

Beispiel. Wir wollen das Signum der Permutation $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\1&3&7&6&2&4&5\end{smallmatrix}\right)$ bestimmen. Dazu bemerken wir zunächst, daß $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\1&3&7&6&2&4&5\end{smallmatrix}\right) = (2,3,7,5)(4,6)$ ist, und erhalten mit Satz 1, daß $\varepsilon_\sigma = (-1)^{(4-1)+(2-1)} = +1$.

1.4 Ringe und Körper

1.4.1 Begriffe

Sei R eine Menge, zusammen mit Abbildungen

$$\begin{array}{rcccccccc} (+) & : & R \times R & \longrightarrow & R & : & (x,y) & \longmapsto & x+y \\ (\cdot) & : & R \times R & \longrightarrow & R & : & (x,y) & \longmapsto & x \cdot y\ . \end{array}$$

Betrachte folgende Bedingungen.

(R 1) $(R, +)$ ist eine abelsche Gruppe (mit neutralem Element 0).

(R 2) $(R, \cdot)$ ist ein Monoid (mit neutralem Element 1).

(R 2a) $(R, \cdot)$ ist ein abelsches Monoid (mit neutralem Element 1).

(R 3) Für alle $x, y, x', y' \in R$ ist $(x+y)\cdot(x'+y') = x\cdot x' + x\cdot y' + y\cdot x' + y\cdot y'$ (Distributivität).

(R 4) $(R \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

Hierbei, wie auch bei allem folgenden, gelte die "Punkt-vor-Strich"-Regel, die besagt, daß bei fehlenden Klammern zuerst die Multiplikation ausgewertet wird. Ferner bezeichne für $x \in R$ und $n \geqslant 1$ die Potenz x^n das n-fache Produkt $x \cdot x \cdots x$. Dazuhin sei stets $x^0 = 1$.

$(R, +, \cdot)$ (oder kurz auch nur R) heißt ein *Ring*, falls (R 1, 2, 3) gelten. In einem Ring wird gerne auch die Notation des Multiplikationszeichens unterschlagen, d.h. $ab = a \cdot b$.

R heißt ein *kommutativer Ring*, falls (R 1, 2a, 3) gelten.

R heißt ein *Körper*, falls (R 1, 2a, 3, 4) gelten. In einem Körper hat also jedes Element, ausgenommen die 0, ein multiplikativ Inverses. Ferner folgt aus $x \cdot y = 0$, daß $x = 0$ oder $y = 0$ – sonst wäre die Multiplikation keine Operation auf $R \setminus \{0\}$, im Widerspruch zu (R 4).

In einem Ring R gilt $0 \cdot x = (1-1)\cdot x = 1 \cdot x - 1 \cdot x = 0$, und genauso $x \cdot 0 = 0$. Ferner ist für alle $x, y \in R$ auch $x \cdot (-y) = x \cdot (-y) + x \cdot y - x \cdot y = x \cdot (-y + y) - x \cdot y = -(x \cdot y)$, und genauso $(-x) \cdot y = -(x \cdot y)$.

Beispiele. $(\mathbf{Z}, +, \cdot)$ ist ein kommutativer Ring. $(\mathbf{Q}, +, \cdot)$ und $(\mathbf{R}, +, \cdot)$ sind Körper. $(\mathbf{N}, +, \cdot)$ ist *kein* Ring, da $(\mathbf{N}, +)$ keine Gruppe bildet.

Lemma. *Sei R ein kommutativer Ring. Es ist R ein Körper genau dann, wenn $0 \neq 1$ und wenn für jedes $x \in R \setminus \{0\}$ ein $y \in R$ so existiert, daß $xy = 1$.*

Beweis. Ist R ein Körper, so ist $0 \neq 1$, da $1 \in R \setminus \{0\}$. Das multiplikativ Inverse existiert in $R \setminus \{0\}$ nach (R 4).

Seien umgekehrt $0 \neq 1$ und das multiplikativ Inverse in $R \setminus \{0\}$ stets existent. Wir haben zu zeigen, daß $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist. Dazu muß die Operation $(\cdot)$ auf

$(R \smallsetminus \{0\}) \times (R \smallsetminus \{0\})$ zunächst Werte in $R \smallsetminus \{0\}$ liefern. Seien also $x, y \in R \smallsetminus \{0\}$ vorgegeben. Wäre $xy = 0$, so wäre mit dem Inversen $z \in R$ zu y auch $x = xyz = 0 \cdot z = 0$, was nicht der Fall ist. Also ist $xy \neq 0$. Die abelschen Gruppenaxiome für $R \smallsetminus \{0\}$ folgen nun, und zwar (G 1, 2, 4) mit (R 2a), und (G 3) nach Voraussetzung. ▫

1.4.2 Ideale

Definition. Ein nichtleere Teilmenge I eines Ringes R heißt *Ideal,* falls für alle $a, a' \in I$ und alle $r \in R$ sowohl $a - a'$, als auch ra, als auch ar wieder in I liegen.

Symbolisch geschrieben, $I \subseteq R$ ist Ideal, falls $I - I \subseteq I$, $RI \subseteq I$ und $IR \subseteq I$. Beachte, daß $I \neq \emptyset$ zusammen mit $I - I \subseteq I$ gerade besagt, daß I eine Untergruppe von R bezüglich $(+)$ ist. Ist R kommutativ, so sind die Aussagen $RI \subseteq I$ und $IR \subseteq I$ äquivalent.

Beispiel. Ist $m \in \mathbf{Z}$ eine ganze Zahl, so ist $m\mathbf{Z} := \{mz \mid z \in \mathbf{Z}\}$ ein Ideal in $\mathbf{Z}$. In der Tat sind für $a = mz, a' = mz' \in m\mathbf{Z}$ und $r \in \mathbf{Z}$ auch $a - a' = m(z - z') \in m\mathbf{Z}$ und $ra = m(rz) \in m\mathbf{Z}$.

Restklassenring. *Sei I ein Ideal in einem Ring R. Wir definieren eine Äquivalenzrelation auf R durch $x \equiv_I y$ (gesprochen x kongruent zu y modulo I) genau dann, wenn $x - y \in I$, und schreiben $R/I := R/\equiv_I$. Die Äquivalenzklassen heißen auch* Restklassen. *Vermöge der Abbildungen*

$$\begin{array}{ccccc} R/I & \times & R/I & \xrightarrow{(+)} & R/I \\ (\bar{x} & , & \bar{y}) & \longmapsto & \overline{x+y} \\ R/I & \times & R/I & \xrightarrow{(\cdot)} & R/I \\ (\bar{x} & , & \bar{y}) & \longmapsto & \overline{x \cdot y} \end{array}$$

wird $(R/I, +, \cdot)$ zu einem Ring, dem Restklassenring R/I *(gesprochen* R modulo I, *oder* R nach I*). Die Restklasse von $0 \in R$ modulo I ist die Null von R/I, die Restklasse von $1 \in R$ modulo I ist die Eins in R/I. Ist R kommutativ, so auch R/I.*

Beweis. Zunächst ist zu zeigen, daß es sich um eine Äquivalenzrelation handelt. (A 1) gilt, da $x \equiv_I x$ gerade $0 = x - x \in I$ bedeutet. Für (A 2) seien uns $x, y \in R$ mit $x \equiv_I y$ gegeben. Dann ist wegen $y - x = (-1)(x - y) \in RI \subseteq I$ auch $y \equiv_I x$. Für (A 3) seien uns $x, y, z \in R$ mit $x \equiv_I y$ und $y \equiv_I z$ gegeben. Dann ist wegen $x - z = (x - y) + (y - z) \in I + I \subseteq I$ auch $x \equiv_I z$.

Die Operationen $(+)$ und $(\cdot)$ auf R/I sollen Paare von Restklassen $(\bar{x}, \bar{y})$ abbilden. Zur Definition des Bildes $\overline{x + y}$ resp. $\overline{x \cdot y}$ wurden aber Repräsentanten x, y verwandt, für die man im Rahmen der Äquivalenzklassen noch eine Wahlfreiheit hat. Damit die Definition einen Sinn ergibt – man sagt auch, damit die Abbildung *wohldefiniert* ist –, muß die Unabhängigkeit des jeweiligen Bildes von der Repräsentantenwahl überprüft werden.

Betrachten wir die Abbildung $(+)$. Zu zeigen ist, daß aus $x \equiv_I x'$ und $y \equiv_I y'$ folgt, daß $\overline{x + y} = \overline{x' + y'}$, d.h. daß $x + y \equiv_I x' + y'$. Nun ist aber $(x + y) - (x' + y') = (x - x') + (y - y') \in I$.

Betrachten wir die Abbildung $(\cdot)$. Zu zeigen ist, daß aus $x \equiv_I x'$ und $y \equiv_I y'$ folgt, daß $xy \equiv_I x'y'$. In der Tat ist

$$xy - x'y' \;=\; x(y-y') + (x-x')y' \;\in\; RI + IR \;\subseteq\; I\;.$$

Nun sind die Ringaxiome (R 1, 2, 3) und ggf. (R 2a) für $(R/I, +, \cdot)$ zu zeigen. Diese folgen aber ohne Schwierigkeiten aus den Axiomen für $(R, +, \cdot)$. Zum Beispiel gilt die Distributivität (R 3) wegen

$$\begin{array}{rcl}(\bar{x}+\bar{y})\cdot(\bar{x}'+\bar{y}') & = & (\overline{x+y})\cdot(\overline{x'+y'}) \\ & = & \overline{(x+y)\cdot(x'+y')} \\ & = & \overline{xx'+xy'+yx'+yy'} \\ & = & \overline{xx'}+\overline{xy'}+\overline{yx'}+\overline{yy'} \\ & = & \bar{x}\bar{x}'+\bar{x}\bar{y}'+\bar{y}\bar{x}'+\bar{y}\bar{y}' \end{array}$$

für $\bar{x}, \bar{x}', \bar{y}, \bar{y}' \in R/I$. ▫

Repräsentantenweise Notation. Alternativ kann man sich auf die Elemente von R/I auch durch Angabe eines jeweiligen Repräsentanten beziehen. In anderen Worten, man unterschlägt die Querstriche. Um dann Verwechslungen auszuschließen, kann man die Gleichheit in R/I als $\equiv_I$ schreiben. Kurz: $\bar{x} = \bar{y}$ und $x \equiv_I y$ sind gleichbedeutende Schreibweisen für Elemente von R/I. Etwas unsauber, aber durchaus gebräuchlich ist es, auch “in R/I gilt $x = y$ ” für $x \equiv_I y$ zu schreiben, und die Querstriche zu unterschlagen.

Beispiel. Sei $m \geqslant 0$ eine ganze Zahl, sei $I = m\mathbf{Z}$. Hier schreibt man auch $\equiv_m$ für $\equiv_{m\mathbf{Z}}$.

Es ist $\mathbf{Z}/0\mathbf{Z}$ nichts anderes als $\mathbf{Z}$, da $\equiv_0$ nichts anderes als $=$ bedeutet.

Es ist $\mathbf{Z}/1\mathbf{Z} = \{0\}$ der Nullring, in welchem $1 = 0$, und auch dies ist nicht sonderlich interessant.

Für $m \geqslant 2$ ist

$$\boxed{\mathbf{Z}/m\mathbf{Z} \;=\; \{0, 1, 2, \ldots, m-1\}\;,}$$

da sich jedes Element $z \in \mathbf{Z}$ eindeutig schreiben läßt als $z = c + dm$ mit $c \in [0, m-1]$ und $d \in \mathbf{Z}$ (verwende Division mit Rest – daher übrigens auch der Name *Rest*klasse).

In $\mathbf{Z}/4\mathbf{Z}$ gilt $2 \cdot 2 \equiv_4 0$, obwohl $2 \not\equiv_4 0$. Der kommutative Ring $\mathbf{Z}/4\mathbf{Z}$ ist kein Körper, denn hätte 2 ein multiplikativ Inverses x, dann wäre $0 \equiv_4 x \cdot 0 \equiv_4 x \cdot 2 \cdot 2 \equiv_4 2$, und das ist nicht der Fall.

Definition. Ist $m = p$ eine Primzahl, so schreiben wir auch

$$\mathbf{F}_p \;:=\; \mathbf{Z}/p\mathbf{Z}\;.$$

Der kommutative Ring $\mathbf{F}_p$ ist ein Beispiel für einen endlichen Körper, wie wir weiter unten sehen werden ($\mathbf{F}_p$ wegen engl. **f**ield).

1.4.3 Ideale in $\mathbf{Z}$

Lemma. *Jedes Ideal ungleich* $\{0\}$ *in* $\mathbf{Z}$ *ist von der Form*

$$m\mathbf{Z} \;=\; \{mz \mid z \in \mathbf{Z}\}$$

für ein positives $m \in \mathbf{Z}$.

Vorsicht. Es ist z.B. $2 < 6$, aber $2\mathbf{Z} \supsetneq 6\mathbf{Z}$.

Beweis des Lemmas. Ein Ideal $I \neq \{0\}$ in $\mathbf{Z}$ enthält ein positives Element, da mit $x \in I$ stets auch $-x \in I$ gilt. Sei m das minimale positive Element von I. Für alle $z \in \mathbf{Z}$ ist dann auch $mz \in I$, also insgesamt $m\mathbf{Z} \subseteq I$. Wir wollen die Gleichheit zeigen. Sei uns ein $x \in I$ vorgegeben. Division mit Rest gibt $x = c + dm$ mit $c \in [0, m-1]$ und $d \in \mathbf{Z}$. Es ist $c = x - dm$ in I. Wegen der Minimalität von m kann c nicht in $[1, m-1]$ liegen. Also ist $c = 0$ und $x = dm \in m\mathbf{Z}$.

Satz 2 (a) *Ist* p *eine Primzahl, so ist* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ *ein Körper. Genauer, für* $m \geqslant 2$ *ist* $\mathbf{Z}/m\mathbf{Z}$ *ein Körper genau dann, wenn* m *eine Primzahl ist.*

Beweis. Ist $m \geqslant 2$ keine Primzahl, so haben wir zu zeigen, daß $\mathbf{Z}/m\mathbf{Z}$ kein Körper ist. Dazu zerlegen wir $m = n \cdot n'$ mit $m > n, n' > 1$. Es sind $n, n' \not\equiv_m 0$, obgleich $n \cdot n' \equiv_m 0$. Damit enthält $\mathbf{Z}/m\mathbf{Z}$ zwei nichtverschwindende Elemente, deren Produkt verschwindet. Dies wäre in einem Körper nicht möglich.

Ist $m =: p$ eine Primzahl, so haben wir zu zeigen, daß $\mathbf{Z}/p\mathbf{Z}$ ein Körper ist. In anderen Worten, wir müssen zu $n \not\equiv_p 0$ ein $s \in \mathbf{Z}$ so finden, daß $ns \equiv_p 1$. Dazu betrachten wir das Ideal

$$I \;:=\; \{ns + pt \mid s, t \in \mathbf{Z}\} \;\subseteq\; \mathbf{Z}\,.$$

Nach obigem Lemma gibt es ein positives $u \in \mathbf{Z}$ mit $I = u\mathbf{Z}$. Insbesondere ist $p = n \cdot 0 + p \cdot 1 \in I = u\mathbf{Z}$, d.h. es gibt ein $v \in \mathbf{Z}$ mit $p = uv$. Wäre $u = p$, so wäre $n \in I = u\mathbf{Z} = p\mathbf{Z}$, und folglich $n \equiv_p 0$, was nicht der Fall ist. Also können wir mit p prim auf $u = 1$ schließen. Insbesondere ist $1 \in u\mathbf{Z} = I$, so daß wir $1 = ns + pt$ schreiben können. Hieraus ersehen wir $1 \equiv_p ns$. □

Lemma. *Sei* K *ein endlicher Körper, und sei* $q := \#K$ *die Anzahl seiner Elemente. Dann ist für alle* $x \in K$ *die Gleichung*

$$x^q \;=\; x$$

erfüllt. Insbesondere gilt für p *prim und* $x \in \mathbf{F}_p$ *stets, daß* $x^p = x$ *ist. In anderen Worten, für alle* $x \in \mathbf{Z}$ *teilt* p *die Differenz* $x^p - x$ *(Kleiner Fermatscher Satz).*

Beweis. Ist $x = 0$, so ist $0^q = 0$. Ist $x \in K \smallsetminus \{0\}$, so hat x als Element der endlichen abelschen Gruppe $(K \smallsetminus \{0\}, \cdot)$, welche $q - 1$ Elemente enthält, eine Ordnung, die $q - 1$ teilt. Folglich ist $x^{q-1} = 1$, und somit auch $x^q = x$. □

1.4.4 Polynomringe

Sei im folgenden K ein Körper.

Definition. Sei X eine formale Variable. Ein *Polynom* $f = f(X)$ mit *Koeffizienten* $a_i \in K$ ist ein Ausdruck der Form

$$f(X) \;=\; \sum_{i\geqslant 0} a_i X^i \;=\; a_m X^m + a_{m-1}X^{m-1} + \cdots + a_2 X^2 + a_1 X^1 + a_0 X^0 \;,$$

wobei $a_i \in K$ für $i \geqslant 0$, und wobei $a_i = 0$ für $i > m$ für ein $m \geqslant 0$ (welches vom Polynom abhängt). Ein Polynom hat also nur endlich viele nichtverschwindende Koeffizienten. Zwei Polynome sind genau dann gleich, wenn alle ihre Koeffizienten übereinstimmen ([2]).

Die Menge der Polynome mit Koeffizienten in K wird $K[X]$ geschrieben. Wir schreiben auch $X^1 = X$ und $X^0 = 1$. Insbesondere werde via *konstanter* Polynome $a_0 = a_0 X^0$ der Koeffizientenkörper K als Teilmenge $K \subseteq K[X]$ aufgefaßt.

Trotz der Schreibweise als $f(X)$ ist ein Polynom *keine Abbildung.* Siehe Bemerkung am Ende des Abschnitts.

Auf $K[X]$ seien folgende Verknüpfungen erklärt.

$$\begin{array}{rcccl} K[X] & \times & K[X] & \xrightarrow{(+)} & K[X] \\ (\sum_{i\geqslant 0} a_i X^i & , & \sum_{i\geqslant 0} b_i X^i) & \longmapsto & \sum_{i\geqslant 0}(a_i + b_i)X^i \\ & & & & \\ K[X] & \times & K[X] & \xrightarrow{(\cdot)} & K[X] \\ (\sum_{i\geqslant 0} a_i X^i & , & \sum_{i\geqslant 0} b_i X^i) & \longmapsto & \sum_{k\geqslant 0}\left(\displaystyle\sum_{i\geqslant 0,\; j\geqslant 0,\; i+j=k} a_i b_j\right) X^k \end{array}$$

Beachte, daß das Resultat der jeweiligen Operation in der Tat nur endlich viele nichtverschwindende Koeffizienten hat.

Lemma. $(K[X], +, \cdot)$ *ist ein kommutativer Ring.*

Beweis. $(K[X], +)$ ist eine abelsche Gruppe mit dem Nullpolynom $0 = 0 \cdot X^0$ als neutralem Element, da die Addition koeffizientenweise definiert ist, und da $(K, +)$ eine abelsche Gruppe ist.

[2] Strenggenommen ist ein Polynom also definiert als das Tupel seiner Koeffizienten. Die Summenschreibweise unter Zuhilfenahme einer formalen Variablen X soll lediglich die Rechenregeln suggerieren, die wir gleich einführen werden.

Wir wollen zeigen, daß $(K[X],\cdot)$ ein abelsches Monoid ist. Die Assoziativität folgt aus

$$\begin{aligned}\left(\left(\sum_{i\geqslant 0} a_i X^i\right)\left(\sum_{j\geqslant 0} b_j X^j\right)\right)\left(\sum_{k\geqslant 0} c_k X^k\right) &= \left(\sum_{l\geqslant 0}\left(\sum_{i+j=l} a_i b_j\right) X^l\right)\left(\sum_{k\geqslant 0} c_k X^k\right)\\ &= \sum_{m\geqslant 0}\left(\sum_{i+j=l,\, l+k=m} a_i b_j c_k\right) X^m\\ &= \sum_{m\geqslant 0}\left(\sum_{i+j+k=m} a_i b_j c_k\right) X^m\\ &= \sum_{m\geqslant 0}\left(\sum_{j+k=l,\, i+l=m} a_i b_j c_k\right) X^m\\ &= \left(\sum_{i\geqslant 0} a_i X^i\right)\left(\sum_{l\geqslant 0}\left(\sum_{j+k=l} b_j c_k\right) X^l\right)\\ &= \left(\sum_{i\geqslant 0} a_i X^i\right)\left(\left(\sum_{j\geqslant 0} b_j X^j\right)\left(\sum_{k\geqslant 0} c_k X^k\right)\right)\ .\end{aligned}$$

Das Einselement ist durch $1 = 1\cdot X^0$ gegeben, und die Kommutativität resultiert aus der Kommutativität von $(K,\cdot)$.

Die Distributivität folgt mit einer ähnlichen Rechnung. Beachte, daß das Multiplikationsgesetz nicht anderes ist als die "distributive Fortsetzung" des Potenzgesetzes $X^i\cdot X^j = X^{i+j}$. $\square$

Allerdings ist $K[X]$ kein Körper, da das Element X kein multiplikativ Inverses besitzt.

Definition. Der *Grad* eines Polynoms $f(X) = \sum_{i\geqslant 0} a_i X^i \in K[X]\smallsetminus\{0\}$ ist definiert als

$$\deg(f) \;=\; \max\{i\geqslant 0 \mid a_i \neq 0\}\ .$$

Wir treffen die Vereinbarung, daß wann immer wir $\deg(f)$ anschreiben, stillschweigend $f\neq 0$ vorausgesetzt ist.

Es ist $\deg(fg) = \deg(f)+\deg(g)$, da

$$(a_m X^m + (\text{kleinere Potenzen}))(b_n X^n + (\text{kleinere Potenzen})) \;=\; a_m b_n X^{m+n} + (\text{kleinere Potenzen})\ ,$$

und da $a_m b_n \neq 0$ falls $a_m\neq 0$ und $b_n\neq 0$.

Definition. Ist $f(X) = \sum_{i\geqslant 0} a_i X^i \in K[X]$ ein Polynom, und ist $m = \deg(f)$, so heißt a_m der *Leitkoeffizient* von f. Ein Polynom mit Leitkoeffizient 1 heißt *normiert.*

Definition. Zu einem Polynom $f(X) = \sum_{i\geqslant 0} a_i X^i \in K[X]$ gehört eine *polynomiale Abbildung* $f : K \longrightarrow K : x \longmapsto f(x) := \sum_{i\in[0,m]} a_i x^i$. Hierfür wird mißbräuchlich die Bezeichnung f weiter verwandt.

Vorsicht. Es ist möglich, daß $f(x) = 0$ für alle $x\in K$, obwohl $f(X)\neq 0$. Sei etwa $K = \mathbf{F}_3$, und sei $f(X) = X^3 - X = X(X-1)(X-2)\neq 0$. Offenbar ist $f(0) = f(1) = f(2) = 0$. Die Abbildung, die einem Polynom seine polynomiale Abbildung zuweist, ist also nicht injektiv.

1.4.5 Ideale in $K[X]$

Was die Ideale anbelangt, verhält sich $K[X]$ wie $\mathbf{Z}$, wobei der Grad die Rolle des Absolutbetrags übernimmt.

Für $f(X) \in K[X]$ schreiben wir

$$f(X)K[X] \; := \; \{f(X)g(X) \mid g(X) \in K[X]\} \; \subseteq K[X] \, ;$$

dies stellt ein Ideal dar. Wir schreiben kurz auch $(\equiv_f)$ für $(\equiv_{f(X)K[X]})$.

Lemma. *Jedes Ideal ungleich* $\{0\}$ *in* $K[X]$ *ist von der Form* $f(X)K[X]$ *für ein normiertes Polynom* $f(X) \in K[X]$.

Beweis. Sei $I \neq \{0\}$ ein Ideal in $K[X]$. Sei $f(X)$ ein Polynom kleinsten Grades in $I \smallsetminus \{0\}$. Wir dürfen $f(X)$ als normiert annehmen, da Multiplikation mit konstanten Polynomen innerhalb I möglich ist. Es ist $f(X)K[X] \subseteq I$, und wir wollen die Gleichheit zeigen. Sei uns ein $h(X) \in I$ vorgegeben. Polynomdivision gibt $h(X) = f(X)s(X) + r(X)$, mit $s(X) \in K[X]$ und mit entweder $\deg(r) \in [0, \deg(f) - 1]$ oder aber $r = 0$. Es ist $r = h - fs \in I$. Wegen der Minimalität von $\deg(f)$ kann r nicht ungleich Null sein. Also ist $r = 0$ und $h = fs \in f(X)K[X]$. □

Definition. Ein Polynom $q(X) \in K[X] \smallsetminus \{0\}$ mit $\deg(q) \geqslant 1$ heißt *irreduzibel,* falls es normiert ist, und falls eine Zerlegung $q(X) = f(X)g(X)$ mit $f(X), g(X) \in K[X]$ nur mit $\deg(f) = 0$ oder $\deg(g) = 0$ möglich ist.

Beispiel. Ein Polynom der Form $X^2 - a$ mit $a \in K$ ist irreduzibel genau dann, wenn es kein $x \in K$ gibt mit $x^2 = a$. In der Tat, in einer Zerlegung $(X^2 - a) = (X - b)(X - c)$ ist notwendig $b = -c$, und folglich $b^2 = a$.

Allgemeiner, ein Polynom der Form $X^2 + aX + b$ mit $a, b \in K$ ist irreduzibel genau dann, wenn es kein $x \in K$ gibt mit $x^2 + ax + b = 0$. Denn nicht irreduzibel zu sein, heißt hier, in zwei Faktoren von Grad 1 zu zerfallen. Einen Faktor von Grad 1 zu haben, heißt aber gerade, eine Nullstelle zu besitzen.

Genauso für ein Polynom der Form $X^3 + aX^2 + bX + c$ mit $a, b, c \in K$ – es ist irreduzibel genau dann, wenn es kein $x \in K$ gibt mit $x^3 + ax^2 + bx + c = 0$. Denn nicht irreduzibel zu sein, heißt hier, in einen Faktor von Grad 1 und einen Faktor von Grad 2 zu zerfallen (wobei letzterer nicht irreduzibel sein muß).

Vorsicht, es ist $X^4 + 2X^2 + 1 = (X^2 + 1)^2 \in \mathbf{R}[X]$ nicht irreduzibel, obwohl es keine Nullstelle in $\mathbf{R}$ besitzt.

Satz 2 (b) *Ist* $q(X)$ *mit* $\deg(q) \geqslant 2$ *ein irreduzibles Polynom, so ist* $K[X]/q(X)K[X]$ *ein Körper. Genauer, für* $f(X) \in K[X]$ *normiert mit* $\deg(f) \geqslant 1$ *ist* $K[X]/f(X)K[X]$ *ein Körper genau dann, wenn* $f(X)$ *irreduzibel ist.*

Beweis. Ist $f(X)$ nicht irreduzibel, so haben wir zu zeigen, daß $K[X]/f(X)K[X]$ kein Körper ist. Dazu zerlegen wir $f(X) = g(X) \cdot \tilde{g}(X)$ mit $\deg(f) > \deg(g), \deg(\tilde{g}) > 0$. Es sind $g(X), \tilde{g}(X) \not\equiv_f 0$, obgleich $g(X) \cdot \tilde{g}(X) \equiv_f 0$. Dies wäre in einem Körper nicht möglich.

Ist $f(X) =: q(X)$ irreduzibel, so haben wir zu zeigen, daß $K[X]/q(X)K[X]$ ein Körper ist. In anderen Worten, wir müssen zu einem Polynom $g(X) \not\equiv_q 0$ ein Polynom $s(X) \in K[X]$ so finden, daß $g(X)s(X) \equiv_q 1$. Dazu betrachten wir das Ideal

$$I \;:=\; \{g(X)s(X) + q(X)t(X) \mid s(X), t(X) \in K[X]\} \;\subseteq\; K[X] \; .$$

Nach obigem Lemma gibt es ein normiertes Polynom $u(X) \in K[X]$ mit $I = u(X)K[X]$. Insbesondere ist $q(X) = g(X)\cdot 0 + q(X)\cdot 1 \in I = u(X)K[X]$, d.h. es gibt ein $v(X) \in K[X]$ mit $q(X) = u(X)v(X)$. Wäre $\deg(u) = \deg(q)$, so wäre $\deg(v) = 0$. Da q und u normiert sind, müßte also $v = 1$ und $q = u$ sein. Da dann aber auch $g(X) \in I = u(X)K[X] = q(X)K[X]$ wäre, wäre $g(X) \equiv_q 0$, was nicht der Fall ist. Also können wir mit q irreduzibel auf $\deg(u) = 0$ und mithin auf $u = 1$ schließen. Insbesondere ist $1 \in u(X)K[X] = I$, so daß wir $1 = g(X)s(X) + q(X)t(X)$ schreiben können. Hieraus ersehen wir $1 \equiv_q g(X)s(X)$. □

Satz 2 (b) ist in noch stärkerem Maße als Satz 2 (a) eine Konstruktionsmaschine für Körper. Bevor wir uns ein paar Körper ausgeben lassen, interessiert uns aber noch, wie man die Elemente eines Quotienten der Form $K[X]/f(X)K[X]$ standardisiert schreiben kann, d.h. wie man ein gutes Repräsentantensystem für die Restklassen, aus denen $K[X]/f(X)K[X]$ ja besteht, finden kann.

Lemma. *Sei $f(X) \in K[X]$, sei $m = \deg(f) \geqslant 1$. Jedes Element $g(X)$ von $K[X]/f(X)K[X]$ läßt sich in eindeutiger Weise in der Form*

$$g(X) \;\equiv_f \sum_{i\in[0,m-1]} a_i X^i$$

schreiben, wobei $a_i \in K$. Insbesondere, ist $\#K = b < \infty$, so ist $\#(K[X]/f(X)K[X]) = b^m$.

Beweis. Wir wollen zunächst zeigen, daß sich jedes Element in dieser Form schreiben läßt. Sei also $g(X) \in K[X]$ vorgegeben. Mit Polynomdivision können wir $g(X) = f(X)s(X) + r(X)$ schreiben, mit $s(X) \in K[X]$ und mit entweder $\deg(r) \in [0, \deg(f) - 1]$ oder aber $r = 0$. Jedenfalls ist $g(X) \equiv_f r(X)$, und $r(X)$ ist ein Repräsentant der gewünschten Form.

Zeigen wir nun, daß eine solche Darstellung eindeutig ist. Seien also $r(X)$ und $\tilde{r}(X)$ gegeben mit $\deg(r) < \deg(f)$ oder $r = 0$, mit $\deg(\tilde{r}) < \deg(f)$ oder $\tilde{r} = 0$ und mit $r(X) \equiv_f \tilde{r}(X)$. Dann ist $\tilde{r}(X) = r(X) + f(X)h(X)$ für ein $h(X) \in K[X]$. Wäre $h(X) \neq 0$, so wäre $\deg(\tilde{r}) \geqslant \deg(f)$. Also ist $h(X) = 0$ und $r(X) = \tilde{r}(X)$. □

1.4.6 Konstruktion von Körpern

1.4.6.1 Die komplexen Zahlen C

Definition. Der Körper der *komplexen Zahlen* ist gegeben durch

$$\mathbf{C} \;:=\; \mathbf{R}[X]/(X^2+1)\mathbf{R}[X] \; .$$

Die Restklasse von X wird auch $i := \bar{X}$ geschrieben. Beachte, daß $X^2 + 1 = X^2 - (-1)$ in der Tat irreduzibel ist, da -1 in $\mathbf{R}$ kein Quadrat ist.

Insbesondere ist

$$\boxed{i^2 = -1}\ .$$

Jedes Element von $\mathbf{C}$ läßt sich eindeutig in der Form $a + bi$ mit $a, b \in \mathbf{R}$ schreiben.

Allgemein ist $(a + bi)(a' + b'i) = (aa' - bb') + (ab' + ba')i$ für $a, b, a', b' \in \mathbf{R}$.

1.4.6.2 Der Körper mit 4 Elementen $\mathbf{F}_4$

Definition. Der Körper $\mathbf{F}_4$ ist gegeben durch

$$\mathbf{F}_4 \ := \ \mathbf{F}_2[X]/(X^2 + X + 1)\mathbf{F}_2[X]\ .$$

Schreibe $\alpha := \bar{X}$. Beachte, daß $X^2 + X + 1$ irreduzibel ist, da es von Grad $\leqslant 3$ ist und keine Nullstelle in $\mathbf{F}_2$ hat.

Insbesondere ist

$$\boxed{\alpha^2 = 1 + \alpha}\ .$$

Jedes Element von $\mathbf{F}_4$ läßt sich eindeutig in der Form $a + b\alpha$ mit $a, b \in \mathbf{F}_2$ schreiben. Der Körper $\mathbf{F}_4$ hat also 4 Elemente, und namentlich ist als Menge

$$\mathbf{F}_4 \ = \ \{0,\ 1,\ \alpha,\ 1 + \alpha\}\ .$$

Darin gilt $(a + b\alpha)(a' + b'\alpha) = (aa' + bb') + (ab' + ba' + bb')\alpha$ für $a, b, a', b' \in \mathbf{F}_2$. In der Praxis verwendet man allerdings nicht diese Formel, sondern rechnet in polynomialen Ausdrücken in α und vereinfacht durch Einsetzen von $\alpha^2 = \alpha + 1$.

Vorsicht. Es ist $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ nach Definition, aber $\mathbf{F}_4 \neq \mathbf{Z}/4\mathbf{Z}$. Es ist $\mathbf{F}_4$ ein Körper, nicht aber $\mathbf{Z}/4\mathbf{Z}$.

1.4.6.3 Der Körper mit 8 Elementen $\mathbf{F}_8$

Definition. Der Körper $\mathbf{F}_8$ ist gegeben durch

$$\mathbf{F}_8 \ := \ \mathbf{F}_2[X]/(X^3 + X + 1)\mathbf{F}_2[X]\ .$$

Schreibe $\beta := \bar{X}$. Beachte, daß $X^3 + X + 1$ irreduzibel ist, da es von Grad $\leqslant 3$ ist und keine Nullstelle in $\mathbf{F}_2$ hat.

Insbesondere ist

$$\boxed{\beta^3 = 1 + \beta}\ .$$

Jedes Element von $\mathbf{F}_8$ läßt sich eindeutig in der Form $a + b\beta + c\beta^2$ mit $a, b, c \in \mathbf{F}_2$ schreiben. Der Körper $\mathbf{F}_8$ hat also 8 Elemente, und namentlich ist als Menge

$$\mathbf{F}_8 \ = \ \{0,\ 1,\ \beta,\ 1 + \beta,\ \beta^2,\ 1 + \beta^2,\ \beta + \beta^2,\ 1 + \beta + \beta^2\}\ .$$

Darin gilt

$$\begin{array}{l}(a+b\beta+c\beta^2)(a'+b'\beta+c'\beta^2) \;=\\ (aa'+bc'+cb')+(ab'+ba'+bc'+cb'+cc')\beta+(ac'+bb'+ca'+cc')\beta^2\end{array}$$

für $a, b, c, a', b', c' \in \mathbf{F}_2$.

1.4.6.4 Der Körper mit 9 Elementen $\mathbf{F}_9$

Definition. Der Körper $\mathbf{F}_9$ ist gegeben durch

$$\mathbf{F}_9 \;:=\; \mathbf{F}_3[X]/(X^2+1)\mathbf{F}_3[X]\ .$$

Schreibe $\iota := \bar{X}$. Beachte, daß X^2+1 irreduzibel ist, da -1 kein Quadrat in $\mathbf{F}_3$ ist.

Insbesondere ist

$$\boxed{\iota^2 = -1}\ .$$

Jedes Element von $\mathbf{F}_9$ läßt sich eindeutig in der Form $a + b\iota$ mit $a, b \in \mathbf{F}_3$ schreiben. Der Körper $\mathbf{F}_9$ hat also 9 Elemente, und namentlich ist als Menge

$$\mathbf{F}_9 \;=\; \{0,\ 1,\ -1,\ \iota,\ \iota+1,\ \iota-1,\ -\iota,\ -\iota+1,\ -\iota-1\}\ .$$

Darin gilt $(a+b\iota)(a'+b'\iota) = (aa'-bb')+(ab'+ba')\iota$ für $a, b, a', b' \in \mathbf{F}_3$.

Man könnte nun für jede Primpotenz p^k einen Körper $\mathbf{F}_{p^k}$ einführen, was wir nicht tun werden. Wie dies ausgehend von einem irreduziblen Polynom in $\mathbf{F}_p[X]$ von Grad k zu geschehen hätte, sollte aber klar geworden sein.

1.4.6.5 Zusammenstellung

Die Liste der Körper, die im folgenden verwandt werden werden, mitsamt Definitionen so erforderlich, hier noch einmal.

$\mathbf{Q}$		
$\mathbf{R}$		
$\mathbf{C}$	$\mathbf{C} := \mathbf{R}[X]/(X^2+1)\mathbf{R}[X]$	$i := \bar{X}$, $i^2 = -1$
$\mathbf{F}_p$ für p prim	$\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$	
$\mathbf{F}_4$	$\mathbf{F}_4 := \mathbf{F}_2[X]/(X^2+X+1)\mathbf{F}_2[X]$	$\alpha := \bar{X}$, $\alpha^2 = 1+\alpha$
$\mathbf{F}_8$	$\mathbf{F}_8 := \mathbf{F}_2[X]/(X^3+X+1)\mathbf{F}_2[X]$	$\beta := \bar{X}$, $\beta^3 = 1+\beta$
$\mathbf{F}_9$	$\mathbf{F}_9 := \mathbf{F}_3[X]/(X^2+1)\mathbf{F}_3[X]$	$\iota := \bar{X}$, $\iota^2 = -1$

Kapitel 2

Vektorräume

Die Lineare Algebra studiert Vektorräume über Körpern, ihre innere Beschaffenheit und ihre wechselseitigen Beziehungen.

2.1 Begriff

Sei $(K, +, \cdot)$ ein Körper. Das kleine griechische Alphabet wird zur Bezeichnung seiner Elemente herangezogen. Vollständig lautet es wie folgt.

α	alpha	η	eta	ν	nü	τ	tau
β	beta	θ	theta	ξ	xi	υ	ypsilon
γ	gamma	ι	iota	o	omikron	φ	phi
δ	delta	κ	kappa	π	pi	χ	chi
ε	epsilon	λ	lambda	ρ	rho	ψ	psi
ζ	zeta	μ	mü	σ	sigma	ω	omega

Die Buchstaben $\alpha \in \mathbf{F}_4$, $\beta \in \mathbf{F}_8$ und $\iota \in \mathbf{F}_9$ sind für vordefinierte Körperelemente reserviert. Der Buchstabe ε bezeichnet die Signumsabbildung, und ρ, σ und τ bleiben Permutationen vorbehalten. Der Buchstabe o ist der Null zu ähnlich, um verwandt zu werden.

Vektorraum. Sei V eine Menge, und seien Abbildungen $V \times V \xrightarrow{(+)} V$ (*Vektoraddition*) und $K \times V \xrightarrow{(\cdot)} V$ (*Skalarmultiplikation*) gegeben. $(V, +, \cdot)$ heißt *Vektorraum (über K),* falls $(\mathrm{V}\,1, 2, 3, 4, 5)$ gelten.

(V 1) $(V, +)$ ist eine abelsche Gruppe.

(V 2) Für alle $y \in V$ ist $1 \cdot y = y$.

(V 3) Für alle $\lambda, \mu \in K$ und alle $y \in V$ ist $\lambda \cdot (\mu \cdot y) = (\lambda \cdot \mu) \cdot y$.

(V 4) Für alle $\lambda, \mu \in K$ und alle $y \in V$ ist $(\lambda + \mu) \cdot y = \lambda \cdot y + \mu \cdot y$.

(V 5) Für alle $\lambda \in K$ und alle $y, z \in V$ ist $\lambda \cdot (y + z) = \lambda \cdot y + \lambda \cdot z$.

Elemente von V heißen auch *Vektoren.* Im Zusammenhang mit Vektorräumen über K spricht man von den Elementen von K auch als *Skalaren,* und von K als dem *Skalarkörper.* Wir bezeichnen die Null in K und die Null in V (den Nullvektor) mit demselben Symbol 0. Oft schreibt man auch $\lambda y := \lambda \cdot y$.

Für $y \in V$ ist $0 \cdot y = 0 \cdot y + 0 \cdot y - 0 \cdot y = (0+0) \cdot y - 0 \cdot y = 0 \cdot y - 0 \cdot y = 0$. Ferner ist für $\lambda \in K$ $(-\lambda) \cdot y = (-\lambda) \cdot y + \lambda \cdot y - \lambda \cdot y = (-\lambda + \lambda) \cdot y - \lambda \cdot y = -\lambda \cdot y$, speziell $(-1) \cdot y = -y$.

Für $\lambda \in K$ und den Nullvektor 0 ist $\lambda \cdot 0 = \lambda \cdot 0 + \lambda \cdot 0 - \lambda \cdot 0 = \lambda \cdot 0 - \lambda \cdot 0 = 0$. Für $y \in V$ ist $\lambda \cdot (-y) = \lambda \cdot (-y) + \lambda \cdot y - \lambda \cdot y = -\lambda \cdot y$.

Ist $\lambda y = 0$ für ein $\lambda \in K \smallsetminus \{0\}$ und ein $y \in V$, so folgt $y = \lambda^{-1}\lambda y = 0$. Es ist $\lambda y = 0$ also genau dann, wenn $\lambda = 0$ oder $y = 0$.

Beispiel. $V = \{0\}$ mit der Addition $0 + 0 = 0$ und der Skalarmultiplikation $\lambda \cdot 0 = 0$ ist ein Vektorraum über K, der *Nullvektorraum.* Wir schreiben auch $V = 0$, wenn keine Verwechslung möglich ist.

Beispiel. $V = K$, mit der Körperaddition $K \times K \xrightarrow{(+)} K$ als Addition und der Körpermultiplikation $K \times K \xrightarrow{(\cdot)} K$ als Skalarmultiplikation, ist ein Vektorraum über K, wie aus den Körperaxiomen folgt.

Standardvektorraum. Sei $n \geqslant 1$, sei $V = K^n = K \times K \times \cdots \times K$ (n cartesische Faktoren) die Menge der n-Tupel mit Einträgen in K, genannt *Standardvektorraum* über K. Wir schreiben die Elemente von K^n als *Spaltenvektoren*

$$y = \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix}, \quad z = \begin{pmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_n \end{pmatrix} \in K^n = V .$$

Wir setzen

$$\begin{array}{rcl} V \times V & \xrightarrow{(+)} & V \\ (y, z) & \longmapsto & y + z = \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix} + \begin{pmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_n \end{pmatrix} := \begin{pmatrix} \eta_1+\zeta_1 \\ \eta_2+\zeta_2 \\ \vdots \\ \eta_n+\zeta_n \end{pmatrix} \end{array}$$

und

$$\begin{array}{rcl} K \times V & \xrightarrow{(\cdot)} & V \\ (\lambda, y) & \longmapsto & \lambda \cdot y = \lambda \cdot \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix} := \begin{pmatrix} \lambda\eta_1 \\ \lambda\eta_2 \\ \vdots \\ \lambda\eta_n \end{pmatrix} . \end{array}$$

In diesem Zusammenhang setzen wir noch $K^0 := 0$.

Wie in dem vorangegangenen Beispiel $V = K = K^1$ sind nun auch hier die Vektorraumaxiome erfüllt, nur nunmehr durch *eintragsweise* Anwendung der Körperaxiome. Zum

Beispiel gilt (V 5) wegen

$$\begin{aligned}
\lambda\cdot(y+z) &= \lambda\cdot\left(\begin{pmatrix}\eta_1\\ \eta_2\\ \vdots\\ \eta_n\end{pmatrix}+\begin{pmatrix}\zeta_1\\ \zeta_2\\ \vdots\\ \zeta_n\end{pmatrix}\right)\\
&= \begin{pmatrix}\lambda\cdot(\eta_1+\zeta_1)\\ \lambda\cdot(\eta_2+\zeta_2)\\ \vdots\\ \lambda\cdot(\eta_n+\zeta_n)\end{pmatrix}\\
&\overset{(\mathrm{R}\,3)}{=} \begin{pmatrix}\lambda\cdot\eta_1+\lambda\cdot\zeta_1\\ \lambda\cdot\eta_2+\lambda\cdot\zeta_2\\ \vdots\\ \lambda\cdot\eta_n+\lambda\cdot\zeta_n\end{pmatrix}\\
&= \lambda\cdot y+\lambda\cdot z\ .
\end{aligned}$$

Beispiele. Der Vektorraum $\mathbf{R}^1$ wird als Gerade veranschaulicht, parametrisiert durch die reellen Zahlen.

Der Vektorraum $\mathbf{R}^2$ wird als mit zwei Koordinaten parametrisierte Ebene veranschaulicht. Ein Vektor $\binom{\xi_1}{\xi_2}\in\mathbf{R}^2$ wird durch einen Pfeil vom Ursprung zum Punkt mit den Koordinaten (ξ_1,ξ_2) dargestellt, die Addition zweier solcher Vektoren durch Aneinandersetzen der Pfeile, und die Multiplikation mit λ durch eine Streckung des Pfeiles um den Faktor λ.

Analog $\mathbf{R}^3$, welcher als mit 3 reellen Koordinaten parametrisierter Raum veranschaulicht wird.

Im Vektorraum $\mathbf{F}_2^2$ gibt es 4 Vektoren, als da wären $\{\binom{0}{0},\binom{1}{0},\binom{0}{1},\binom{1}{1}\}$.

Beispiel. Sei $V=K[X]$, mit der Addition aus dem Ring

$$\left(\sum_{i\geqslant 0}a_iX^i\right)+\left(\sum_{i\geqslant 0}b_iX^i\right)\ :=\ \sum_{i\geqslant 0}(a_i+b_i)X^i$$

und der Multiplikation

$$\lambda\cdot\left(\sum_{i\geqslant 0}a_iX^i\right)\ :=\ \sum_{i\geqslant 0}\lambda\cdot a_iX^i$$

für $\lambda\in K$ und $\sum_{i\geqslant 0}a_iX^i,\sum_{i\geqslant 0}b_iX^i\in K[X]$. Da die Multiplikation mit $\lambda\in K$ der Multiplikation im Ring mit dem konstanten Polynom $\lambda\in K[X]$ entspricht, folgen die Vektorraumaxiome aus den Ringaxiomen für $K[X]$.

Beispiel. Sei $f(X)\in K[X]$ ein normiertes Polynom von Grad $\geqslant 1$, und sei $V=K[X]/f(X)K[X]$. Genauso wie im vorangegangenen Beispiel wird auch hier V zu einem Vektorraum, d.h. unter Verwendung der Ringaddition, und der Ringmultiplikation mit Restklassen konstanter Polynome.

Insbesondere ist $\mathbf{C}=\mathbf{R}[X]/(X^2+1)\mathbf{R}[X]$ ein Vektorraum über $K=\mathbf{R}$. Ferner sind $\mathbf{F}_4=\mathbf{F}_2[X]/(X^2+X+1)\mathbf{F}_2[X]$ und $\mathbf{F}_8=\mathbf{F}_2[X]/(X^3+X+1)\mathbf{F}_2[X]$ Vektorräume über $\mathbf{F}_2$, und schließlich ist auch $\mathbf{F}_9=\mathbf{F}_3[X]/(X^2+1)\mathbf{F}_3[X]$ ein Vektorraum über $\mathbf{F}_3$.

2.2 Basis und Dimension

Sei V ein Vektorraum über einem Körper K.

Definition. Ist $(x_1, \ldots, x_m)$ ein Tupel von Vektoren in V, so sei seine *Länge* die Anzahl m seiner Einträge. Ein Vektor $y \in V$ heißt *Linearkombination* in $(x_1, \ldots, x_m)$, falls es $\lambda_1, \ldots, \lambda_m \in K$ gibt mit

$$y \;=\; \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m \;=\; \sum_{i \in [1,m]} \lambda_i x_i \,.$$

Die Elemente λ_i heißen die *Koeffizienten* dieser Linearkombination.

Die Menge der Linearkombinationen in $(x_1, \ldots, x_m)$ wird als *Erzeugnis* von $(x_1, \ldots, x_m)$ bezeichnet, und mit spitzen Klammern

$$\Big\langle x_1, \ldots, x_m \Big\rangle \;:=\; \left\{ \sum_{i \in [1,m]} \lambda_i x_i \;\middle|\; \lambda_i \in K \right\}$$

geschrieben. Ist $\langle x_1, \ldots, x_m \rangle = V$, so heißt $(x_1, \ldots, x_m)$ ein *erzeugendes* Tupel in V. Man sagt auch, $(x_1, \ldots, x_m)$ *erzeugt* V.

Das Tupel $(x_1, \ldots, x_m)$ von Vektoren in V heißt *linear abhängig,* falls es eine Linearkombination

$$0 \;=\; \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m$$

der Null gibt, in welcher nicht alle λ_i verschwinden, d.h. für welche es ein $j \in [1, m]$ mit $\lambda_j \neq 0$ gibt.

Umgekehrt, das Tupel $(x_1, \ldots, x_m)$ von Vektoren in V heißt *linear unabhängig,* falls

$$0 \;=\; \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m$$

nur für $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$ möglich ist.

Das leere Tupel ( ) sei ebenfalls linear unabhängig.

Beispiel. Ein Tupel (x_1) in V der Länge 1 ist linear abhängig genau dann, wenn $x_1 = 0$ ist. In der Tat folgt aus $\lambda x_1 = 0$ falls $x_1 \neq 0$, daß $\lambda = 0$. Auf der anderen Seite ist der Nullvektor 0 wegen $1 \cdot 0 = 0$ linear abhängig.

Allgemeiner ist ein Tupel von Vektoren, das den Nullvektor enthält, linear abhängig, da man den Nullvektor als Linearkombination dieser Vektoren darstellen kann mit einem einzigen nichtverschwindenden Koeffizienten beim Nullvektor.

Ähnlich sieht man, daß ein Tupel von Vektoren mit zwei gleichen Einträgen an verschiedenen Stellen linear abhängig ist.

Beispiel. Sei $K = \mathbf{R}$, sei $V = \mathbf{R}^3$, und seien

$$x_1 \;=\; \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} , \qquad x_2 \;=\; \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} , \qquad x_3 \;=\; \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} .$$

Wegen

$$-2x_1 + x_2 + x_3 \;=\; 0$$

ist (x_1, x_2, x_3) linear abhängig.

Betrachten wir nun x_1 und x_2. Mit $\lambda_1, \lambda_2 \in K$ wird

$$\lambda_1 x_1 + \lambda_2 x_2 \;=\; \left(\begin{smallmatrix} \lambda_1 + 2\lambda_2 \\ -\lambda_2 \\ \lambda_2 \end{smallmatrix}\right) .$$

Diese Linearkombination verschwindet nur dann, wenn $\lambda_2 = 0$, wie man dem zweiten oder dritten Eintrag ansieht. Dies wiederum impliziert $\lambda_1 = 0$, wie man dem ersten Eintrag ansieht. Der Nullvektor ist also nicht aus x_1, x_2 linear kombinierbar, ohne daß die Koeffizienten alle verschwinden. Mit anderen Worten, (x_1, x_2) ist linear unabhängig.

Dimension. Gibt es in V ein linear unabhängiges Tupel der Länge n, ist aber jedes Tupel der Länge $n+1$ linear abhängig, so nennen wir n die *Dimension* von V, geschrieben

$$n \;=\; \dim_K V \;=\; \dim V \;;$$

letzteres, falls der Skalarkörper K aus dem Kontext hervorgeht. Kurz: die Dimension ist dann die maximale Länge, die ein linear unabhängiges Tupel in V haben kann.

Ein Vektorraum hat also eine Dimension genau dann, wenn die Länge linear unabhängiger Tupel in V nach oben beschränkt ist. Diesenfalls heißt V *endlichdimensional,* und ansonsten *unendlichdimensional.*

Beispiel. $V = K[X]$ ist unendlichdimensional, da $(X^0, X^1, \ldots, X^m)$ linear unabhängig ist für jedes $m \geqslant 0$.

$V = 0$ hat Dimension $\dim 0 = 0$.

Der Standardvektorraum K^n sollte Dimension n haben. Um dies einzusehen, benötigen wir noch einen weiteren Begriff.

Basis. Ein linear unabhängiges und zugleich erzeugendes Tupel $(x_1, \ldots, x_n)$ in V heißt auch *Basis* von V (über K).

Beispiel. Sei $n \geqslant 1$. Das Tupel

$$(e_1, \ldots, e_n) \;:=\; \left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right)$$

ist eine Basis des Standardvektorraums K^n, genannt die *Standardbasis.*

Das leere Tupel ( ) ist eine Basis des Nullvektorraums $V = 0 = K^0$.

Beispiel. Ein Vektorraum hat im allgemeinen mehr als nur eine Basis. Etwa ist neben der Standardbasis $\left(\binom{1}{0}, \binom{0}{1}\right)$ von $V = \mathbf{R}^2$ über $K = \mathbf{R}$ auch das Tupel $\left(\binom{1}{0}, \binom{1}{1}\right)$ eine Basis.

Lemma. *Das Tupel* $(x_1, \ldots, x_m)$ *ist genau dann linear unabhängig, wenn sich jeder Vektor* $y \in V$ *für höchstens ein Tupel* $(\lambda_1, \ldots, \lambda_m)$*, von Koeffizienten* $\lambda_j \in K$ *als Linearkombination*

$$y \;=\; \lambda_1 x_1 + \cdots + \lambda_m x_m \;=\; \sum_{i\in[1,m]} \lambda_i x_i$$

darstellen läßt.

Beweis. Sei jeder Vektor in V auf höchstens eine Weise als Linearkombination in $(x_1, \ldots, x_m)$ schreibbar. Da sich auch der Nullvektor eindeutig als Linearkombination in $(x_1, \ldots, x_m)$ schreiben läßt, namentlich mit allen Koeffizienten gleich Null, ist $(x_1, \ldots, x_m)$ linear unabhängig.

Umgekehrt, sei $(x_1, \ldots, x_m)$ linear unabhängig. Nehmen wir zwei Darstellungen eines Vektors $y = \sum_{i\in[1,m]} \lambda_i x_i = \sum_{i\in[1,m]} \mu_i x_i$ mit $\lambda_i, \mu_i \in K$ als gegeben an. Es folgt $\sum_{i\in[1,m]}(\lambda_i - \mu_i)x_i = 0$. Der linearen Unabhängigkeit von $(x_1, \ldots, x_m)$ entnehmen wir nun $\lambda_i - \mu_i = 0$, d.h. $\lambda_i = \mu_i$ für alle $i \in [1, m]$. ▫

Zusammenstellung. Ein Tupel $(x_1, \ldots, x_m)$ in V ist

- erzeugend genau dann, wenn jeder Vektor in V *wenigstens* eine Darstellung als Linearkombination in $(x_1, \ldots, x_m)$ hat,
- linear unabhängig genau dann, wenn jeder Vektor in V *höchstens* eine Darstellung als Linearkombination in $(x_1, \ldots, x_m)$ hat, und
- eine Basis genau dann, wenn jeder Vektor in V *genau* eine Darstellung als Linearkombination in $(x_1, \ldots, x_m)$ hat.

Beispiel. Sei $f(X) \in K[X]$ von Grad n gegeben. Da wir jedes Element von $V = K[X]/f(X)K[X]$ eindeutig als Linearkombination in $(\bar{X}^0, \bar{X}^1, \ldots, \bar{X}^{n-1})$ schreiben können, ist $(\bar{X}^0, \bar{X}^1, \ldots, \bar{X}^{n-1})$ eine Basis von V über K. Insbesondere ist $(1, i)$ eine Basis von $\mathbf{C}$ über $\mathbf{R}$. Ferner ist $(1, \alpha)$ eine Basis von $\mathbf{F}_4$ über $\mathbf{F}_2$, es ist $(1, \beta, \beta^2)$ eine Basis von $\mathbf{F}_8$ über $\mathbf{F}_2$, und schließlich ist $(1, \iota)$ eine Basis von $\mathbf{F}_9$ über $\mathbf{F}_3$.

Vorsicht. Die Eigenschaft eines Tupels von Vektoren, Basis eines Vektorraumes zu sein, hängt vom Grundkörper ab. Dies liegt daran, daß mit einem größeren Vorrat an Skalaren, also mit mehr Möglichkeiten, linear zu kombinieren, mehr Tupel in die lineare Abhängigkeit getrieben werden. Etwa ist in $V = \mathbf{C}$ das Tupel $(1, i)$ linear abhängig über $K = \mathbf{C}$, da $1 \cdot 1 + i \cdot i = 0$ gilt, wohingegen es über $K = \mathbf{R}$ eine Basis ist. Über $K = \mathbf{C}$ hat $V = \mathbf{C}$ vielmehr zum Beispiel die Basis (1).

Lemma. *Sei* $(x_1, \ldots, x_k)$ *linear unabhängig, aber nicht erzeugend in* V*, und sei* $(y_1, \ldots, y_l)$ *erzeugend in* V*. Dann gibt es ein* $i \in [1, l]$ *mit* $(x_1, \ldots, x_k, y_i)$ *linear unabhängig in* V*.*

Beweis. Wäre y_i für alle $i \in [1, l]$ im Erzeugnis von $(x_1, \ldots, x_k)$ enthalten, so könnte man jede Linearkombination in $(y_1, \ldots, y_l)$ in eine Linearkombination in $(x_1, \ldots, x_k)$ umformen, und folglich wäre $V = \langle x_1, \ldots, x_k\rangle$, was wir ausgeschlossen hatten. Wir können also ein $i \in [1, l]$ mit $y_i \notin \langle x_1, \ldots, x_k\rangle$ wählen.

In einer Linearkombination

$$\lambda_1 x_1 + \cdots + \lambda_k x_k + \mu y_i \;=\; 0$$

mit Koeffizienten $\lambda_j, \mu \in K$ ist $\mu = 0$, da ansonsten nach Multiplikation mit $-\mu^{-1}$ folgte, daß $y_i \in \langle x_1, \ldots, x_k \rangle$ ist, der Wahl von i widersprechend. Aus $\mu = 0$ folgt nun aber wegen der linearen Unabhängigkeit von $(x_1, \ldots, x_k)$, daß $\lambda_j = 0$ für alle $j \in [1, k]$. Also ist $(x_1, \ldots, x_k, y_i)$ linear unabhängig. □

Lemma. *Sei $(x_1, \ldots, x_k)$ linear unabhängig in V, und sei $(y_1, \ldots, y_l)$ erzeugend in V. Es gibt ein linear unabhängiges Tupel der Form $(y_{i_1}, \ldots, y_{i_k})$ für gewisse, paarweise verschiedene $i_j \in [1, l]$, wobei $j \in [1, k]$. Insbesondere ist $k \leqslant l$.*

Beweis. Wir dürfen $k \geqslant 1$ voraussetzen. Es ist $x_k \notin \langle x_1, \ldots, x_{k-1} \rangle$, da eine Gleichung der Form $x_k = \sum_{i \in [1,k-1]} \lambda_i x_i$ der linearen Unabhängkeit von $(x_1, \ldots, x_k)$ widerspräche. Also ist $(x_1, \ldots, x_{k-1})$ nicht erzeugend in V, und wir finden mit vorigem Lemma ein $i_1 \in [1, l]$ so, daß $(x_1, \ldots, x_{k-1}, y_{i_1})$ linear unabhängig ist.

Da nun $(x_1, \ldots, x_{k-2}, y_{i_1})$ ebensowenig erzeugt, findet man nun genauso ein $i_2 \in [1, l]$ so, daß $(x_1, \ldots, x_{k-2}, y_{i_1}, y_{i_2})$ linear unabhängig ist.

Fährt man so fort, so hat man nach k Schritten ein linear unabhängiges Tupel $(y_{i_1}, \ldots, y_{i_k})$ konstruiert. Aus der linearen Unabhängigkeit folgt nun, daß die Indexabbildung

$$\begin{array}{rcl} [1, k] & \longrightarrow & [1, l] \\ j & \longmapsto & i_j \end{array}$$

injektiv ist. Mithin ist $k \leqslant l$. □

Satz 3 *Sei V ein endlichdimensionaler Vektorraum über K, sei $n := \dim V$.*

(i) *Der Vektorraum V besitzt (mindestens) eine Basis. Alle Basen von V haben die gleiche Länge, nämlich $n = \dim V$.*

(ii) *Jedes linear unabhängige Tupel in V läßt sich zu einer Basis ergänzen. Jedes erzeugende Tupel in V enthält eine Basis.*

(iii) *Jedes linear unabhängige Tupel in V von Länge n ist eine Basis. Jedes erzeugende Tupel in V von Länge n ist eine Basis.*

Beweis. Zu (i). Gemäß der Definition der Dimension gibt es ein linear unabhängiges Tupel $(x_1, \ldots, x_n)$ in V. Wir behaupten, daß jedes solche linear unabhängige Tupel der Länge n eine Basis darstellt, d.h. wir zeigen zunächst die erste Aussage von (iii). Dazu bleibt uns zu zeigen, daß $(x_1, \ldots, x_n)$ ein Erzeugendensystem von V ist. Für ein gegebenes $y \in V$ haben wir hierzu $y \in \langle x_1, \ldots, x_n \rangle$ nachzuweisen.

Das Tupel $(x_1, \ldots, x_n, y)$ ist von Länge $n + 1$, und somit nach Definition der Dimension linear abhängig. Sei

$$0 \;=\; \lambda_1 x_1 + \cdots + \lambda_n x_n + \mu y$$

eine entsprechende Linearkombination mit nicht allen Koeffizienten gleich Null. Nun kann μ nicht verschwinden, da dies der linearen Unabhängigkeit von $(x_1, \ldots, x_n)$ widerspräche. Nach Multiplikation mit $-\mu^{-1}$ sehen wir, daß $y \in \langle x_1, \ldots, x_n \rangle$. Damit ist $(x_1, \ldots, x_n)$ als Basis nachgewiesen.

Ist $(y_1, \ldots, y_m)$ eine weitere Basis, so ist mit vorigem Lemma sowohl $m \leqslant n$ als auch $n \leqslant m$, insgesamt also $n = m$. Damit haben alle Basen dieselbe Länge $n = \dim V$.

Zu (ii). Iterierte Anwendung des vorvorigen Lemmas auf das fragliche linear unabhängige Tupel $(x_1, \ldots, x_k)$ und ein beliebiges erzeugendes Tupel $(y_1, \ldots, y_l)$ (z.B. eine Basis) liefert die Basisergänzung, da die Iteration abbricht, sobald das ergänzte Tupel sowohl linear unabhängig als auch erzeugend ist. Wegen $\dim V = n$ muß das Verfahren nach spätestens $n - k$ Schritten abbrechen.

Mit vorigem Lemma, angewandt auf eine Basis $(x_1, \ldots, x_n)$ und das fragliche erzeugende Tupel $(y_1, \ldots, y_l)$, findet man ein linear unabhängiges Tupel von Länge n, welches aus gewissen Einträgen von $(y_1, \ldots, y_l)$ besteht. Mit der bereits gezeigten ersten Aussage von (iii) folgt, daß es sich dabei um eine Basis handelt.

Zu (iii), zweite Aussage. Mit (ii) läßt sich auch aus jedem erzeugenden Tupel der Länge n eine Basis auswählen. Da jede Basis aber mit (i) gerade Länge n hat, muß das fragliche erzeugende Tupel bereits eine Basis gewesen sein.

Beispiel. Für $n \geqslant 0$ ist $\dim K^n = n$, wie man der Standardbasis entnimmt.

Beispiel. Es ist $\dim_{\mathbf{R}} \mathbf{C} = 2$, $\dim_{\mathbf{F}_2} \mathbf{F}_4 = 2$, $\dim_{\mathbf{F}_2} \mathbf{F}_8 = 3$, und $\dim_{\mathbf{F}_3} \mathbf{F}_9 = 2$. Vorsicht, es ist $\dim_{\mathbf{C}} \mathbf{C} = 1 \neq 2 = \dim_{\mathbf{R}} \mathbf{C}$, etc.

2.3 Unterräume

Sei V ein Vektorraum über einem Körper K.

Definition. Eine Teilmenge $U \subseteq V$ heißt *Unterraum* von V, falls $0 \in U$ und falls

$$\lambda y + \mu z \;\in\; U$$

für alle $\lambda, \mu \in K$ und alle $y, z \in U$.

Mit $\lambda = 1$ und $\mu = -1$ folgt dann, daß U eine Untergruppe der additiven Gruppe von V ist. Wir werden daher mißbräuchlicherweise auch die Unterraumbeziehung als $U \leqslant V$ notieren.

Mit den eingeschränkten Operationen $U \times U \xrightarrow{(+)} U$ und $K \times U \xrightarrow{(\cdot)} U$ wird U zu einem Vektorraum über K, da sich die Gültigkeit von (V 1-5) von V nach U vererbt.

Ist V endlichdimensional und $U \leqslant V$, so ist auch U endlichdimensional. Denn ist die Länge eines linear unabhängigen Tupels in V nach oben beschränkt, so gilt dies erst recht in U.

Beispiel. $0 := \{0\}$ und V sind Unterräume von V.

Lemma. *Sei $(x_1, \ldots, x_m)$ ein Tupel von Vektoren in V. Ihr Erzeugnis $\langle x_1, \ldots, x_m \rangle$ ist ein Unterraum von V. Es ist*

$$\dim \langle x_1, \ldots, x_m \rangle \;\leqslant\; m \;,$$

mit Gleichheit genau dann, wenn $(x_1, \ldots, x_m)$ linear unabhängig ist.

Beweis. Zunächst ist $0 = \sum_{i \in [1,m]} 0 \cdot x_i \in U := \langle x_1, \ldots, x_m \rangle$. Sind ferner $\lambda, \mu \in K$ und sind $y = \sum_{i \in [1,m]} \eta_i x_i$ und $z = \sum_{i \in [1,m]} \zeta_i x_i$ in U, $\zeta_i,\, \eta_i \in K$, so ist auch

$$\lambda y + \mu z \;=\; \sum_{i \in [1,m]} (\lambda \eta_i + \mu \zeta_i) x_i \;\in U \;,$$

woraus $U \leqslant V$.

Es ist nun $(x_1, \ldots, x_m)$ ein erzeugendes Tupel von U. Nach Satz 3.(ii) können wir aus diesem eine Basis von U auswählen. Nach Satz 3.(i) ist die Dimension von U gleich der Länge dieses ausgewählten Tupels, was die behauptete Ungleichung zeigt.

Ist $(x_1, \ldots, x_m)$ linear unabhängig, so ist es eine Basis von U, und wir haben Gleichheit.

Ist umgekehrt Gleichheit vorausgesetzt, so darf für die Basisauswahl aus $(x_1, \ldots, x_m)$ kein Vektor weggelassen werden, da sonst eine Basis von Länge $< m$ resultierte. In anderen Worten, $(x_1, \ldots, x_m)$ ist eine Basis. ▫

Beispiel. Sei $K = \mathbf{R}$. Ist $V = \mathbf{R}^2$, so ist der eindimensionale Unterraum $\langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle$ veranschaulicht durch eine Ursprungsgerade, nämlich die erste Winkelhalbierende.

Ist $V = \mathbf{R}^3$, so ist der eindimensionale Unterraum $\langle \left(\begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix}\right) \rangle$ veranschaulicht durch die Ursprungsgerade, die den Vektor $\left(\begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix}\right)$ enthält. Der zweidimensionale Unterraum $\langle \left(\begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 \\ 2 \\ 3 \end{smallmatrix}\right) \rangle$ ist die Ursprungsebene, die von den Vektoren $\left(\begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -1 \\ 2 \\ 3 \end{smallmatrix}\right)$ aufgespannt wird.

Lemma. *Ist $U \leqslant V$, und ist $\dim U = \dim V$, so ist $U = V$.*

Beweis. Schreibe $n = \dim U = \dim V$, und sei $(x_1, \ldots, x_n)$ eine Basis von U. Nach Satz 3.(ii) können wir diese zu einer Basis von V ergänzen, welche nach Satz 3.(i) ebenfalls Länge n hat, und also bereits gleich $(x_1, \ldots, x_n)$ ist. Es folgt $U = \langle x_1, \ldots, x_n \rangle = V$. ▫

Für $T, U \leqslant V$ setzen wir

$$\begin{array}{rcl} T \cap U & := & \{x \in V \mid x \in T \text{ und } x \in U\} \\ T + U & := & \{t + u \mid t \in T,\ u \in U\} \;. \end{array}$$

Lemma. *Sind $T, U \leqslant V$, so ist sowohl $T \cap U \leqslant V$ als auch $T + U \leqslant V$.*

Beweis. Wir betrachten $T \cap U$ und stellen fest, daß $0 \in T \cap U$. Seien nun $y, z \in T \cap U$ und $\lambda, \mu \in K$ gegeben. Es ist $\lambda y + \mu z \in T$, da $T \leqslant V$, und $\lambda y + \mu z \in U$, da $U \leqslant V$. Also ist $\lambda y + \mu z \in T \cap U$.

Wir betrachten $T + U$ und stellen fest, daß $0 = 0 + 0 \in T + U$. Seien $y, z \in T + U$, genauer, seien $y = t + u$ und $z = t' + u'$ mit $t, t' \in T$ und $u, u' \in U$. Für $\lambda, \mu \in K$ wird

$$\lambda y + \mu z \;=\; (\lambda t + \mu t') + (\lambda u + \mu u') \;\in\; T + U \;.$$

▫

Direkte Summe. Sei $k \geqslant 2$, und seien U_1, U_2, …, U_k Unterräume von V. Gibt es für jeden Vektor $x \in \sum_{j\in[1,k]} U_j := U_1 + U_2 + \cdots + U_k$ *genau* eine Darstellung der Form

$$x \;=\; \sum_{j\in[1,k]} u_j \;=\; u_1 + u_2 + \cdots + u_k \qquad \text{mit } u_j \in U_j \text{ für alle } j \in [1,k]\,,$$

so heißt die Summe $U_1 + U_2 + \cdots + U_k$ *direkt,* und man schreibt

$$\sum_{j\in[1,k]} U_j \;=\; U_1 + U_2 + \cdots + U_k \;=:\; U_1 \oplus U_2 \oplus \cdots \oplus U_k \;=\; \bigoplus_{j\in[1,k]} U_j\,.$$

Das Symbol $\oplus$ bezeichnet also den durch die Summe gebildeten Unterraum, zusammen mit der Information, daß diese Summe direkt ist.

Lemma. *Ist $V = \bigoplus_{j\in[1,m]} U_j$ für Unterräume $U_j \leqslant V$, und ist jeweils $(x_{j,1},\dots,x_{j,l_j})$ eine Basis von U_j, so ist das zusammengesetzte Tupel*

$$\underline{x} \;:=\; (x_{1,1},\dots,x_{1,l_1},\; x_{2,1},\dots,x_{2,l_2},\; \dots,\; x_{m,1},\dots,x_{m,l_m})$$

eine Basis von V.

Beweis. Zeigen wir, daß $\underline{x}$ erzeugend in V ist. Sei $y \in V$. Da $V = \sum_{i\in[1,m]} U_j$, können wir $y = \sum_{j\in[1,m]} u_j$ mit $u_j \in U_j$ schreiben. Da $U_j = \langle x_{j,1},\dots,x_{j,l_j}\rangle$, gibt es $\lambda_{j,k} \in K$ mit $u_j = \sum_{k\in[1,l_j]} \lambda_{j,k}x_{j,k}$. Insgesamt wird

$$y \;=\; \sum_{j\in[1,m]}\sum_{k\in[1,l_j]} \lambda_{j,k}x_{j,k} \;\in\; \langle\underline{x}\rangle\,.$$

Zeigen wir, daß $\underline{x}$ linear unabhängig ist. Sei

$$\sum_{j\in[1,m]}\sum_{k\in[1,l_j]} \lambda_{j,k}x_{j,k} \;=\; 0$$

für gewisse $\lambda_{j,k} \in K$. Wegen der Direktheit von $\bigoplus_{j\in[1,m]} U_j$ folgt mit $\sum_{k\in[1,l_j]} \lambda_{j,k}x_{j,k} \in U_j$, und der alternativen Darstellung des Nullvektors als $\sum_{j\in[1,m]} 0 = 0$ mit jeweils $0 \in U_j$, daß $\sum_{k\in[1,l_j]} \lambda_{j,k}x_{j,k} = 0$ für alle $j \in [1,m]$. Mit der linearen Unabhängigkeit von $(x_{j,1},\dots,x_{j,l_j})$ folgt, daß $\lambda_{j,k} = 0$ stets. ▫

Lemma. *Die Summe $U_1 + U_2 + \cdots + U_k$ der Unterräume $U_j \leqslant V$ ist direkt genau dann, wenn*

$$U_l \cap \Big(\sum_{j\in[1,k]\smallsetminus\{l\}} U_j\Big) \;=\; 0$$

für alle $l \in [1,k]$. Insbesondere, ist $k = 2$, so ist $U_1 + U_2$ direkt genau dann, wenn $U_1 \cap U_2 = 0$.

Beweis. Sei die Summe direkt, sei $l \in [1,k]$ gegeben, und sei $u_l \in U_l \cap (\sum_{j\in[1,k]\smallsetminus\{l\}} U_j)$, d.h. wir können schreiben

$$u_l \;=\; \sum_{j\in[1,k]\smallsetminus\{l\}} (-u_j)\,,$$

wobei $u_j \in U_j$ stets. Daraus folgt nun $\sum_{j\in[1,k]} u_j = 0$, und da alternativ $\sum_{j\in[1,k]} 0 = 0$ mit $0 \in U_j$ stets, folgt aus der vorausgesetzten Eindeutigkeit der Darstellung, daß $u_j = 0$ stets, insbesondere $u_l = 0$.

Sei umgekehrt $U_l \cap (\sum_{j\in[1,k]\smallsetminus\{l\}} U_j) = 0$ für $l \in [1,k]$, und seien $x = \sum_{j\in[1,k]} u_j = \sum_{j\in[1,k]} u'_j$ zwei Darstellungen der verlangten Art, d.h. mit $u_j,\, u'_j \in U_j$ stets. Aus $u'_l - u_l = \sum_{j\in[1,k]\smallsetminus\{l\}} (u_j - u'_j) \in U_l \cap (\sum_{j\in[1,k]\smallsetminus\{l\}} U_j) = 0$ folgt nun $u'_l - u_l = 0$, und dies für alle $l \in [1,k]$. ▫

Satz 4 *Ist V endlichdimensional und sind $T,\, U \leqslant V$, so ist*

$$\dim(T+U) + \dim(T\cap U) \;=\; \dim T + \dim U\ .$$

Für eine direkte Summe gilt insbesondere $\dim(T \oplus U) = \dim T + \dim U$.

Beweis. Sei $(x_1,\ldots,x_m)$ eine Basis von $T\cap U$, ergänzt mit Satz 3.(ii) zu einer Basis $(x_1,\ldots,x_m,y_1,\ldots,y_k)$ von T und zu einer Basis $(x_1,\ldots,x_m,z_1,\ldots,z_l)$ von U. Wir haben zu zeigen, daß $(x_1,\ldots,x_m,y_1,\ldots,y_k,z_1,\ldots,z_l)$ eine Basis von $T+U$ ist, denn dann ist $\dim T+U = m+k+l$, während $\dim T\cap U = m$, $\dim T = m+k$ und $\dim U = m+l$ sind.

Zeigen wir zunächst, daß dieses Tupel $T+U$ erzeugt. Ist uns ein Vektor $x = t+u$ mit $t \in T$ und $u \in U$ gegeben, so können wir t als Linearkombination in $(x_1,\ldots,x_m,y_1,\ldots,y_k)$ und u als Linearkombination in $(x_1,\ldots,x_m,z_1,\ldots,z_l)$ schreiben. Ihre Summe $t+u$ ist mithin eine Linearkombination in $(x_1,\ldots,x_m,y_1,\ldots,y_k,z_1,\ldots,z_l)$.

Zeigen wir nun die lineare Unabhängigkeit. Sei also

$$0 \;=\; \left(\sum_{i\in[1,m]} \xi_i x_i\right) + \left(\sum_{i\in[1,k]} \eta_i y_i\right) + \left(\sum_{i\in[1,l]} \zeta_i z_i\right)$$

mit $\xi_i, \eta_i, \zeta_i \in K$. Es folgt $\sum_{i\in[1,k]} \eta_i y_i \in T\cap U$, in T nach Konstruktion, in U wegen dieser Linearkombination. Da aber $(x_1,\ldots,x_m)$ eine Basis von $T\cap U$ ist, ist jedes Element darin eine Linearkombination in $(x_1,\ldots,x_m)$, welche durch Nullkoeffizienten eindeutig fortgesetzt werden kann zu einer Linearkombination von $(x_1,\ldots,x_m,y_1,\ldots,y_k)$. Da die Koeffizienten von $\sum_{i\in[1,k]} \eta_i y_i \in T$ in dieser Basis eindeutig sind, folgt $\eta_i = 0$ für alle $i \in [1,k]$. Die lineare Unabhängigkeit von $(x_1,\ldots,x_m,z_1,\ldots,z_l)$ zeigt nun $\xi_i = 0$ für alle $i \in [1,m]$ und $\zeta_i = 0$ für alle $i \in [1,l]$. ▫

Beispiel. Ist $K = \mathbf{R}$, $V = \mathbf{R}^3$, $T = \langle \left(\begin{smallmatrix}1\\0\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}\right) \rangle$ und $U = \langle \left(\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\\1\end{smallmatrix}\right) \rangle$, so ist $T\cap U = \langle \left(\begin{smallmatrix}1\\-1\\0\end{smallmatrix}\right) \rangle$ und $T+U = V$. Wir verifizieren

$$\dim(T\cap U) + \dim(T+U) \;=\; 1+3 \;=\; 2+2 \;=\; \dim T + \dim U\ .$$

2.4 Lineare Abbildungen

Seien V, W und Y Vektorräume über einem Körper K.

Definition. Eine Abbildung $V \xrightarrow{f} W$ heißt *linear* oder *K-linear,* falls für alle $\lambda, \mu \in K$ und alle $y, z \in V$ gilt, daß

$$f(\lambda y + \mu z) \;=\; \lambda f(y) + \mu f(z)\;.$$

Kurz: f respektiert Linearkombinationen.

Sind $V \xrightarrow{f} W \xrightarrow{g} Y$ zwei lineare Abbildungen, so ist auch $V \xrightarrow{g\circ f} Y$ eine lineare Abbildung.

Falls $V = W$, so heißt $V \xrightarrow{f} V$ *Endomorphismus* (griech. "endon" = innerhalb).

Falls f bijektiv ist, so heißt $V \xrightarrow[\sim]{f} W$ *Isomorphismus* (griech. "iso" = gleich). Gibt es (wenigstens) einen Isomorphismus von V nach W, so heißen V und W *isomorph,* geschrieben $V \simeq W$.

Ist $V \xrightarrow{f} W$ eine lineare Abbildung, so sehen wir wegen $f(y+z) = f(y)+f(z)$ für $y, z \in V$, daß f insbesondere ein Gruppenmorphismus der abelschen Gruppe $(V, +)$ in die abelsche Gruppe $(W, +)$ ist. Wie für jeden Gruppenmorphismus ist also

$$\operatorname{Kern} f \;=\; \{x \in V \mid f(x) = 0\}$$

genau dann gleich 0, wenn f injektiv ist.

Es ist stets $\operatorname{Kern} f \leqslant V$. In der Tat, ist $f(y) = 0$ und $f(z) = 0$ für $y, z \in V$, und sind $\mu, \lambda \in K$, so ist auch $f(\mu y+\lambda z) = \mu f(y)+\lambda f(z) = 0$. Wegen $f(0) = 0$ ist auch $0 \in \operatorname{Kern} f$.

Für das Bild von V unter f schreiben wir auch

$$\operatorname{Im} f \;:=\; f(V)$$

(engl. "image").

Es ist stets $\operatorname{Im} f \leqslant W$. In der Tat ist für $y, z \in V$ und $\mu, \lambda \in K$ die Linearkombination $\mu f(y) + \lambda f(z) = f(\mu y + \lambda z)$ wieder im Bild enthalten. Wegen $f(0) = 0$ ist auch $0 \in \operatorname{Im} f$.

Beispiel. Seien $K = \mathbf{R}$, $V = \mathbf{R}^2$, $W = \mathbf{R}^3$ und sei $f\left(\left(\begin{smallmatrix}\xi_1\\ \xi_2\end{smallmatrix}\right)\right) \;=\; \begin{pmatrix}\xi_2+2\xi_1\\ \xi_1\\ -3\xi_2\end{pmatrix}$. Eintragsweise erkennt man, daß f linear ist.

Beispiel. Sei $V = W = K[X]$. Die Ableitung eines Polynoms $f(X) = \sum_{i\geqslant 0} a_i X^i \in K[X]$ werde formal definiert als

$$Df(X) \;=\; f'(X) \;=\; (f(X))' \;:=\; \sum_{i\geqslant 1} a_i i X^{i-1}\;.$$

Zum Beispiel ist für $K = \mathbf{F}_p$ und $f(X) = X^p + X$ die Ableitung $f'(X) = 1$.

Für allgemeines K ist die Abbildung

$$\begin{array}{rcl} K[X] & \xrightarrow{D} & K[X] \\ f(X) & \longmapsto & Df(X) := f'(X) \end{array}$$

linear. Es handelt sich also um einen Endomorphismus. Dieser ist nicht injektiv, da konstante Polynome auf 0 gehen. Im allgemeinen ist er auch nicht surjektiv. So etwa hat $X^{p-1} \in \mathbf{F}_p[X]$ kein Urbild unter D. Für $K = \mathbf{R}$ ist der Endomorphismus $\mathbf{R}[X] \xrightarrow{D} \mathbf{R}[X]$ aber sehr wohl surjektiv, wenn auch nicht injektiv.

Beispiel. Sei $V = \mathbf{F}_4$. Die Frobenius-Abbildung

$$\begin{array}{rcl} \mathbf{F}_4 & \overset{F}{\underset{\sim}{\longrightarrow}} & \mathbf{F}_4 \\ a + b\alpha & \longmapsto & (a+b\alpha)^2 \;=\; a + b\alpha^2 \;=\; (a+b) + b\alpha \qquad (a, b \in \mathbf{F}_2) \end{array}$$

ist ein $\mathbf{F}_2$-linearer Isomorphismus von $\mathbf{F}_4$ in sich. Dieser ist allerdings nicht $\mathbf{F}_4$-linear, vielmehr gilt

$$F((a+b\alpha)\cdot(a'+b'\alpha)) \;=\; (a+b\alpha)^2 \cdot (a'+b'\alpha)^2 \;=\; F(a+b\alpha)\cdot F(a'+b'\alpha)\;.$$

Satz 5 *Sei $(x_1, \ldots, x_n)$ eine Basis von V und sei $V \xrightarrow{f} W$ eine lineare Abbildung.*

(i) *Die Abbildung $V \xrightarrow{f} W$ ist injektiv genau dann, wenn $(f(x_1), \ldots, f(x_n))$ linear unabhängig in W ist.*

(ii) *Die Abbildung $V \xrightarrow{f} W$ ist surjektiv genau dann, wenn $(f(x_1), \ldots, f(x_n))$ erzeugend in W ist.*

(iii) *Die Abbildung $V \xrightarrow{f} W$ ist bijektiv genau dann, wenn $(f(x_1), \ldots, f(x_n))$ eine Basis von W ist. Diesenfalls ist die Umkehrabbildung $W \xrightarrow{f^{-1}} V$ ebenfalls linear.*

(iv) *Ein Endomorphismus eines* endlich*dimensionalen Vektorraums ist bijektiv genau dann, wenn er injektiv ist, und auch genau dann, wenn er surjektiv ist.*

Beweis. Zu (i). Sei f injektiv, und sei $\sum_{i\in[1,n]} \lambda_i f(x_i) = 0$. Dann ist auch $f(\sum_{i\in[1,n]} \lambda_i x_i) = 0$, so daß mit der Injektivität von f folgt, daß $\sum_{i\in[1,n]} \lambda_i x_i = 0$, und schließlich mit der linearen Unabhängigkeit von $(x_1, \ldots, x_n)$, daß $\lambda_i = 0$ für $i \in [1, n]$.

Sei umgekehrt $(f(x_1), \ldots, f(x_n))$ linear unabhängig in W, und sei $y \in V$ gegeben mit $f(y) = 0$. Es ist zu zeigen, daß $y = 0$. Wir schreiben $y = \sum_{i\in[1,n]} \lambda_i x_i$ und erhalten $0 = f(\sum_{i\in[1,n]} \lambda_i x_i) = \sum_{i\in[1,n]} \lambda_i f(x_i)$, so daß mit der linearen Unabhängigkeit von $(f(x_1), \ldots, f(x_n))$ folgt, daß $\lambda_i = 0$ für $i \in [1, n]$.

Zu (ii). Sei f surjektiv, und sei uns ein $z \in W$ vorgegeben, welches wir als Linearkombination in $(f(x_1), \ldots, f(x_n))$ auszudrücken haben. Die Surjektivität von f gibt uns ein $y = \sum_{i\in[1,n]} \lambda_i x_i \in V$ mit

$$z \;=\; f(y) \;=\; \sum_{i\in[1,n]} \lambda_i f(x_i)\;.$$

Sei umgekehrt $(f(x_1), \dots, f(x_n))$ erzeugend, und sei uns ein $z \in W$ vorgegeben. Schreiben wir $z = \sum_{i\in[1,n]} \lambda_i f(x_i) = f\Big(\sum_{i\in[1,n]} \lambda_i x_i\Big)$, so sehen wir $z \in f(V)$.

Zu (iii). Mit (i) und (ii) bleibt zu zeigen, daß $W \xrightarrow{f^{-1}} V$ linear ist. Seien $y, z \in W$ und $\lambda, \mu \in K$ gegeben. Aus

$$f(f^{-1}(\lambda y + \mu z)) \;=\; \lambda y + \mu z \;=\; \lambda f(f^{-1}(y)) + \mu f(f^{-1}(z)) \;=\; f(\lambda f^{-1}(y) + \mu f^{-1}(z))$$

folgt mit f injektiv, daß in der Tat $f^{-1}(\lambda y + \mu z) = \lambda f^{-1}(y) + \mu f^{-1}(z)$.

Zu (iv). Ist $V \xrightarrow{f} V$ injektiv, so schickt f mit (i) eine Basis auf ein linear unabhängiges Tupel. Da dies ebenfalls Länge n hat, ist es eine Basis nach Satz 3.(iii), und f ist bijektiv mit (iii).

Ist $V \xrightarrow{f} V$ surjektiv, so schickt f mit (ii) eine Basis auf ein erzeugendes Tupel. Da dies ebenfalls Länge n hat, ist es eine Basis nach Satz 3.(iii), und f ist bijektiv mit (iii). ▫

Aus Satz 5.(iii) ersehen wir, daß isomorphe endlichdimensionale Vektorräume dieselbe Dimension haben. Genauer, existiert eine injektive lineare Abbildung $V \xrightarrow{f} W$, so ist $\dim V \leqslant \dim W$, existiert eine surjektive solche Abbildung, so ist $\dim V \geqslant \dim W$.

Lemma. *Sei $\underline{x} = (x_1, \dots, x_n)$ eine Basis von V. Zu jedem Tupel $(y_1, \dots, y_n)$ von Vektoren in W gibt es genau eine lineare Abbildung $V \xrightarrow{f} W$ so, daß $f(x_i) = y_i$ für alle $i \in [1, n]$.*

Beweis. Sind die Bilder $(y_1, \dots, y_n)$ der Basiselemente $(x_1, \dots, x_n)$ unter einer linearen Abbildung f bekannt, so auch das Bild eines allgemeinen Elements $\sum_{i\in[1,n]} \lambda_i x_i \in V$, da

$$f\left(\sum_{i\in[1,n]} \lambda_i x_i\right) \;=\; \sum_{i\in[1,n]} \lambda_i f(x_i) \;=\; \sum_{i\in[1,n]} \lambda_i y_i\ .$$

Hieraus folgt die Eindeutigkeit.

Für die Existenz setzen wir für $z = \sum_{i\in[1,n]} \lambda_i x_i \;\in\; V$, wobei $\lambda_i \in K$, das Bild zu

$$f(z) = f\left(\sum_{i\in[1,n]} \lambda_i x_i\right) \;:=\; \sum_{i\in[1,n]} \lambda_i y_i\ .$$

Dies liefert eine Abbildung von V nach W, da die Koeffizienten λ_i durch Angabe von $z \in V$ eindeutig festliegen. Die Linearität dieser Abbildung folgt aus

$$\begin{array}{rcl} f(\mu z + \mu' z') & = & f\left(\mu\left(\sum_{i\in[1,n]} \lambda_i x_i\right) + \mu'\left(\sum_{i\in[1,n]} \lambda'_i x_i\right)\right) \\ & = & f\left(\sum_{i\in[1,n]} (\mu\lambda_i + \mu'\lambda'_i) x_i\right) \\ & \overset{\text{Def.}}{=} & \sum_{i\in[1,n]} (\mu\lambda_i + \mu'\lambda'_i) y_i \\ & = & \mu f(z) + \mu' f(z') \end{array}$$

für $z = \sum_{i\in[1,n]} \lambda_i x_i \in V$, $z' = \sum_{i\in[1,n]} \lambda'_i x_i \in V$, mit $\lambda_i, \lambda'_i \in K$, und für $\mu, \mu' \in K$. ▫

Folgerung. *Jeder endlichdimensionale Vektorraum V über K ist isomorph zu einem Standardvektorraum K^n, wobei $n = \dim V$.*

Beweis. Sei $\underline{x} = (x_1, \ldots, x_n)$ eine Basis von V. Die vom vorigen Lemma gelieferte Abbildung $K^n \longrightarrow V$, die die Standardbasis $(e_1, \ldots, e_n)$ auf $(x_1, \ldots, x_n)$ schickt, ist nach Satz 5.(iii) ein Isomorphismus. ▫

Satz 6 *Ist V endlichdimensional und $V \xrightarrow{f} W$ eine lineare Abbildung, so gilt*

$$\dim \mathrm{Kern}\, f + \dim \mathrm{Im}\, f \;=\; \dim V\ .$$

Beweis. Sei $(x_1, \ldots, x_k)$ eine Basis von Kern f, erweitert zu einer Basis $(x_1, \ldots, x_k, y_1, \ldots, y_l)$ von V. Dann erzeugt $(f(y_1), \ldots, f(y_l))$ den Unterraum Im f von W. Die Behauptung wird folgen, sobald wir $(f(y_1), \ldots, f(y_l))$ als linear unabhängig kennen, da dann $\dim V = k+l = \dim \mathrm{Kern}\, f + \dim \mathrm{Im}\, f$ folgt. Sei dazu

$$0 \;=\; \sum_{i\in[1,l]} \lambda_i f(y_i) \;=\; f\left(\sum_{i\in[1,l]} \lambda_i y_i\right)$$

mit $\lambda_i \in K$ angesetzt. Da $\sum_{i\in[1,l]} \lambda_i y_i$ deswegen in Kern f liegt, ist es zugleich eine Linearkombination in $(x_1, \ldots, x_k)$, die mit Nullkoeffizienten zu einer Linearkombination in $(x_1, \ldots, x_k, y_1, \ldots, y_l)$ fortgesetzt werden kann. Da die Koeffizienten einer Darstellung in $(x_1, \ldots, x_k, y_1, \ldots, y_l)$ aber eindeutig sind, folgt $\lambda_i = 0$ für alle $i \in [1, l]$. ▫

Beispiel. Sei $K = \mathbf{F}_2$, sei $V = \mathbf{F}_2^3$, sei $W = \mathbf{F}_2^4$, und sei

$$f : V \longrightarrow W : \begin{pmatrix}\eta_1\\ \eta_2\\ \eta_3\end{pmatrix} \longmapsto \begin{pmatrix}\eta_1+\eta_2\\ \eta_1+\eta_3\\ \eta_2+\eta_3\\ 0\end{pmatrix}\ .$$

Wir erhalten eine Basis $\langle \begin{pmatrix}1\\1\\1\end{pmatrix} \rangle$ des Kerns, und eine Basis $\langle \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\end{pmatrix} \rangle$ des Bildes. Zusammen ergibt sich die Dimension $1 + 2 = 3$ von V.

Definition. Die Menge der linearen Abbildungen von V nach W schreiben wir $\mathrm{Lin}_K(V, W)$ oder $\mathrm{Lin}(V, W)$. Mittels

$$\begin{array}{rcl} \mathrm{Lin}(V,W) \times \mathrm{Lin}(V,W) & \xrightarrow{(+)} & \mathrm{Lin}(V,W) \\ (f,g) & \longmapsto & f+g : y \longmapsto f(y)+g(y) \\ K \times \mathrm{Lin}(V,W) & \xrightarrow{(\cdot)} & \mathrm{Lin}(V,W) \\ (\lambda, f) & \longmapsto & \lambda\cdot f : y \longmapsto \lambda \cdot f(y) \end{array}$$

wird $\mathrm{Lin}(V, W)$ zu einem Vektorraum über K. Sind vier lineare Abbildungen

$$V \underset{f'}{\overset{f}{\rightrightarrows}} W \underset{g'}{\overset{g}{\rightrightarrows}} Y$$

gegeben, so gilt

$$(g+g')\circ(f+f') \;=\; g\circ f + g\circ f' + g'\circ f + g'\circ f'\,.$$

Ferner ist für $\lambda\in K$ auch

$$g\circ(\lambda\cdot f) \;=\; (\lambda\cdot g)\circ f \;=\; \lambda\cdot(g\circ f)\,.$$

Ist insbesondere $V=W$, so schreiben wir $\mathrm{End}(V)=\mathrm{End}_K(V):=\mathrm{Lin}(V,V)$ und sehen, daß $(\mathrm{End}(V),+,\circ)$ einen Ring bildet, mit der Nullabbildung als 0 und der Identität 1_V als 1.

Lemma. *Sei R ein beliebiger Ring, und bezeichne*

$$\mathrm{Inv}(R) \;:=\; \{x\in R \mid \textit{es gibt ein } y\in R \textit{ mit } xy=yx=1\} \;\subseteq\; R$$

die Teilmenge der invertierbaren *Elemente. Dann ist* $\mathrm{Inv}(R)$, *zusammen mit der auf* $\mathrm{Inv}(R)$ *eingeschränkten Multiplikation, eine Gruppe. Das daher eindeutig festliegende Inverse y von $x\in$* $\mathrm{Inv}(R)$ *wird als $x^{-1}:=y$ geschrieben.*

Beweis. Zunächst müssen wir sehen, daß für $x,x'\in\mathrm{Inv}(R)$ auch das Produkt xx' wieder in $\mathrm{Inv}(R)$ liegt. Sei $xy=yx=1$, und sei $x'y'=y'x'=1$. Dann ist $xx'y'y=1$ und $y'yxx'=1$. Damit ist $\mathrm{Inv}(R)\times\mathrm{Inv}(R)\xrightarrow{(\cdot)}\mathrm{Inv}(R)$ wohldefiniert, und wir können nach den Gruppenaxiomen fragen. Die Assoziativität (G 1) und das neutrale Element (G 2) vererben sich von (R 2) (es ist $1\in\mathrm{Inv}(R)$). Zu (G 3) merken wir an, daß das Inverse y zu $x\in\mathrm{Inv}(R)$ nach Konstruktion von $\mathrm{Inv}(R)$ vorhanden ist – zunächst ist $y\in R$, wegen $xy=yx=1$ ist dann auch $y\in\mathrm{Inv}(R)$. ▫

Beispiel. Es ist $\mathrm{Inv}(\mathbf{Z})=\{-1,+1\}$. Es ist $\mathrm{Inv}(\mathbf{Z}/10\mathbf{Z})=\{1,3,7,9\}$. Für einen Körper K ist $\mathrm{Inv}(K)=K\smallsetminus\{0\}$, und auch $\mathrm{Inv}(K[X])=K\smallsetminus\{0\}$.

Bemerkung. Ist V endlichdimensional und ist $f\in\mathrm{End}\,V$, so ist für ein $g\in\mathrm{End}\,V$ genau dann $f\circ g=1_V$, wenn $g\circ f=1_V$. Denn ist $f\circ g=1_V$, so ist f surjektiv, und also mit Satz 5 auch injektiv. Daher folgt aus $f\circ g\circ f=f$, daß auch $g\circ f=1_V$. Umgekehrt, ist $g\circ f=1_V$, so ist f injektiv, und also mit Satz 5 auch surjektiv. Daher folgt aus $f\circ g\circ f=f$, daß auch $f\circ g=1_V$.

Mit Satz 5 ist also f invertierbar genau dann, wenn es ein Isomorphismus ist.

Definition. Die *allgemeine lineare Gruppe* von V ist definiert als $\mathrm{GL}(V):=\mathrm{Inv}(\mathrm{End}(V))$, d.h. als die Menge der Isomorphismen von V in sich, mit der Komposition als Multiplikation.

Definition. Sei $n\geqslant 1$ und $V=K^n$. Wir haben einen injektiven Gruppenmorphismus

$$\begin{array}{ccl} \mathcal{S}_n & \xrightarrow{\pi} & \mathrm{GL}(K^n) \\ \sigma & \longmapsto & \pi(\sigma) : e_i \longmapsto e_{\sigma(i)}\;. \end{array}$$

Denn für $\sigma,\rho\in\mathcal{S}_n$ bildet $\pi(\sigma)\circ\pi(\rho)$ das Basiselement e_i auf $e_{\sigma(\rho(i))}$ ab, genauso wie $\pi(\sigma\circ\rho)$, woraus wir $\pi(\sigma)\circ\pi(\rho)=\pi(\sigma\circ\rho)$ ersehen. Ferner ist in der Tat $\sigma=1$ die einzige Permutation, für welche $\pi(\sigma)=1_V$, was die Injektivität zeigt.

Insbesondere ist $\mathrm{GL}(K^n)$ im allgemeinen nicht abelsch, und also $\mathrm{End}(K^n)$ im allgemeinen nicht kommutativ.

Ein Element der Form $\pi(\sigma) \in \mathrm{GL}(K^n)$ mit $\sigma \in \mathcal{S}_n$ wird auch als *Permutationsendomorphismus* bezeichnet.

Die innere Beschaffenheit der eben definierten Gebilde $\mathrm{Lin}(V, W)$, $\mathrm{End}(V)$ und $\mathrm{GL}(V)$ wird sich unter Zuhilfenahme der Matrixrechnung des nächsten Kapitels klären.

Kapitel 3

Matrizen

Die Matrixrechnung ist der Kalkül der Linearen Algebra. Eine Matrix stellt hierbei eine in gewissem Sinne standardisierte lineare Abbildung dar. Deren Eigenschaften werden in den Eigenschaften der Matrix reflektiert – die Invertierbarkeit etwa in der Determinante.

Sei K ein Körper.

3.1 Begriffe

3.1.1 Der Matrixbegriff

Seien $m, n \geqslant 1$. Eine *Matrix* A (der Größe $m \times n$) ist ein $m \cdot n$-Tupel von Elementen von K, angeordnet in einer Tafel

$$A \;=\; (a_{i,j})_{i\in[1,m],\, j\in[1,n]} \;=\; (a_{i,j})_{i,j} \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,n} \end{pmatrix}.$$

Die Menge der $m \times n$-Matrizen wird mit $K^{m\times n}$ bezeichnet. Die j-te Spalte von A wird mit $a_{*,j} \in K^{m\times 1}$, und die i-te Zeile mit $a_{i,*} \in K^{1\times n}$ bezeichnet.

Vermittels eintragsweiser Addition und eintragsweiser skalarer Multiplikation wird $K^{m\times n}$ zu einem Vektorraum über K, isomorph zu K^{mn}.

Einträge von Matrizen werden mit kleinen lateinischen Buchstaben bezeichnet. Einträge von Vektoren im Standardvektorraum K^n werden weiterhin hauptsächlich mit kleinen griechischen Buchstaben bezeichnet.

Für ein Tupel von Vektoren $(y_1, \ldots, y_n)$ aus K^m werden wir uns gelegentlich mit derselben Schreibweise $(y_1, \ldots, y_n)$ auf die Matrix beziehen, die in der i-ten Zeile und der j-ten Spalte den i-ten Eintrag von y_j stehen hat für $i \in [1, m]$ und $j \in [1, n]$. D.h. $(y_1, \ldots, y_n)$ bezeichnet zugleich auch die Matrix, die aus diesem Vektorentupel durch Nebeneinanderschreiben hervorgeht.

3.1.2 Matrixmultiplikation

Seien $m, n, r, s \geqslant 1$. Wir haben eine Multiplikationsabbildung

$$\begin{array}{rcl} K^{m\times n} \times K^{n\times r} & \xrightarrow{(\cdot)} & K^{m\times r} \\ (A = (a_{i,j})_{i,j},\ B = (b_{j,k})_{j,k}) & \longmapsto & A \cdot B \ = \ AB \ := \ (\sum_{j\in[1,n]} a_{i,j} b_{j,k})_{i,k} \end{array}$$

Das neutrale Element der Addition in $K^{m\times n}$, namentlich die Matrix mit nur Nulleinträgen, heißt auch die *Nullmatrix* $0 = 0_{m,n}$.

Wir definieren für $n \geqslant 1$ die *Einheitsmatrix* durch $E = E_n := (a_{i,j})_{i,j} \in K^{n\times n}$ mit $a_{i,j} = 1$ für $i = j$ und $a_{i,j} = 0$ für $i \neq j$, wobei $i, j \in [1, n]$. In anderen Worten,

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

Für $A, A' \in K^{m\times n}$, $B, B' \in K^{n\times r}$ und $C \in K^{r\times s}$ gelten die folgenden Regeln.

$$\begin{array}{rcl} (A \cdot B) \cdot C & = & A \cdot (B \cdot C) \\ (A + A') \cdot (B + B') & = & AB + A'B + AB' + A'B' \\ A \cdot E_n & = & A \\ E_m \cdot A & = & A \end{array}$$

Zum Beispiel gilt die Assoziativität wegen

$$(AB)C \ = \ \left(\sum_{j\in[1,n],\ k\in[1,r]} a_{i,j} b_{j,k} c_{k,l} \right)_{i,l} \ = \ A(BC) \ ,$$

wobei $A = (a_{i,j})_{i,j}$, $B = (b_{j,k})_{j,k}$ und $C = (c_{k,l})_{k,l}$.

Insbesondere bildet $K^{n\times n}$ einen Ring, mit multiplikativ neutralem Element E_n.

Wir schreiben $\mathrm{GL}_n(K) := \mathrm{Inv}(K^{n\times n})$.

Beispiel. Es ist $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{smallmatrix}\right)$. So ist etwa $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, während $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Der Ring $K^{2\times 2}$ ist also nicht kommutativ. Ferner ist $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)^2 = 0$, während $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \neq 0$.

Ein Vektor $x \in K^n$ kann nun vermittels einer Identifikation $K^n = K^{n\times 1}$ als $n \times 1$-Matrix aufgefaßt werden. Auf diese Weise erhalten wir auch eine Produktverknüpfung

$$\begin{array}{rcl} K^{m\times n} \times K^n & \xrightarrow{(\cdot)} & K^m \\ (A, x) & \longmapsto & A \cdot x \;=\; Ax \end{array}$$

mit den entsprechenden Eigenschaften.

3.1.3 Transposition

Die *transponierte Matrix* $A^{\mathrm{t}} \in K^{n\times m}$ einer Matrix $A \in K^{m\times n}$ geht aus A durch Spiegelung an der Diagonalen hervor. Genauer, ist $A = (a_{i,j})_{i\in[1,m],j\in[1,n]}$, so ist $A^{\mathrm{t}} = (a_{i,j})_{j\in[1,n],i\in[1,m]}$. Für $A, A' \in K^{m\times n}$, $B \in K^{n\times s}$ und $\lambda, \lambda' \in K$ gelten die Regeln

$$\begin{array}{rcl} (A^{\mathrm{t}})^{\mathrm{t}} & = & A \\ (\lambda A + \lambda' A')^{\mathrm{t}} & = & \lambda A^{\mathrm{t}} + \lambda' A'^{\mathrm{t}} \\ (AB)^{\mathrm{t}} & = & B^{\mathrm{t}} A^{\mathrm{t}} \;. \end{array}$$

Beispiel. Ist $A = \left(\begin{smallmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{smallmatrix}\right)$, so ist $A^{\mathrm{t}} = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 3 \\ 4 & 9 \end{smallmatrix}\right)$.

3.2 Lineare Abbildungen und Matrizen

Wir werden lineare Abbildungen als Matrizen beschreiben, um Eigenschaften von linearen Abbildungen anhand dieser Matrizen studieren zu können.

3.2.1 Beschreibende Matrizen

Sei V ein Vektorraum mit Basis $\underline{y} = (y_1, \ldots, y_n)$, sei W ein Vektorraum mit Basis $\underline{z} = (z_1, \ldots, z_m)$ und sei

$$V \xrightarrow{f} W$$

eine lineare Abbildung. Wir definieren die *beschreibende* (oder *darstellende*) Matrix

$$A(f)_{\underline{z},\underline{y}} \;=\; (a_{i,j})_{i,j} \;\in\; K^{m\times n}$$

von f bezüglich $\underline{y}$ und $\underline{z}$ mittels

$$(*) \qquad f(y_j) \;=\; \sum_{i\in[1,m]} z_i a_{i,j}$$

für $j \in [1, n]$ (wozu wir die Skalarmultiplikation rechts notieren). Dies ist möglich, da die Koeffizienten $a_{i,j}$ wegen $\underline{z}$ Basis eindeutig festliegen. So finden wir etwa $A(1_V)_{\underline{y},\underline{y}} = E_n$.

Umgekehrt definiert jede Matrix $A \in K^{m\times n}$ via $(*)$ eine lineare Abbildung. Auf diese Weise vermitteln die Basen $\underline{y}$ und $\underline{z}$ eine Bijektion

$$\begin{array}{rcl} \mathrm{Lin}(V,W) & \xrightarrow{\sim} & K^{m\times n} \\ f & \longmapsto & A(f)_{\underline{z},\underline{y}}\ , \end{array}$$

die dazuhin linear ist, d.h. es ist $A(\mu f + \mu' f')_{\underline{z},\underline{y}} = \mu A(f)_{\underline{z},\underline{y}} + \mu' A(f')_{\underline{z},\underline{y}}$ für $\mu,\mu' \in K$ und $f, f' \in \mathrm{Lin}(V,W)$. Aus diesem Isomorphismus können wir etwa $\dim \mathrm{Lin}(V,W) = \dim V \cdot \dim W$ ersehen.

Satz 7 *Sei U ein Vektorraum mit Basis $\underline{x} = (x_1,\ldots,x_r)$, sei V ein Vektorraum mit Basis $\underline{y} = (y_1,\ldots,y_n)$, sei W ein Vektorraum mit Basis $\underline{z} = (z_1,\ldots,z_m)$, und seien lineare Abbildungen*

$$U \xrightarrow{g} V \xrightarrow{f} W$$

gegeben. Dann ist

$$A(f\circ g)_{\underline{z},\underline{x}} \;=\; \underbrace{A(f)_{\underline{z},\underline{y}}}_{\in K^{m\times n}} \cdot \underbrace{A(g)_{\underline{y},\underline{x}}}_{\in K^{n\times r}}\ .$$

In anderen Worten, die Komposition ist gegeben durch Matrixmultiplikation.

Beweis. Wir schreiben $A(g)_{\underline{y},\underline{x}} = (a'_{j,k})_{j,k}$, $A(f)_{\underline{z},\underline{y}} = (a_{i,j})_{i,j}$ und berechnen den Eintrag an Position (i,k) der Matrix der linken Seite, wobei $i \in [1,m]$ und $k \in [1,r]$. Nach $(*)$ ergibt sich dieser Eintrag aus

$$\begin{array}{rcl} (f\circ g)(x_k) & = & f\left(\sum_{j\in[1,n]} y_j a'_{j,k}\right) \\ & = & \sum_{j\in[1,n]} f(y_j) a'_{j,k} \\ & = & \sum_{j\in[1,n]} \left(\sum_{i\in[1,m]} z_i a_{i,j}\right) a'_{j,k} \\ & = & \sum_{i\in[1,m]} z_i \left(\sum_{j\in[1,n]} a_{i,j} a'_{j,k}\right)\ , \end{array}$$

zu $\sum_{j\in[1,n]} a_{i,j}a'_{j,k}$, was mit dem Eintrag an Position (i,k) der Matrix der rechten Seite übereinstimmt. □

Bemerkung. Nun kann man die Assoziativität der Komposition dazu verwenden, um die Assoziativität der Matrixmultiplikation erneut zu zeigen; und analog die anderen oben angeführten Regeln.

Bemerkung. Insbesondere kann man auf diese Weise nach Wahl einer Basis $\underline{y}$ von V die Ringe $\mathrm{End}(V)$ und $K^{n\times n}$ identifizieren, da sich die Bijektion $f \longmapsto A(f)_{\underline{y},\underline{y}}$ nicht nur mit Linearkombinationen, sondern auch noch mit der Ringmultiplikation verträgt wie in Satz 7 beschrieben.

Bemerkung. Bezüglich der Standardbasen $\underline{e}$ von K^n und $\underline{e}$ von K^m ist für $A \in K^{m\times n}$ die beschreibende Matrix der linearen Abbildung $f : K^n \longrightarrow K^m$, $x \longmapsto Ax$, gegeben durch $A(f)_{\underline{e},\underline{e}} = A$.

Lemma (Folgerung aus Satz 5.)

Sei $A(f)_{\underline{z},\underline{y}} = (a_{i,j})_{i,j}$ die beschreibende Matrix von $V \xrightarrow{f} W$.

(i) *Die Abbildung f ist injektiv genau dann, wenn das Tupel der Spaltenvektoren* $(a_{*,1}, a_{*,2}, \ldots, a_{*,n})$ *in K^m linear unabhängig ist.*

(ii) *Die Abbildung f ist surjektiv genau dann, wenn das Tupel der Spaltenvektoren* $(a_{*,1}, a_{*,2}, \ldots, a_{*,n})$ *in K^m erzeugend ist.*

(iii) *Die Abbildung f ist bijektiv genau dann, wenn das Tupel der Spaltenvektoren* $(a_{*,1}, a_{*,2}, \ldots, a_{*,n})$ *eine Basis von K^m bildet. Insbesondere ist dann $n = m$.*

Beweis. Dies ist eine Konsequenz aus Satz 5, da $f(y_j) = \sum_{i \in [1,m]} z_i a_{i,j}$ unter dem Isomorphismus $W \xrightarrow{\sim} K^m : z_i \longmapsto e_i$ auf $a_{*,j}$ kommt, und also $(f(y_1), \ldots, f(y_n))$ genau dann linear unabhängig bzw. erzeugend ist, wenn dies für das Bildtupel $(a_{*,1}, \ldots, a_{*,n})$ gilt. □

Beispiel. Die Matrix $A = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \end{smallmatrix}\right) \in \mathbf{R}^{2\times 3}$ beschreibt eine surjektive, aber nicht injektive Abbildung. Bezüglich der Standardbasen bedeutet dies ausgeschrieben, daß die Abbildung

$$\mathbf{R}^3 \longrightarrow \mathbf{R}^2 \;:\; \left(\begin{smallmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{smallmatrix}\right) \;\longmapsto\; \left(\begin{smallmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} \eta_1 + \eta_3 \\ 2\eta_1 + \eta_2 + 3\eta_3 \end{smallmatrix}\right)$$

surjektiv, aber nicht injektiv ist. So schickt sie etwa $\left(\begin{smallmatrix} 1 \\ 1 \\ -1 \end{smallmatrix}\right)$ auf $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$.

Bemerkung. Sei $n \geqslant 1$. Die Bijektion $\operatorname{End} K^n \xrightarrow{\sim} K^{n\times n}$ schränkt ein auf den bijektiven Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{GL}(K^n) & \xrightarrow{\sim} & \mathrm{GL}_n(K) \\ f & \longmapsto & A(f)_{\underline{e},\underline{e}} \\ (x \longmapsto Ax) & \longleftarrow\!\!\shortmid & A\,, \end{array}$$

da die Invertierbarkeit eines Endomorphismus f in $\operatorname{End} V$ mit Satz 7 die Invertierbarkeit von $A(f)_{\underline{e},\underline{e}}$ nach sich zieht, und da umgekehrt aus $AB = BA = E$ folgt, daß $(x \longmapsto Ax)$ von $(x \longmapsto Bx)$ beidseitig invertiert wird.

Es ist eine Matrix $A = (a_{i,j})_{i,j}$ also genau dann invertierbar, wenn die Abbildung $x \longmapsto Ax$ invertierbar ist, und das ist mit vorstehendem Lemma genau dann der Fall, wenn ihr Spaltentupel $(a_{*,1}, \ldots, a_{*,n})$ linear unabhängig ist.

Sei $A \in K^{n\times n}$ gegeben. Der Bijektion entnehmen wir, daß für $B \in K^{n\times n}$ genau dann $AB = E$ ist, wenn $BA = E$ ist. Denn bezeichnen wir $f_A : x \longmapsto Ax$, so ist $f_{AB} = f_A \circ f_B = f_E = 1_{K^n}$ genau dann, wenn $f_{BA} = f_B \circ f_A = f_E = 1_{K^n}$ ist. Wir bezeichnen dann diese *inverse Matrix* mit $A^{-1} := B$ und werden uns später noch mit ihrer praktischen Berechnung beschäftigen.

Matrizen in $\mathrm{GL}_n(K)$ heißen auch *regulär*, Matrizen in $K^{n\times n} \smallsetminus \mathrm{GL}_n(K)$ heißen auch *singulär.* Es ist für $A = (a_{i,j})_{i,j} \in K^{n\times n}$ mithin:

$$A \text{ regulär} \iff A \text{ invertierbar} \iff A \in \mathrm{GL}_n(K) \iff (a_{*,1}, \ldots, a_{*,n}) \text{ l. u.}$$

Beispiel. Sei $K = \mathbf{R}$ und $n = 2$. Es ist $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ regulär, und $\left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$ singulär.

Beispiel. Ist $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K^{2\times 2}$, und ist $ad - bc \neq 0$, so ist $A^{-1} = \frac{1}{ad-bc} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, wie man anhand von $AA^{-1} = E$ oder von $A^{-1}A = E$ verifiziert.

Bemerkung. Wir hatten im letzten Kapitel einen Gruppenmorphismus $\mathcal{S}_n \xrightarrow{\pi} \mathrm{GL}(K^n)$ definiert. Wir bezeichnen nun für $\sigma \in \mathcal{S}_n$ die das Element $\pi(\sigma)$ bezüglich der Standardbasen beschreibende Matrix mißbräuchlich ebenfalls wieder mit $\pi(\sigma) := A(\pi(\sigma))_{\underline{e},\underline{e}} \in \mathrm{GL}_n(K)$. Ausgeschrieben hat $\pi(\sigma)$ an den Positionen $(\sigma(j), j)$ für alle $j \in [1, n]$ einen Eintrag 1, und an allen übrigen Positionen einen Eintrag 0. Etwa erhalten wir für $(1, 2, 3) \in \mathcal{S}_3$ die Matrix $\pi((1, 2, 3)) = \begin{pmatrix} 0&0&1 \\ 1&0&0 \\ 0&1&0 \end{pmatrix} \in \mathrm{GL}_3(K)$. Allgemein gilt $\pi(\sigma \circ \rho) = \pi(\sigma) \cdot \pi(\rho)$ für $\sigma, \rho \in \mathcal{S}_n$. Eine Matrix der Form $\pi(\sigma)$ für ein $\sigma \in \mathcal{S}_n$ heißt auch *Permutationsmatrix.*

3.2.2 Basiswechsel

Wir behalten die Bezeichnungen des vorigen Abschnitts bei. Sei $\underline{y'} = (y'_1, \ldots, y'_n)$ eine weitere Basis von V und sei $\underline{z'} = (z'_1, \ldots, z'_m)$ eine weitere Basis von W. Es stellt sich die Frage, wie die beschreibende Matrix $A(f)_{\underline{z'},\underline{y'}}$ bezüglich der Basen $\underline{y'}$ und $\underline{z'}$ aus der beschreibenden Matrix $A(f)_{\underline{z},\underline{y}}$ bezüglich der Basen $\underline{y}$ und $\underline{z}$ hervorgeht.

Basiswechsellemma. *Es ist*

$$A(f)_{\underline{z'},\underline{y'}} \;=\; A(1_W)_{\underline{z'},\underline{z}} \cdot A(f)_{\underline{z},\underline{y}} \cdot A(1_V)_{\underline{y},\underline{y'}} \;.$$

Beweis. Das ist eine zweimalige Anwendung von Satz 7. ▫

Beispiel. Sei $K = \mathbf{R}$, sei $V = \mathbf{R}^2$, sei $W = \mathbf{R}^3$, und sei $f : \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} \longmapsto \begin{pmatrix} \eta_2 \\ \eta_1+\eta_2 \\ \eta_1-\eta_2 \end{pmatrix}$. Bezüglich der Standardbasen $\underline{y} := \underline{e}$ von V und $\underline{z} := \underline{e}$ von W erhalten wir also $A(f)_{\underline{z},\underline{y}} = \begin{pmatrix} 0&1 \\ 1&1 \\ 1&-1 \end{pmatrix}$. Sei nun $\underline{y'} = (\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix})$ eine weitere Basis von V, und sei $\underline{z'} = (\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix})$ eine weitere Basis von W. Wir sehen direkt, daß

$$\begin{array}{rclcrcrcr} f(\begin{pmatrix} 1 \\ 2 \end{pmatrix}) &=& \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} &=& (-1) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &+& 3 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &+& 0 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \\ f(\begin{pmatrix} -1 \\ 1 \end{pmatrix}) &=& \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix} &=& (-1/2) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &+& 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &+& 3/2 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \end{array}$$

d.h. $A(f)_{\underline{z'},\underline{y'}} = \begin{pmatrix} -1&-1/2 \\ 3&0 \\ 0&3/2 \end{pmatrix}$. Berechnen wir dies nun über das Basiswechsellemma. Wegen

$$\begin{array}{rclcrcr} 1_V(\begin{pmatrix} 1 \\ 2 \end{pmatrix}) &=& \begin{pmatrix} 1 \\ 2 \end{pmatrix} &=& 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &+& 2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1_V(\begin{pmatrix} -1 \\ 1 \end{pmatrix}) &=& \begin{pmatrix} -1 \\ 1 \end{pmatrix} &=& (-1) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &+& 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array}$$

ist $A(1_V)_{\underline{y},\underline{y'}} = \begin{pmatrix} 1&-1 \\ 2&1 \end{pmatrix}$. Wegen

$$\begin{array}{rclcrcrcr} 1_W(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}) &=& \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} &=& 1/2 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &+& 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &+& 1/2 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \\ 1_W(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}) &=& \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} &=& (-1/2) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &+& 1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &+& (-1/2) \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \\ 1_W(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}) &=& \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} &=& 1/2 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &+& 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &+& (-1/2) \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \end{array}$$

ist $A(1_W)_{\underline{z}',\underline{z}} = \begin{pmatrix} 1/2 & -1/2 & 1/2 \\ 0 & 1 & 0 \\ 1/2 & -1/2 & -1/2 \end{pmatrix}$. In der Tat ist nun

$$\begin{array}{rcl} A(1_W)_{\underline{z}',\underline{z}} \cdot A(f)_{\underline{z},\underline{y}} \cdot A(1_V)_{\underline{y},\underline{y}'} & = & \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 0 \\ 1 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \\ & = & \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 0 \\ 1 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 3 & 0 \\ -1 & -2 \end{pmatrix} \\ & = & \frac{1}{2}\begin{pmatrix} -2 & -1 \\ 6 & 0 \\ 0 & 3 \end{pmatrix} \;=\; A(f)_{\underline{z}',\underline{y}'} \,. \end{array}$$

3.3 Lineare Gleichungssysteme

3.3.1 Berechnung der Zeilenstufenform – Gaußscher Algorithmus

Wir werden folgende Typen von Matrizen als operierende Matrizen verwenden.

Elementarmatrizen. Sei $m \geqslant 1$, seien $k, l \in [1, m]$ mit $k \neq l$ und sei $\eta \in K$. Sei die Matrix $E_{k,l}(\eta) = (a_{i,j})_{i,j} \in \mathrm{GL}_m(K)$ gegeben durch $a_{k,l} = \eta$, durch $a_{i,i} = 1$ für $i \in [1, m]$ und durch $a_{i,j} = 0$ falls $i \neq j$ und $(i, j) \neq (k, l)$. D.h. $E_{k,l}(\eta)$ ist konstant 1 auf der Diagonalen, hat noch einen Nebendiagonaleintrag η bei (k, l), und ansonsten Null. Matrizen der Form $E_{k,l}(\eta)$ heißen auch *Elementarmatrizen.*

Diagonalmatrizen. Eine Matrix $A = (a_{i,j})_{i,j} \in K^{m\times m}$ mit $a_{i,j} = 0$ für $i \neq j$ heißt *Diagonalmatrix.* Wir schreiben auch $A = \mathrm{diag}(a_{1,1}, a_{2,2}, \ldots , a_{m,m})$. Beachte, daß

$$\mathrm{diag}(a_{1,1}, \ldots , a_{m,m}) \cdot \mathrm{diag}(b_{1,1}, \ldots , b_{m,m}) \;=\; \mathrm{diag}(a_{1,1}b_{1,1}, \ldots , a_{m,m}b_{m,m}) \,.$$

Insbesondere ist $\mathrm{diag}(a_{1,1}, \ldots , a_{m,m})$ invertierbar genau dann, wenn $a_{i,i} \neq 0$ für alle $i \in [1, m]$.

Permutationsmatrizen von der Form $\pi(\sigma) \in \mathrm{GL}_m(K)$ für ein $\sigma \in \mathcal{S}_m$.

Zeilenstufenform. Seien $m, n \geqslant 1$. Eine Matrix $A = (a_{i,j})_{i,j} \in K^{m\times n}$ ist *in Zeilenstufenform,* falls es *ausgewählte Spaltenindizes*

$$1 \;\leqslant\; k_1 \;<\; k_2 \;<\; \cdots \;<\; k_l \;\leqslant\; n$$

mit $l \in [0, m]$ so gibt, daß (Z 1, 2) gelten. Wir setzen dazu formal noch $k_i := n + 1$ für $i \in [l + 1, m]$.

(Z 1) Für $i \in [1, m]$ und $j \in [1, n]$ mit $j < k_i$ ist $a_{i,j} = 0$.

(Z 2) Für $t \in [1, l]$ ist $a_{t,k_t} = 1$ und $a_{i,k_t} = 0$ für $i \in [1, m] \smallsetminus \{t\}$.

D.h. in den Spalten k_t steht in Zeile t eine 1, sonst 0. Und ansonsten ist jeder Eintrag links von einer solchen 1 oder in Zeile $\geqslant l + 1$ gleich 0.

Beispiel. Die Nullmatrix $0_{m,n}$ ist in Zeilenstufenform. Die Einheitsmatrix E_n ist in Zeilenstufenform; sie ist die einzige Matrix in $\mathrm{GL}_n(K)$ in Zeilenstufenform.

Beispiel. Die Matrix

$$A = \begin{pmatrix} 0&1&*&0&0&*&0 \\ 0&0&0&1&0&*&0 \\ 0&0&0&0&1&*&0 \\ 0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0 \end{pmatrix} \in \mathbf{R}^{5\times 7}$$

ist mit beliebigen Einträgen an den mit $*$ markierten Positionen in Zeilenstufenform. Es sind $k_1 = 2$, $k_2 = 4$, $k_3 = 5$ und $k_4 = 7$.

Das wesentliche am folgenden Satz ist das in seinem Beweis dargelegte Verfahren, auch *Gaußscher Algorithmus* genannt.

Satz 8 *Sei $m, n \geqslant 1$, und sei $A \in K^{m\times n}$ gegeben. Es gibt eine Matrix $G \in \mathrm{GL}_m(K)$, die sich als Produkt von Elementarmatrizen, Permutationsmatrizen und invertierbaren Diagonalmatrizen (in gemischter Anordnung der Faktoren) schreiben läßt, dergestalt, daß $G \cdot A$ Zeilenstufenform hat.*

Beweis. Multiplikation mit einer Permutationsmatrix von links bewirkt eine Zeilenvertauschung in A. Multiplikation mit einer Elementarmatrix $E_{k,l}(\eta)$ von links bewirkt die Addition des η-fachen der l-ten Zeile von A zur k-ten Zeile von A. Multiplikation mit einer invertierbaren Diagonalmatrix $\mathrm{diag}(d_1, \ldots, d_m)$ von links bewirkt die Multiplikation der i-ten Zeile von A mit d_i für alle i. Im folgenden werden wir diese drei Arten von Zeilenoperationen anwenden, angedeutet durch P, E, D. Das Produkt der dafür benötigten Matrizen, mit dem ersten Matrixfaktor rechts und dem letzten Matrixfaktor links, ergibt dann die gesuchte Matrix G.

Starte mit der Matrix A.

Sei k_1 der Index der ersten Spalte von links, in welcher in den Zeilen $[1, m]$ ein Eintrag ungleich Null steht – so vorhanden, ansonsten breche ab. Multipliziere diese Zeile mit dem Inversen dieses Eintrags (D). Tausche diese Zeile in die erste Zeile (P). Subtrahiere die erste Zeile, multipliziert mit dem Eintrag an Position (i, k_1), von der i-ten Zeile für alle $i \in [1, n] \smallsetminus \{1\}$ (E). Wir erhalten eine Matrix, in welcher links von Spalte k_1 bereits (Z 1) und in Spalte k_1 bereits (Z 2) gilt.

Sei k_2 der Index der ersten Spalte von links, in welcher in den Zeilen $[2, m]$ ein Eintrag ungleich Null steht – so vorhanden, ansonsten breche ab. Multipliziere diese Zeile mit dem Inversen dieses Eintrags (D). Tausche diese Zeile in die zweite Zeile (P). Subtrahiere die zweite Zeile, multipliziert mit dem Eintrag an Position (i, k_2), von der i-ten Zeile für alle $i \in [1, n] \smallsetminus \{2\}$ (E). Wir erhalten eine Matrix, in welcher links von Spalte k_2 bereits (Z 1) und in den Spalten k_1, k_2 bereits (Z 2) gilt.

Setze das Verfahren fort. Es bricht spätestens bei der Suche nach dem Index k_{m+1} ab, ohne einen solchen zu finden.

Es wird so $1 \leqslant k_1 < \cdots < k_l \leqslant n$, wenn k_l der letzte so gefundene Spaltenindex ist. Hierbei ist $l \in [0, m]$ (wobei $l = 0$ schlicht die Abwesenheit von Nichtnulleinträgen in A signalisiert, d.h. in der Nullmatrix finden wir überhaupt keinen solchen Spaltenindex k_t).$\square$

Beispiel. Sei

$$A = \begin{pmatrix} 0&0&0&2 \\ 0&2&1&4 \\ 0&2&1&8 \end{pmatrix} \in \mathbf{R}^{3\times 4} .$$

Es ist $k_1 = 2$. Multiplikation von links mit $\operatorname{diag}(1, 1/2, 1) = \begin{pmatrix} 1&0&0 \\ 0&1/2&0 \\ 0&0&1 \end{pmatrix}$, dann mit $\pi((1, 2)) = \begin{pmatrix} 0&1&0 \\ 1&0&0 \\ 0&0&1 \end{pmatrix}$ und dann mit $E_{3,1}(-2) = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ -2&0&1 \end{pmatrix}$ liefert

$$\begin{pmatrix} 0&1&1/2&2 \\ 0&0&0&2 \\ 0&0&0&4 \end{pmatrix} .$$

Somit ist $k_2 = 4$. Multiplikation von links mit $\operatorname{diag}(1, 1/2, 1) = \begin{pmatrix} 1&0&0 \\ 0&1/2&0 \\ 0&0&1 \end{pmatrix}$, mit $\pi(1) = E$, mit $E_{3,2}(-4) = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&-4&1 \end{pmatrix}$ und mit $E_{1,2}(-2) = \begin{pmatrix} 1&-2&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}$ liefert

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

Hier bricht der Algorithmus ab, die Matrix ist in Zeilenstufenform. Wir erhalten

$$G = \begin{pmatrix} 1&-2&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&-4&1 \end{pmatrix} \begin{pmatrix} 1&0&0 \\ 0&1/2&0 \\ 0&0&1 \end{pmatrix} \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ -2&0&1 \end{pmatrix} \begin{pmatrix} 0&1&0 \\ 1&0&0 \\ 0&0&1 \end{pmatrix} \begin{pmatrix} 1&0&0 \\ 0&1/2&0 \\ 0&0&1 \end{pmatrix} = \begin{pmatrix} -1&1/2&0 \\ 1/2&0&0 \\ -2&-1&1 \end{pmatrix} .$$

Bemerkung. Es folgt insbesondere, daß jede Matrix in $\operatorname{GL}_n(K)$ ein Produkt von Elementarmatrizen, invertierbaren Diagonalmatrizen und Permutationsmatrizen ist. Wegen

$$\begin{pmatrix} 0&1 \\ 1&0 \end{pmatrix} = E_{1,2}(1) E_{2,1}(-1) E_{1,2}(1) \operatorname{diag}(-1, 1)$$

können hierbei die Permutationsmatrizen hierbei auch weggelassen werden.

3.3.2 Lösungsverfahren

Sei eine Matrix $A = (a_{i,j})_{i,j} \in K^{m\times n}$ und ein Vektor $b = (\vartheta_i)_i = \begin{pmatrix} \vartheta_1 \\ \vdots \\ \vartheta_m \end{pmatrix} \in K^m$ vorgegeben. Gesucht ist die Menge

$$\{x \in K^n \mid A \cdot x = b\} .$$

Wir spalten das Problem in zwei Teilprobleme. Hat man eine *Partikulärlösung* x_0 mit $Ax_0 = b$ gefunden, so gilt für jedes x mit $Ax = b$ für die Differenz $A(x - x_0) = 0$. Umgekehrt, ist $Ax_1 = 0$, so ist $A(x_0 + x_1) = b$. Kurz,

$$\{x \in K^n \mid A \cdot x = b\} = x_0 + \{x_1 \in K^n \mid A \cdot x_1 = 0\} .$$

Wir suchen also zuerst eine solche Partikulärlösung $x_0 \in K^n$ mit $A \cdot x_0 = b$ und dann die allgemeine Lösung x_1 der zugehörigen *homogenen Gleichung* $A \cdot x_1 = 0$.

3.3.2.1 Partikulärlösung

Mit Satz 8 dürfen wir A in Zeilenstufenform annehmen, mit ausgewählten Spalten $1 \leqslant k_1 < \cdots < k_l \leqslant n$. In der Praxis heißt dies, man forme zunächst A in Zeilenstufenform um und führe dabei sämtliche Umformungen simultan für b durch. In anderen Worten, man multipliziert beide Seiten der Gleichung von links mit der invertierbaren Matrix G, um zunächst diese Form zu erreichen.

Fall I. Es gibt ein $i \in [l+1, m]$ mit $\vartheta_i \neq 0$. Dann ist $Ax = b$ unlösbar, d.h.

$$\{x \in K^n \mid Ax = b\} \; = \; \emptyset \; .$$

Fall II. Es ist für alle $i \in [l+1, m]$ der Eintrag $\vartheta_i = 0$. Schreibe $x_0 = (\xi_i)_i$ und wähle

$$\xi_{k_t} \; := \; \vartheta_t$$

für $t \in [1, l]$, und die sonstigen Einträge von x_0 zu Null (positives Einfüllen). Wegen der Gestalt von A ist dann $Ax_0 = b$, d.h. x_0 ist eine Partikulärlösung.

3.3.2.2 Allgemeine homogene Lösung

Wir suchen nun die allgemeine Lösung für die zugehörige homogene Gleichung $Ax_1 = 0$. Mit Satz 8 dürfen wir A in Zeilenstufenform annehmen. In der Praxis hat man an dieser Stelle die dazu notwendigen Umformungen bereits für die Partikulärlösung durchgeführt.

Durchlaufe nun $1 \leqslant k'_1 < k'_2 < \cdots < k'_{n-l} \leqslant n$ die Indizes der *nicht* ausgewählten Spalten.

Wir wollen für jedes $u \in [1, n-l]$ eine Lösung $x_{1;u} \in K^n$ konstruieren, und setzen dazu $x_{1;u} = (\xi_i)_i$ an. Wähle $\xi_{k'_u} = 1$, wähle $\xi_{k'_t} = 0$ für $t \in [1, n-l] \smallsetminus \{u\}$, und wähle $\xi_{k_t} := -a_{t,k'_u}$ für $t \in [1, l]$ (negatives Einfüllen). Wegen der Gestalt von A ist in der Tat $Ax_{1;u} = 0$. Ferner ist das Tupel $(x_{1;u} \mid u \in [1, n-l])$ linear unabhängig, wie man an den Einträgen an den Positionen $k'_1, \ldots, k'_{n-l}$ erkennt.

Sei $f : K^n \longrightarrow K^m : x \longmapsto Ax$. Aus $\dim \operatorname{Im} f = l$ folgt mit Satz 6, daß $\dim \operatorname{Kern} f = n - l$. Also ist $(x_{1;u} \mid u \in [1, n-l])$ eine Basis des Kerns. In anderen Worten, jede Lösung x_1 der Gleichung $Ax_1 = 0$ läßt sich (mit eindeutigen Koeffizienten) als Linearkombination in $(x_{1;u} \mid u \in [1, n-l])$ schreiben.

3.3.2.3 Allgemeine Lösung

Ist x_0 eine Partikulärlösung $Ax_0 = b$, so ist die allgemeine Lösung von $Ax = b$ gegeben als Summe von x_0 und der allgemeinen Lösung x_1 der zugehörigen homogenen Gleichung $Ax_1 = 0$. Genauer, es ist wie eingangs erwähnt

$$\{x \in K^n \mid Ax = b\} \; = \; x_0 + \{x_1 \in K^n \mid Ax_1 = 0\} \; = \; x_0 + \langle x_{1;1}, \ldots, x_{1;n-l} \rangle \; .$$

3.3.2.4 Beispiel

Seien $K = \mathbf{R}$, $m = 4$, $n = 8$ und

$$A \;=\; \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 4 & 0 & 6 \\ 0 & -1 & -2 & -3 & 1 & 1 & 1 & 9 \\ 0 & 1 & 2 & 3 & 0 & 4 & 1 & 14 \\ 0 & -1 & -2 & -3 & -1 & -9 & -3 & -37 \end{pmatrix} \;\in\; \mathbf{R}^{4\times 8}\;.$$

Sei $b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, sei $c = \begin{pmatrix} 9 \\ 12 \\ 20 \\ 52 \end{pmatrix}$. Gesucht seien $\{x \in \mathbf{R}^8 \mid Ax = b\}$ und $\{x \in \mathbf{R}^8 \mid Ax = c\}$.

Wir notieren bei der Umformung die Matrix neben den mitzuführenden Vektoren, d.h. wir formen

$$(A\,|\,b\,|\,c) \;=\; \left(\begin{array}{rrrrrrrr|r|r} 0 & 1 & 2 & 3 & 0 & 4 & 0 & 6 & 1 & 9 \\ 0 & -1 & -2 & -3 & 1 & 1 & 1 & 9 & 1 & 12 \\ 0 & 1 & 2 & 3 & 0 & 4 & 1 & 14 & 0 & 20 \\ 0 & -1 & -2 & -3 & -1 & -9 & -3 & -37 & 0 & -52 \end{array}\right)$$

simultan um zu

$$\left(\begin{array}{rrrrrrrr|r|r} 0 & 1 & 2 & 3 & 0 & 4 & 0 & 6 & 1 & 9 \\ 0 & 0 & 0 & 0 & 1 & 5 & 0 & 7 & 1 & 10 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8 & -1 & 11 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

Wir haben also die ausgewählten Spalten $k_1 = 2$, $k_2 = 5$ und $k_3 = 7$.

Und wir haben die nichtausgewählten Spalten $k'_1 = 1$, $k'_2 = 3$, $k'_3 = 4$, $k'_4 = 6$ und $k'_5 = 8$.

Bezüglich b sind wir in Fall I, da eine Nullzeile auf einen nichtverschwindenden Eintrag des Vektors trifft, und wir erhalten $\{x \in \mathbf{R}^8 \mid Ax = b\} = \emptyset$.

Berechnen wir nun $\{x \in \mathbf{R}^8 \mid Ax = c\}$.

Wir erhalten durch positives Einfüllen die Partikulärlösung $x_0 = \begin{pmatrix} 0 \\ 9 \\ 0 \\ 0 \\ 10 \\ 0 \\ 11 \\ 0 \end{pmatrix}$.

Für den Vektor $x_{1;1}$ setzen wir in Position $k'_1 = 1$ eine 1, an die übrigen nichtausgewählten Positionen eine 0 und erhalten durch negatives Einfüllen der 1ten Spalte $x_{1;1} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Für den Vektor $x_{1;2}$ setzen wir in Position $k'_2 = 3$ eine 1, an die übrigen nichtausgewählten Positionen eine 0 und erhalten durch negatives Einfüllen der 3ten Spalte $x_{1;2} = \begin{pmatrix} 0 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Für den Vektor $x_{1;3}$ setzen wir in Position $k'_3 = 4$ eine 1, an die übrigen nichtausgewählten Positionen eine 0 und erhalten durch negatives Einfüllen der 4ten Spalte $x_{1;3} = \begin{pmatrix} 0 \\ -3 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Für den Vektor $x_{1;4}$ setzen wir in Position $k'_4 = 6$ eine 1, an die übrigen nichtausgewählten Positionen eine 0 und erhalten durch negatives Einfüllen der 6ten Spalte $x_{1;4} = \begin{pmatrix} 0 \\ -4 \\ 0 \\ 0 \\ -5 \\ 1 \\ 0 \\ 0 \end{pmatrix}$.

Für den Vektor $x_{1;5}$ setzen wir in Position $k'_5 = 8$ eine 1, an die übrigen nichtausgewählten Positionen eine 0 und erhalten durch negatives Einfüllen der 8ten Spalte $x_{1;5} = \begin{pmatrix} 0 \\ -6 \\ 0 \\ 0 \\ -7 \\ 0 \\ -8 \\ 1 \end{pmatrix}$.

Insgesamt wird

$$\{x \in \mathbf{R}^8 \mid Ax = c\} \;=\; \begin{pmatrix} 0 \\ 9 \\ 0 \\ 0 \\ 10 \\ 0 \\ 11 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -3 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -4 \\ 0 \\ 0 \\ -5 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -6 \\ 0 \\ 0 \\ -7 \\ 0 \\ -8 \\ 1 \end{pmatrix} \right\rangle .$$

3.3.3 Die inverse Matrix

Sei $n \geqslant 1$, sei $A \in \mathrm{GL}_n(K) \subseteq K^{n\times n}$ und sei nach der Matrix $A^{-1} \in \mathrm{GL}_n(K)$ gefragt, d.h. nach der eindeutigen Lösung von $BA = E$ mit $B \in K^{n\times n}$. Denn daraus folgt, daß auch $AB = E$.

Wir bringen A auf Zeilenstufenform GA vermittels $G \in \mathrm{GL}_n(K)$. Dies bedeutet wegen $A \in \mathrm{GL}_n(K)$ aber gerade, daß $GA = E$, da E die einzige invertierbare Matrix in $K^{n\times n}$ in Zeilenstufenform ist, da jede Matrix in Zeilenstufenform ungleich E linear abhängige Spalten hat. Also haben wir $A^{-1} = G$.

In der Praxis formt man die um die Einheitsmatrix ergänzte Matrix $(A|E)$ so um, daß im linken Teil Zeilenstufenform entsteht, da dann $G(A|E) = (GA|GE) = (E|G) = (E|A^{-1})$.

Hat man dieses Verfahren versehentlich mit einer nichtinvertierbaren Matrix A begonnen, so bemerkt man das daran, daß ihre Zeilenstufenform nicht gleich E wird.

Beispiel. Sei $A = \begin{pmatrix} 1&0&1 \\ 1&2&1 \\ 0&1&1 \end{pmatrix}$. Wir formen

$$(A \,|\, E) \;=\; \left(\begin{array}{ccc|ccc} 1&0&1&1&0&0 \\ 1&2&1&0&1&0 \\ 0&1&1&0&0&1 \end{array}\right)$$

so von links um, daß A Zeilenstufenform erhält. Z.B. kann man wie folgt vorgehen.

$$\left(\begin{array}{ccc|ccc} 1&0&1&1&0&0 \\ 1&2&1&0&1&0 \\ 0&1&1&0&0&1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1&0&1&1&0&0 \\ 0&2&0&-1&1&0 \\ 0&1&1&0&0&1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1&0&1&1&0&0 \\ 0&1&0&-1/2&1/2&0 \\ 0&0&1&1/2&-1/2&1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1&0&0&1/2&1/2&-1 \\ 0&1&0&-1/2&1/2&0 \\ 0&0&1&1/2&-1/2&1 \end{array}\right) .$$

Wir erhalten also $A^{-1} = \begin{pmatrix} 1/2 & 1/2 & -1 \\ -1/2 & 1/2 & 0 \\ 1/2 & -1/2 & 1 \end{pmatrix}$.

Wer hier keine Probe $AA^{-1} = E$ oder $A^{-1}A = E$ macht, dem ist leider nicht zu helfen.

3.3.4 Der Rang einer Matrix

Rang. Seien $m, n \geqslant 1$, sei $A = (a_{i,j})_{i,j} \in K^{m\times n}$, und sei $f : K^n \longrightarrow K^m : x \longmapsto Ax$, so daß $A = A(f)_{\underline{e},\underline{e}}$ die Abbildung f beschreibt. Wir setzen

$$\operatorname{rk} A \;=\; \operatorname{rk}_K A \;:=\; \dim_K \operatorname{Im} f$$

(nach engl. rank = Rang). Wegen $\operatorname{Im} f = \langle a_{*,1}, \dots, a_{*,n}\rangle$ ist

$$\operatorname{rk} A \;=\; \dim \operatorname{Im} f \;=\; \dim\langle a_{*,1}, \dots, a_{*,n}\rangle$$

die maximale Länge eines linear unabhängigen Tupels von Spalten von A. Es ist f surjektiv, falls $\operatorname{rk} A = m$; es ist f injektiv, falls die Spalten von A linear unabhängig sind, d.h. falls $\operatorname{rk} A = n$.

Lemma. *Seien $U \xrightarrow{f} V \xrightarrow{g} W \xrightarrow{h} Y$ lineare Abbildungen zwischen endlichdimensionalen Vektorräumen. Dann ist*

$$\dim \operatorname{Im} g \;\geqslant\; \dim \operatorname{Im}(h \circ g \circ f)\ .$$

Die Gleichheit gilt hier, falls f surjektiv ist und h injektiv ist.

Beweis. Zeigen wir die Ungleichung. Es ist $\operatorname{Im}(h \circ g \circ f) \leqslant \operatorname{Im}(h \circ g)$, zu zeigen bleibt also $\dim \operatorname{Im} g \geqslant \dim \operatorname{Im}(h \circ g)$. Ist $(x_1, \dots, x_k)$ eine Basis von $\operatorname{Im} g \leqslant W$, so erzeugt $(h(x_1), \dots, h(x_k))$ den Unterraum $\operatorname{Im}(h \circ g) \leqslant Y$. Aus letzterem Tupel können wir also eine Basis von $\operatorname{Im}(h \circ g)$ von Länge $\leqslant k = \dim \operatorname{Im} g$ auswählen.

Zeigen wir die Gleichheit, falls f surjektiv und h injektiv ist. In der Tat ist dann im voranstehenden Argument $\operatorname{Im}(h \circ g \circ f) = \operatorname{Im}(h \circ g)$, und $(h(x_1), \dots, h(x_k))$ ist bereits eine Basis von $\operatorname{Im}(h \circ g) \leqslant Y$. $\square$

Lemma. *Seien m, n, s, $t \geqslant 1$ gegeben. Ist $A \in K^{m\times n}$, und sind $B \in K^{s\times m}$ und $C \in K^{n\times t}$, so ist*

$$\operatorname{rk} A \;\geqslant\; \operatorname{rk}(BAC)\ ,$$

mit Gleichheit, falls $\operatorname{rk} B = m$ und $\operatorname{rk} C = n$. Insbesondere liegt Gleichheit vor, falls $B \in \mathrm{GL}_m(K)$ und $C \in \mathrm{GL}_n(K)$.

Beweis. Wir wenden das vorige Lemma an auf

$$\begin{array}{ccccccc}
K^t & \xrightarrow{f} & K^n & \xrightarrow{g} & K^m & \xrightarrow{h} & K^s \\
x & \longmapsto & Cx & & x & \longmapsto & Bx \\
& & x & \longmapsto & Ax & &
\end{array}$$

$\square$

Lemma. *Ist $A \in K^{m\times n}$ und ist $G \in \mathrm{GL}_m(K)$ mit GA in Zeilenstufenform mit ausgewählten Spalten $1 \leqslant k_1 < \dots < k_l \leqslant n$, so ist $\operatorname{rk} A = l$.*

Beweis. Nach vorigem Lemma ist $\operatorname{rk} A = \operatorname{rk}(GA)$. Das Tupel $(\tilde a_{*,k_1}, \dots, \tilde a_{*,k_l})$ der ausgewählten Spalten von $GA = (\tilde a_{i,j})_{i,j}$ ist ein linear unabhängiges Tupel, welches wegen

$\langle \tilde{a}_{*,k_1}, \dots, \tilde{a}_{*,k_l} \rangle = \langle \tilde{a}_{*,1}, \dots, \tilde{a}_{*,n} \rangle$ eine Basis des letztgenannten Erzeugnisses darstellt. Also ist

$$l \;=\; \dim\langle \tilde{a}_{*,1}, \dots, \tilde{a}_{*,n} \rangle \;=\; \operatorname{rk}(GA) \;=\; \operatorname{rk} A\,.$$

□

Beispiel. Die Nullmatrix $0 \in K^{m\times n}$ hat $\operatorname{rk} 0 = 0$. Eine Matrix $A \in K^{n\times n}$ hat $\operatorname{rk} A = n$ genau dann, wenn $A \in \operatorname{GL}_n(K)$.

Lemma. *Ist $A \in K^{m\times n}$, so ist $\operatorname{rk} A = \operatorname{rk} A^{\mathrm{t}}$. In anderen Worten, die maximale Länge eines linear unabhängigen Spaltentupels von A ist gleich der maximalen Länge eines linear unabhängigen Zeilentupels von A.*

Beweis. Sei $G \in \operatorname{GL}_m(K)$ so, daß GA Zeilenstufenform annimmt. Mit obigem Lemma ist $\operatorname{rk}(GA) = \operatorname{rk} A$ und auch $\operatorname{rk}(GA)^{\mathrm{t}} = \operatorname{rk} A^{\mathrm{t}} G^{\mathrm{t}} = \operatorname{rk} A^{\mathrm{t}}$. Somit dürfen wir die Matrix A als in Zeilenstufenform gegeben annehmen, mit ausgewählten Spalten $1 \leqslant k_1 < \dots < k_l \leqslant n$.

Wir wissen bereits, daß $\operatorname{rk} A = l$. Nun sehen wir aber, daß das Tupel der ersten l Spalten von A^{t} linear unabhängig ist, und daß die weiteren Spalten alle verschwinden. Damit ist auch $\operatorname{rk} A^{\mathrm{t}} = l$. □

Seien $A = (a_{i,j})_{i,j} \in K^{m\times n}$ und $b \in K^m$ gegeben. Sei $(A|b) = (a_{*,1}, \dots, a_{*,n}, b) \in K^{m\times(n+1)}$ die um b ergänzte Matrix A.

Lemma. *Es gibt genau dann ein $x \in K^n$ mit $Ax = b$, wenn $\operatorname{rk} A = \operatorname{rk}(A|b)$.*

Beweis. Es gibt genau dann ein x mit $Ax = b$, wenn $b \in \langle a_{*,1}, \dots, a_{*,n} \rangle$, d.h. genau dann, wenn $\langle a_{*,1}, \dots, a_{*,n}, b \rangle = \langle a_{*,1}, \dots, a_{*,n} \rangle$. Da die Inklusion $\geqslant$ stets gilt, ist dies wiederum äquivalent zu

$$\operatorname{rk}(A|b) \;=\; \dim\langle a_{*,1}, \dots, a_{*,n}, b \rangle \;=\; \dim\langle a_{*,1}, \dots, a_{*,n} \rangle \;=\; \operatorname{rk} A\,.$$

□

3.4 Determinanten

Was das Signum für Permutationen, ist die Determinante für Matrizen.

3.4.1 Begriff

Definition. Sei $n \geqslant 1$, sei R ein kommutativer Ring, und sei $A = (a_{i,j}) \in R^{n\times n}$ eine $n\times n$-Matrix mit Einträgen in R. Die *Determinante* von A ist gegeben durch die *Leibnizsche Formel*

$$\det A \;:=\; \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\prod_{i\in[1,n]} a_{\sigma(i),i} \right) \;\in R\,.$$

Beispiel. Ist $n = 1$, so ist $\det(a_{1,1}) = a_{1,1}$. Ist $n = 2$, so ist $\det \left(\begin{smallmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{smallmatrix}\right) = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$.

Bemerkung. Für $n \geqslant 1$ und $D = \mathrm{diag}(d_1, \ldots, d_n)$ ist $\det D = \prod_{i \in [1,n]} d_i$, da in der Leibnizschen Formel nur der Summand zu $\sigma = 1$ zu berücksichtigen ist. Insbesondere ist $\det E_n = 1$.

Bemerkung. Für $\rho \in \mathcal{S}_n$ ist $\det \pi(\rho) = \varepsilon_\rho$, da in der Leibnizschen Formel nur der Summand $\varepsilon_\rho \prod_{i \in [1,n]} a_{\rho(i),i} = \varepsilon_\rho$ zu berücksichtigen ist.

Für $n \geqslant 3$ ist es untersagt, die Leibnizsche Formel zur praktischen Berechnung direkt anzuwenden – siehe vielmehr §3.4.4.

3.4.2 Charakterisierung

Sei K ein Körper, sei $n \geqslant 1$.

Satz 9 *Sei* $K^{n \times n} \xrightarrow{d} K$ *eine Abbildung.*

Die Abbildung d erfüllt (D 2, 3) *genau dann, wenn* $d(A) = d(E_n) \cdot \det A$ *gilt für alle* $A \in K^{n \times n}$.

Die Abbildung d erfüllt (D 1, 2, 3) *genau dann, wenn* $d(A) = \det A$ *gilt für alle* $A \in K^{n \times n}$, *d.h. wenn* $d = \det$.

(D 1) *Es ist* $d(E_n) = 1$ *(Normiertheit).*

(D 2) *Für alle* $A = (a_{i,j})_{i,j} \in K^{n \times n}$ *und für alle Spaltenpositionen* $j \in [1, n]$ *ist*

$$\begin{array}{rcl} K^n & \longrightarrow & K \\ x = (\xi_i)_i & \longmapsto & d(a_{*,1}, \ldots, a_{*,j-1}, \xi_*, a_{*,j+1}, \ldots, a_{*,n}) \end{array}$$

eine lineare Abbildung (Multilinearität).

(D 3) *Hat eine Matrix* $A \in K^{n \times n}$ *zwei übereinstimmende Spalten an verschiedenen Spaltenpositionen, so ist* $d(A) = 0$ *(Alternativität).*

Beweis. Wir haben zum einen zu zeigen, daß die Determinante det die Eigenschaften (D 1, 2, 3) hat, und zum anderen, daß für zwei Abbildungen d und d', die (D 2, 3) erfüllen, stets $d(A)d'(E_n) = d'(A)d(E_n)$ gilt. Denn dann folgt aus (D 2, 3) für d, daß $d(A) = \det(E_n)d(A) = d(E_n)\det(A)$; und umgekehrt, ist $d(A) = d(E_n)\det(A)$ stets, so folgen dann (D 2, 3) für d aus (D 2, 3) für det.

Wir behaupten zunächst, daß det den Forderungen (D 1, 2, 3) genügt.

Zu (D 1). Wir haben oben bereits angemerkt, daß $\det E_n = 1$.

Zu (D 2). Seien $A \in K^{n\times n}$, $x = (\xi_i)_i, y = (\eta_i)_i \in K^n$ und $\lambda, \mu \in K$ gegeben. Es wird

$$\begin{array}{l}\det(a_{*,1}, \ldots, a_{*,j-1}, \lambda\xi_* + \mu\eta_*, a_{*,j+1}, \ldots, a_{*,n}) \\ \quad = \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left((\lambda\xi_{\sigma(j)} + \mu\eta_{\sigma(j)}) \prod_{i\in[1,n]\smallsetminus\{j\}} a_{\sigma(i),i}\right) \\ \quad = \lambda \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\xi_{\sigma(j)} \prod_{i\in[1,n]\smallsetminus\{j\}} a_{\sigma(i),i}\right) + \mu \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\eta_{\sigma(j)} \prod_{i\in[1,n]\smallsetminus\{j\}} a_{\sigma(i),i}\right) \\ \quad = \lambda \det(a_{*,1}, \ldots, a_{*,j-1}, \xi_*, a_{*,j+1}, \ldots, a_{*,n}) + \mu \det(a_{*,1}, \ldots, a_{*,j-1}, \eta_*, a_{*,j+1}, \ldots, a_{*,n}) \; .\end{array}$$

Zu (D 3). Sei $A \in K^{n\times n}$ so gegeben, daß $l, l' \in [1, n]$ mit $l \neq l'$ und $a_{*,l} = a_{*,l'}$ existieren. Mit $\tau := (l, l') \in \mathcal{S}_n$ wird

$$\begin{array}{rcl}\det A & = & \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\prod_{i\in[1,n]} a_{\sigma(i),i}\right) \\ & = & \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\prod_{i\in[1,n]} a_{i,\sigma^{-1}(i)}\right) \\ & = & \left(\sum_{\sigma\in\mathcal{S}_n,\, \varepsilon_\sigma=+1} \left(\prod_{i\in[1,n]} a_{i,\sigma^{-1}(i)}\right)\right) - \left(\sum_{\sigma\in\mathcal{S}_n,\, \varepsilon_\sigma=+1} \left(\prod_{i\in[1,n]} a_{i,(\tau\circ\sigma^{-1})(i)}\right)\right) \\ & = & \left(\sum_{\sigma\in\mathcal{S}_n,\, \varepsilon_\sigma=+1} \left(\prod_{i\in[1,n]} a_{i,\sigma^{-1}(i)}\right)\right) - \left(\sum_{\sigma\in\mathcal{S}_n,\, \varepsilon_\sigma=+1} \left(\prod_{i\in[1,n]} a_{i,\sigma^{-1}(i)}\right)\right) \\ & = & 0 \; .\end{array}$$

Für die zweite Gleichheit wurde hierbei verwandt, daß ganz allgemein $\prod_{i\in[1,n]} d_i = \prod_{i\in[1,n]} d_{\sigma^{-1}(i)}$ für $d_i \in K$ und $\sigma \in \mathcal{S}_n$ gilt. Für die dritte Gleichheit wurde verwandt, daß wenn σ die Permutationen mit Signum $+1$ durchläuft, $\sigma \circ \tau$ die Permutationen mit Signum -1 durchläuft. Die vierte Gleichheit folgt schließlich aus $a_{i,j} = a_{i,\tau(j)}$, was nach Voraussetzung für alle $i, j \in [1, n]$ gegeben ist.

Seien nun Abbildungen $K^{n\times n} \overset{d}{\underset{d'}{\rightrightarrows}} K$ gegeben, die beide (D 2, 3) erfüllen. Können wir zeigen, daß $d(A)d'(E_n) = d'(A)d(E_n)$ für alle $A \in K^{n\times n}$ gilt, die als Spalten Standardbasisvektoren enthält, so folgt, daß diese Gleichung für alle $A \in K^{n\times n}$ zutrifft, da für $A = (a_{i,j})_{i,j}$ mit (D 2)

$$d(A)d'(E_n) \;=\; d(a_{*,1}, \ldots, a_{*,n})d'(E_n) \;=\; \sum_{i_1\in[1,n]} \cdots \sum_{i_n\in[1,n]} a_{i_1,1} \cdots a_{i_n,n} \cdot d(e_{i_1}, \ldots, e_{i_n}) \cdot d'(E_n) \; ,$$

und genauso für $d'(A)d(E_n)$.

Treten in einer solchen Matrix A gleiche Standardbasisvektoren an verschiedenen Stellen auf, so folgt aus (D 3), daß $d(A)d'(E_n) = 0 = d'(A)d(E_n)$.

Bleibt der Fall einer Permutationsmatrix $A = \pi(\sigma)$ mit einem $\sigma \in \mathcal{S}_n$ zu betrachten. Schreiben wir σ in Zykeldarstellung, und zerlegen die einzelnen Zykel gemäß $(d_1, \ldots, d_l) = (d_1, d_2)\circ \cdots \circ(d_{l-1}, d_l)$ in ein Produkt von Transpositionen, so sehen wir, daß wir insgesamt σ als Produkt von Transpositionen τ_i schreiben können, $\sigma = \tau_1 \circ \cdots \circ \tau_k$. Damit wird aus A nach k Vertauschungen je zweier Spalten die Einheitsmatrix E_n.

Mit (D 2) und (D 3) bewirkt jede solche Vertauschung eine Negation des Wertes von d. In der Tat ist

$$\begin{array}{rcl}0 & \overset{\text{(D 3)}}{=} & d(\ldots, a_{*,j} + a_{*,j'}, \ldots, a_{*,j} + a_{*,j'}, \ldots) \\ & \overset{\text{(D 2, 3)}}{=} & d(\ldots, a_{*,j}, \ldots, a_{*,j'}, \ldots) + d(\ldots, a_{*,j'}, \ldots, a_{*,j}, \ldots) \; .\end{array}$$

Genauso für d'. Wir erhalten $d(A)d'(E_n) = (-1)^k d(E_n)d'(E_n) = d'(A)d(E_n)$. ▫

3.4.3 Eigenschaften

Lemma. *Für* $A, B \in K^{n\times n}$ *ist* $\det(AB) = (\det A)(\det B)$. *Für* $S \in \mathrm{GL}_n(K)$ *ist insbesondere* $\det(S^{-1}AS) = \det A$.

Beweis. Wir betrachten die Abbildung $K^{n\times n} \xrightarrow{d} K$, $B \longmapsto d(B) := \det(AB)$. Diese erfüllt (D 2, 3), da die Linksmultiplikation mit A Linearkombinationen von Spalten auf entsprechende Linearkombinationen von mit A multiplizierten Spalten schickt, da gleiche Spalten in gleiche Spalten überführt werden, und da schließlich die Determinantenabbildung (D 2, 3) erfüllt. Es wird $\det(AB) \overset{\text{Def. } d}{=} d(B) \overset{\text{Satz 9}}{=} d(E_n)(\det B) \overset{\text{Def. } d}{=} (\det A)(\det B)$.

Damit wird nun $\det(S^{-1}AS) = (\det S^{-1})(\det A)(\det S) = (\det S^{-1})(\det S)(\det A) = \det(S^{-1}S)(\det A) = \det A$. ▫

Lemma. *Eine Matrix* $A \in K^{n\times n}$ *ist regulär genau dann, wenn* $\det A \neq 0$. *Insbesondere ist* $\mathrm{GL}_n(K) \xrightarrow{\det} \mathrm{GL}_1(K) = K \smallsetminus \{0\}$ *ein Gruppenmorphismus.*

Beweis. Ist A regulär, so ist wegen $1 = \det E_n = (\det A)(\det A^{-1})$ auch $\det A \neq 0$.

Sei nun A singulär. Sei $\sum_{i\in[1,n]} \lambda_i a_{*,i} = 0$ mit $\lambda_i \in K$, und sei $\lambda_j \neq 0$. Mit $\mu_i := -\lambda_i/\lambda_j$ läßt sich $a_{*,j} = \sum_{i\in[1,n]\smallsetminus\{j\}} \mu_i a_{*,i}$ schreiben, und es wird

$$\begin{array}{rcl} \det A & = & \det(a_{*,1}, \ldots, a_{*,j-1}, a_{*,j}, a_{*,j+1}, \ldots, a_{*,n}) \\ & \overset{\text{(D 2)}}{=} & \sum_{i\in[1,n]\smallsetminus\{j\}} \mu_i \det(a_{*,1}, \ldots, a_{*,j-1}, a_{*,i}, a_{*,j+1}, \ldots, a_{*,n}) \\ & \overset{\text{(D 3)}}{=} & 0 \,. \end{array}$$

Damit ist die Abbildung $\mathrm{GL}_n(K) \xrightarrow{\det} K \smallsetminus \{0\}$ wohldefiniert. Nach vorigem Lemma ist sie ein Gruppenmorphismus. ▫

Lemma. *Für* $A \in K^{n\times n}$ *ist* $\det A^{\mathrm{t}} = \det A$.

Beweis. Wir schreiben $A = (a_{i,j})_{i,j}$, mithin $A^{\mathrm{t}} = (a_{i,j})_{j,i}$, und berechnen

$$\begin{array}{rcl} \det A^{\mathrm{t}} & = & \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\prod_{i\in[1,n]} a_{i,\sigma(i)}\right) \\ & = & \sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\prod_{i\in[1,n]} a_{\sigma^{-1}(i),i}\right) \\ & = & \sum_{\rho\in\mathcal{S}_n} \varepsilon_{\rho^{-1}} \left(\prod_{i\in[1,n]} a_{\rho(i),i}\right) \\ & = & \sum_{\rho\in\mathcal{S}_n} \varepsilon_\rho \left(\prod_{i\in[1,n]} a_{\rho(i),i}\right) \\ & = & \det A \,. \end{array}$$

▫

Lemma. *Sei* $A = (a_{i,j})_{i,j} \in K^{n\times n}$ *gegeben mit einem Index* $k \in [1, n]$ *so, daß* $a_{i,j} = 0$ *für alle* $(i, j) \in [k + 1, n] \times [1, k]$. *Dann ist*

$$\det A \;=\; \det(a_{i,j})_{i\in[1,n],\, j\in[1,n]} \;=\; \left(\det(a_{i,j})_{i\in[1,k],\, j\in[1,k]}\right) \left(\det(a_{i,j})_{i\in[k+1,n],\, j\in[k+1,n]}\right) \,.$$

In anderen Worten, die Determinante einer oberen Blockdreiecksmatrix ist gleich dem Produkt der Determinanten der Blöcke auf der Diagonalen. Genauso auch für untere Blockdreiecksmatrizen.

Beweis. Für $\sigma \in \mathcal{S}_n$ verschwindet der Summand $\prod_{i\in[1,n]} a_{\sigma(i),i}$ aus der Leibnizschen Formel, falls es ein $i \in [1,k]$ gibt mit $\sigma(i) \in [k+1,n]$. In Zykelschreibweise gibt es daher keinen Zykel von σ, der sowohl ein Element von $[1,k]$ als auch von $[k+1,n]$ enthält. Damit können wir in eindeutiger Weise $\sigma = \rho \circ \tau$ schreiben, wobei ρ die Teilmenge $[k+1,n]$ festläßt, und wobei τ die Teilmenge $[1,k]$ festläßt. Bezeichnen wir in $\mathcal{S}_n$ die Untergruppe der Permutationen, die $[k+1,n]$ festlassen, mit $\mathcal{S}_{[1,k]}$ $(= \mathcal{S}_k)$, und die Untergruppe der Permutationen, die $[1,k]$ festlassen, mit $\mathcal{S}_{[k+1,n]}$, so wird

$$
\begin{aligned}
\det A &= \textstyle\sum_{\sigma\in\mathcal{S}_n} \varepsilon_\sigma \left(\prod_{i\in[1,n]} a_{\sigma(i),i}\right) \\
&= \textstyle\sum_{\rho\in\mathcal{S}_{[1,k]},\ \tau\in\mathcal{S}_{[k+1,n]}} \varepsilon_{\rho\circ\tau} \left(\prod_{i\in[1,k]} a_{\rho(i),i}\right)\left(\prod_{i\in[k+1,n]} a_{\tau(i),i}\right) \\
&= \left(\textstyle\sum_{\rho\in\mathcal{S}_{[1,k]}} \varepsilon_\rho \left(\prod_{i\in[1,k]} a_{\rho(i),i}\right)\right)\left(\textstyle\sum_{\tau\in\mathcal{S}_{[k+1,n]}} \varepsilon_\tau \left(\prod_{i\in[k+1,n]} a_{\tau(i),i}\right)\right) \\
&= (\det(a_{i,j})_{i\in[1,k],\ j\in[1,k]})(\det(a_{i,j})_{i\in[k+1,n],\ j\in[k+1,n]})\ .
\end{aligned}
$$

Da $\det A = \det A^{\mathrm{t}}$, gilt die entsprechende Aussage auch für untere Blockdreiecksmatrizen. □

3.4.4 Berechnung

3.4.4.1 Gaußscher Algorithmus

Sei $A \in K^{n\times n}$ gegeben. Sei GA in Zeilenstufenform. Dann ist $\det(GA) = \det E_n = 1$, falls A regulär ist, und $\det(GA) = 0$ sonst. Im ersten Fall haben wir somit $\det A = (\det G)^{-1}$ zu berechnen.

Schreiben wir nun die Matrix G als Produkt $G = T_k \cdots T_2 \cdot T_1$ von zu einzelnen Umformungsschritten gehörenden Matrizen $T_i \in \mathrm{GL}_n(K)$, so wird $\det A = \prod_{i\in[1,k]}(\det T_i)^{-1}$. Eine solche Matrix T_i ist nun eine Elementarmatrix, eine Permutationsmatrix oder eine invertierbare Diagonalmatrix. Stellen wir zusammen:

(E) Für $k, l \in [1,n]$, $k \neq l$ und $\eta \in K$ ist $\det E_{k,l}(\eta) = 1$.

(D) Es ist $\det \mathrm{diag}(d_1,\ldots,d_n) = \prod_{i\in[1,n]} d_i$ für beliebige Diagonaleinträge $d_i \in K$.

(P) Für $\sigma \in \mathcal{S}_n$ ist $\det \pi(\sigma) = \varepsilon_\sigma$.

Diese Regeln wurden entweder schon eingesehen, oder folgen aus dem Lemma über Blockdreiecksmatrizen. Eine vollständige Zeilenstufenform muß unter Zuhilfenahme des Lemmas über Blockdreiecksmatrizen in der Regel nicht erreicht werden, um die Determinante angeben zu können.

Beispiel. Wir erhalten über $K = \mathbf{R}$

$$\det \begin{pmatrix} 2&4&2 \\ 5&3&0 \\ 2&3&1 \end{pmatrix} \;=\; 2\det \begin{pmatrix} 1&2&1 \\ 0&-7&-5 \\ 0&-1&-1 \end{pmatrix} \;=\; 2\det \begin{pmatrix} 1&2&1 \\ 0&1&1 \\ 0&0&2 \end{pmatrix} \;=\; 4\ .$$

Oder aber, über $K = \mathbf{F}_2$,

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

3.4.4.2 Laplacescher Entwicklungssatz

Sei $n \geqslant 2$.

Definition. Sei $A = (a_{i,j})_{i,j} \in K^{n\times n}$. Für $k, l \in [1, n]$ schreiben wir

$$A_{k,l} \;:=\; (a_{i,j})_{i\in[1,n]\smallsetminus\{k\},\, j\in[1,n]\smallsetminus\{l\}} \;\in\; K^{(n-1)\times(n-1)}$$

für die Matrix, die aus A durch Streichen der $k$ten Zeile und der $l$ten Spalte hervorgeht. Vorsicht, $A_{k,l} \in K^{(n-1)\times(n-1)}$ und $a_{k,l} \in K$ nicht verwechseln.

Satz 10 *Sei* $A = (a_{i,j})_{i,j} \in K^{n\times n}$.

(i) *Sei* $l \in [1, n]$. *Eine* Entwicklung von $\det A$ nach der $l$ten Spalte *gibt*

$$\det A \;=\; \sum_{k\in[1,n]} (-1)^{k+l} a_{k,l} \det A_{k,l}\ .$$

(ii) *Sei* $k \in [1, n]$. *Eine* Entwicklung von $\det A$ nach der $k$ten Zeile *gibt*

$$\det A \;=\; \sum_{l\in[1,n]} (-1)^{k+l} a_{k,l} \det A_{k,l}\ .$$

Beweis. Zu (i). Es wird

$$\begin{aligned} &\det \begin{pmatrix} a_{1,1} & \cdots & a_{1,l-1} & a_{1,l} & a_{1,l+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,l-1} & a_{n,l} & a_{n,l+1} & \cdots & a_{n,n} \end{pmatrix} \\ \overset{\text{(D 2)}}{=}\;\; & \textstyle\sum_{k\in[1,n]} a_{k,l} \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,l-1} & 0 & a_{1,l+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,l-1} & 1 & a_{k,l+1} & \cdots & a_{k,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,l-1} & 0 & a_{n,l+1} & \cdots & a_{n,n} \end{pmatrix} \end{aligned}$$

$$\overset{\text{(D 3)}}{=} \quad \sum_{k\in[1,n]} a_{k,l}(-1)^{l-1} \det \begin{pmatrix} 0 & a_{1,1} & \cdots & a_{1,l-1} & a_{1,l+1} & \cdots & a_{1,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & a_{k,1} & \cdots & a_{k,l-1} & a_{k,l+1} & \cdots & a_{k,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,l-1} & a_{n,l+1} & \cdots & a_{n,n} \end{pmatrix}$$

$$\overset{\text{(D 3)}}{=} \quad \sum_{k\in[1,n]} a_{k,l}(-1)^{l-1}(-1)^{k-1} \det \begin{pmatrix} 1 & a_{k,1} & \cdots & a_{k,l-1} & a_{k,l+1} & \cdots & a_{k,n} \\ 0 & a_{1,1} & \cdots & a_{1,l-1} & a_{1,l+1} & \cdots & a_{1,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{k-1,1} & \cdots & a_{k-1,l-1} & a_{k-1,l+1} & \cdots & a_{k-1,n} \\ 0 & a_{k+1,1} & \cdots & a_{k+1,l-1} & a_{k+1,l+1} & \cdots & a_{k+1,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,l-1} & a_{n,l+1} & \cdots & a_{n,n} \end{pmatrix}$$

$$\overset{\text{Blockdreiecksmatrix}}{=} \quad \sum_{k\in[1,n]}(-1)^{k+l} a_{k,l} \det A_{k,l} \ .$$

Zu (ii). Dies folgt aus (i) mit der Invarianz der Determinante unter Transposition und mit $(A_{k,l})^{\mathrm{t}} = (A^{\mathrm{t}})_{l,k}$. □

In der Praxis verwendet man in der Regel eine Kombination von Gaußschem Algorithmus, Laplacescher Entwicklung und dem Lemma über die Determinante von Blockdreiecksmatrizen, um eine Determinante auszurechnen. Ausnahme: $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc$ wird besser ohne weitere Umformung berechnet.

Beispiel. Sei $K = \mathbf{R}$. Es ist

$$\det\left(\begin{smallmatrix} 2 & 4 & 2 \\ 5 & 3 & 0 \\ 2 & 3 & 1 \end{smallmatrix}\right) \;=\; (-5)\cdot\det\left(\begin{smallmatrix} 4 & 2 \\ 3 & 1 \end{smallmatrix}\right) + 3\cdot\det\left(\begin{smallmatrix} 2 & 2 \\ 2 & 1 \end{smallmatrix}\right) \;=\; -5\cdot(-2) + 3\cdot(-2) \;=\; 4 \ .$$

3.4.5 Die Cramersche Regel

Eine Matrix $A \in K^{n\times n}$ ist invertierbar genau dann, wenn ihre Determinante nicht verschwindet, wenn man also $(\det A)^{-1}$ bilden kann. Wir wollen nun für $A \in \mathrm{GL}_n(K)$ eine Formel für A^{-1} angeben, in welcher der Faktor $(\det A)^{-1}$ in der Tat auftritt. Zur praktischen Berechnung von A^{-1} für $n \geqslant 3$ sei aber weiterhin auf den Gaußschen Algorithmus verwiesen.

Satz 11 *Sei $A = (a_{i,j})_{i,j} \in K^{n\times n}$. Es ist*

$$(\det A)\cdot E_n \;=\; \left((-1)^{i+j}\det A_{j,i}\right)_{i,j}\cdot A \ .$$

Falls $\det A \neq 0$, *so wird insbesondere* $A^{-1} \;=\; (\det A)^{-1}\left((-1)^{i+j}\det A_{j,i}\right)_{i,j}$.

Beweis. Wir haben den Eintrag des Produktes $B = (b_{i,k})_{i,k} := \left((-1)^{i+j}\det A_{j,i}\right)_{i,j}\cdot A$ an der Position (i,k) zu berechnen.

Ist $i = k$, so erhalten wir mit Entwicklung von $\det A$ nach der $i$ten Spalte gemäß Satz 10

$$b_{i,i} \;=\; \sum_{j\in[1,n]} (-1)^{i+j} \det A_{j,i} \cdot a_{j,i} \;=\; \det A\,.$$

Ist $i \neq k$, so sei $A' = (a_{*,1}, \dots, a_{*,i-1}, a_{*,k}, a_{*,i+1}, \dots, a_{*,n})$. Mit Satz 10 wird mit Entwicklung von $\det A'$ nach der $i$ten Spalte

$$\begin{array}{rcl} b_{i,k} & = & \sum_{j\in[1,n]} (-1)^{i+j} \det A_{j,i} \cdot a_{j,k} \\ & = & \sum_{j\in[1,n]} (-1)^{i+j} \det A'_{j,i} \cdot a_{j,k} \\ & = & \det A' \\ & = & 0\,. \end{array}$$

$\square$

Beispiel. Seien $a, b, c, d \in K$, und sei $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Wir erhalten

$$\begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \;=\; \begin{pmatrix} +d & -b \\ -c & +a \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}\,.$$

Ist nun $\det A = ad - bc \neq 0$, so folgt $A^{-1} = \frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

Beispiel. Sei $A = (a_{i,j})_{i,j} \in \mathrm{GL}_3(K)$. Der Eintrag von A^{-1} an Position $(1,2)$ ergibt sich zu $-(\det A)^{-1} \det A_{2,1} = -(\det A)^{-1} \det \left(\begin{smallmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{smallmatrix}\right)$.

Kapitel 4

Normalformen

Durch geeignete Basiswahl kann man der beschreibenden Matrix eines Endomorphismus $K^n \xrightarrow{f} K^n$ eine handliche Gestalt geben, die nicht allzuweit von einer Diagonalmatrix entfernt ist. In der Praxis heißt dies, man kann für jedes $A \in K^{n\times n}$ eine Matrix $S \in \mathrm{GL}_n(K)$ so finden, daß $S^{-1}AS$ diese Gestalt, Jordanform genannt, annimmt. Im Spezialfall einer hermiteschen Matrix $A \in \mathbf{C}^{n\times n}$, d.h. einer Matrix, deren Einträge an den an der Hauptdiagonalen gespiegelten Positionen bis auf Konjugation übereinstimmen, kann man sogar eine Diagonalmatrix erreichen, und zusätzlich für S eine unitäre Matrix verwenden, d.h. eine Matrix mit einer Orthonormalbasis in den Spalten.

Definition. Ein Körper K heißt *algebraisch abgeschlossen,* falls jedes Polynom $f(X) \in K[X] \smallsetminus K$ eine Nullstelle $x \in K$ besitzt, für welche also $f(x) = 0$ ist.

Ist K algebraisch abgeschlossen, so zerfällt jedes Polynom in $K[X] \smallsetminus K$ in ein Produkt von Polynomen von Grad 1. Dies erkennt man durch sukzessives Abspalten von zu Nullstellen gehörenden Faktoren von Grad 1.

Satz (ohne Beweis). *Der Körper* $\mathbf{C}$ *der komplexen Zahlen ist algebraisch abgeschlossen.*

Zum Beweis verweisen wir auf [**3,** Kap. 4] oder auf §4.5.2.1. In unseren Beispielen werden wir uns auf Polynome in $\mathbf{C}[X]$ beschränken, die auch ohne Kenntnis dieses Satzes in Faktoren von Grad 1 zerlegt werden können.

Bemerkung. Ein endlicher Körper K ist nicht algebraisch abgeschlossen, da mit $q := \#K$ das Polynom $X^q - X + 1$ von Grad $q > 1$ bei allen $x \in K$ konstant den Wert 1 annimmt.

Satz (ohne Beweis). *Jeder Körper K ist in einem algebraisch abgeschlossenen Körper (als Teilkörper) enthalten.*

Zum Beweis verweisen wir auf [**9,** §6, Satz 2].

Bemerkung. Ist K ein Körper, so läßt sich der Polynomring $K[X]$ in einen größeren Körper als Teilring einbetten (nämlich in den Körper der rationalen Funktionen, bestehend aus Brüchen von Polynomen). Daher sind die in §3.4 hergeleiteten Rechenregeln für Determinanten auch für Determinanten mit Einträgen in $K[X]$ entsprechend gültig.

In diesem Kapitel sei nun K ein algebraisch abgeschlossener Körper.

4.1 Eigenwerte und Eigenvektoren

Definition. Sei $n \geqslant 1$, sei $A \in K^{n\times n}$. Sei $\lambda \in K$. Gibt es einen Vektor $x \in K^n \setminus \{0\}$, für den

$$Ax \;=\; \lambda x$$

gilt, so heißt λ ein *Eigenwert* von A. Der Vektor x heißt dann *Eigenvektor* von A (zum Eigenwert λ).

Für $l, m \geqslant 1$ und $B \in K^{l\times m}$ schreiben wir auch

$$\begin{array}{rclcl} \operatorname{Im} B & := & \operatorname{Im}(x \longmapsto Bx) & = & \{Bx \mid x \in K^m\} & \leqslant & K^l \\ \operatorname{Kern} B & := & \operatorname{Kern}(x \longmapsto Bx) & = & \{x \in K^m \mid Bx = 0\} & \leqslant & K^m\,. \end{array}$$

Eigenraum. Wir setzen

$$E_A(\lambda) \;:=\; \operatorname{Kern}(\lambda E - A) \;=\; \{x \in K^n \mid Ax = \lambda x\} \;\leqslant\; K^n\,,$$

genannt der *Eigenraum* von A zum Eigenwert λ. In anderen Worten, $E_A(\lambda)$ ist die Menge der Eigenvektoren von A zum Eigenwert λ, ergänzt um den Nullvektor.

Charakteristisches Polynom. Sei $A \in K^{n\times n}$. Das Polynom

$$\chi_A(X) \;:=\; \det(X \cdot E_n - A) \;\in\; K[X]$$

heißt *charakteristisches Polynom von A.* Es ist, wie man der Leibnizschen Formel entnimmt, normiert von Grad $\deg(\chi_A) = n$.

Bemerkung. Wegen $\chi_{S^{-1}AS}(X) = \det(XE - S^{-1}AS) = \det(S^{-1})\det(XE - A)\det(S) = \det(XE - A) = \chi_A(X)$ für $S \in \mathrm{GL}_n(K)$ ist das charakteristische Polynom invariant unter *Konjugation* $A \longmapsto S^{-1}AS$.

Lemma. *Es ist $\lambda \in K$ ein Eigenwert von A genau dann, wenn $\chi_A(\lambda) = 0$.*

Beweis. Es ist $\chi_A(\lambda) = \det(\lambda E_n - A)$ genau dann gleich 0, wenn $\operatorname{rk}(\lambda E_n - A) < n$ ist, also genau dann, wenn $\operatorname{Kern}(\lambda E - A) \neq 0$. Dies wiederum ist äquivalent zur Existenz eines Eigenvektors zum Eigenwert λ. $\square$

Definition. Die *Spur* von $A = (a_{i,j})_{i,j}$ ist definiert als $\operatorname{tr} A := \sum_{i\in[1,n]} a_{i,i}$ (engl. trace).

Lemma. *Schreiben wir $\chi_A(X) =: X^n + h_{n-1}X^{n-1} + \cdots + h_0X^0$ mit $h_i \in K$, so ist $h_0 = (-1)^n \det A$ und $h_{n-1} = -\operatorname{tr} A$. Schreiben wir $\chi_A(X) =: \prod_{i\in[1,n]}(X - \lambda_i)$, so ist $\det A = \prod_{i\in[1,n]} \lambda_i$ und $\operatorname{tr} A = \sum_{i\in[1,n]} \lambda_i$.*

Beweis. Substituiert man X durch 0 in der Definition des charakteristischen Polynoms, so folgen die Aussagen über die Determinante. Für die Aussage für die Spur betrachtet man die Leibnizsche Formel für $\det(XE - A)$. Der einzige Summand darin, der einen Beitrag zum Koeffizienten von X^{n-1} liefert, ist $(X - a_{1,1}) \cdots (X - a_{n,n})$, und dieser Beitrag beträgt gerade $-\operatorname{tr} A$. Aus $\chi_A(X) = \prod_{i\in[1,n]}(X-\lambda_i)$ lesen wir auf der anderen Seite ab, daß dieser Koeffizient auch gleich $-\sum_{i\in[1,n]}\lambda_i$ ist. ▫

Geometrische und algebraische Vielfachheit. Sei $\lambda \in K$ ein Eigenwert der Matrix A. Die Dimension des Eigenraums $E_A(\lambda)$ heißt die *geometrische Vielfachheit* von λ. Die Anzahl der Faktoren gleich $X-\lambda$ in einer Zerlegung von $\chi_A(X)$ in ein Produkt von Faktoren der Form $X-\mu$, $\mu \in K$, heißt *algebraische Vielfachheit* von λ.

Bemerkung. Mit dem charakteristischen Polynom ist auch die algebraische Vielfachheit eines Eigenwertes invariant unter Konjugation. Dies trifft nun wegen

$$\begin{array}{rcl} S \cdot E_{S^{-1}AS}(\lambda) & = & \{Sx \mid x \in K^n,\ (\lambda E - S^{-1}AS)x = 0\} \\ & = & \{Sx \mid x \in K^n,\ S^{-1}(\lambda E - A)Sx = 0\} \\ & = & \{y \in K^n \mid (\lambda E - A)y = 0\} \\ & = & E_A(\lambda) \end{array}$$

für $S \in \mathrm{GL}_n(K)$ auch für die geometrische Vielfachheit zu.

Bemerkung. Seien $\lambda_1, \ldots, \lambda_k$ die Eigenwerte von A mit jeweiligen algebraischen Vielfachheiten $m_1, \ldots, m_k$. Dann ist $\sum_{i\in[1,k]} m_i = n$.

Beispiel. Sei $K = \mathbf{C}$, sei $A = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. Es ist $\chi_A(X) = \det \left(\begin{smallmatrix} X-1 & 0 & 0 \\ 0 & X & 1 \\ 0 & -1 & X \end{smallmatrix}\right) = (X-1)(X^2+1)$. Damit hat A die Eigenwerte 1, i und $-i$. Ein Eigenvektor zu 1 berechnet sich aus dem Gleichungssystem $(1 \cdot E - A)x = 0$ zu $\left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right)$. Ein Eigenvektor zu i berechnet sich aus dem Gleichungssystem $(i \cdot E - A)x = 0$ zu $\left(\begin{smallmatrix} 0 \\ 1 \\ -i \end{smallmatrix}\right)$. Ein Eigenvektor zu $-i$ berechnet sich aus dem Gleichungssystem $((-i) \cdot E - A)x = 0$ zu $\left(\begin{smallmatrix} 0 \\ 1 \\ i \end{smallmatrix}\right)$. Alle Eigenwerte haben geometrische und algebraische Vielfachheit 1.

Beispiel. Sei $K = \mathbf{C}$, sei $A = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Es ist $\chi_A(X) = (X-1)^3$. Der Eigenraum zum Eigenwert 1 berechnet sich zu $E_A(1) = \langle \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right) \rangle$. Damit hat der Eigenwert 1 die geometrische Vielfachheit 1 und die algebraische Vielfachheit 3.

4.2 Vereinfachte Berechnung des charakteristischen Polynoms

Bei der direkten Berechnung des charakteristischen Polynoms $\chi_A(X)$ einer Matrix $A \in K^{n\times n}$ als Determinante von $X \cdot E_n - A$ stößt man auf das Problem, daß sowohl bei Gaußvereinfachungsschritten als auch bei Laplaceentwicklung Polynome von Grad $\geqslant 2$ als Einträge auftreten können. Wir wollen auf simple Weise eine Basis von K^n so finden, daß bei Basiswechsel dieses Problem verschwindet. Die bei Basiswechsel resultierende Matrix kann als Vorstufe einer Normalform von A betrachtet werden. Der weiter unten angeführten Berechnung der Jordanform kann diese Vorstufe als Vorvereinfachung vorangestellt werden, muß aber nicht.

4.2.1 Der Algorithmus

Lemma. *Sei $k \geqslant 1$. Seien gegeben $\lambda_i \in K$ für $i \in [0, k-1]$. Sei*

$$B = \begin{pmatrix} 0 & & & & -\lambda_0 \\ 1 & 0 & & & -\lambda_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -\lambda_{k-1} \end{pmatrix},$$

wobei nicht erwähnte Einträge gleich 0 seien. Es ist $\chi_B(X) = X^k + \lambda_{k-1}X^{k-1} + \cdots + \lambda_0 X^0$.

Beweis. Wir führen eine Induktion nach k, erhalten für $k = 1$ das verlangte Ergebnis, und für $k \geqslant 2$ mit einer Entwicklung nach der ersten Spalte

$$\begin{aligned} \chi_B(X) &= \det \begin{pmatrix} X & & & & \lambda_0 \\ -1 & X & & & \lambda_1 \\ & -1 & \ddots & & \vdots \\ & & \ddots & X & \lambda_{k-2} \\ & & & -1 & X+\lambda_{k-1} \end{pmatrix} \\ &= X \det \begin{pmatrix} X & & & & \lambda_1 \\ -1 & X & & & \lambda_2 \\ & -1 & \ddots & & \vdots \\ & & \ddots & X & \lambda_{k-2} \\ & & & -1 & X+\lambda_{k-1} \end{pmatrix} + \det \begin{pmatrix} 0 & & & & \lambda_0 \\ -1 & X & & & \lambda_2 \\ & -1 & \ddots & & \vdots \\ & & \ddots & X & \lambda_{k-2} \\ & & & -1 & X+\lambda_{k-1} \end{pmatrix} \\ &= (X^k + \lambda_{k-1}X^{k-1} + \cdots + \lambda_1 X^1) + (-1)^{k-1} \cdot \lambda_0 \cdot (-1)^{k-1} \\ &= X^k + \lambda_{k-1}X^{k-1} + \cdots + \lambda_0 X^1 + \lambda_0 \,. \end{aligned}$$

□

Algorithmus. Sei $n \geqslant 1$. Sei $A \in K^{n \times n}$. Sei $W_0 := \{0\} \subseteq K^n$.

Schritt 1. Wähle $b_1 \in K^n \smallsetminus W_0$. Bestimme $k_1 \geqslant 1$ maximal so, daß

$$(A^0 b_1,\ A^1 b_1,\ \ldots,\ A^{k_1 - 1} b_1)$$

linear unabhängig ist. Sei W_1 der von diesem Tupel erzeugte Unterraum in K^n. Merke die Koeffizienten $\lambda_{1,i}$ in

$$A^{k_1} b_1 + \sum_{i \in [0,\, k_1 - 1]} \lambda_{1,i} A^i b_1 \in W_0 \,.$$

Ist $k_1 = n$, so brich das Verfahren ab.

Schritt 2. Wähle $b_2 \in K^n \smallsetminus W_1$. Bestimme $k_2 \geqslant 1$ maximal so, daß

$$(A^0 b_1,\ \ldots,\ A^{k_1-1}b_1,\ A^0 b_2,\ \ldots,\ A^{k_2-1}b_2)$$

linear unabhängig ist. Sei W_2 der von diesem Tupel erzeugte Unterraum in K^n. Merke die Koeffizienten $\lambda_{2,i}$ in

$$A^{k_2}b_2 + \sum_{i\in[0,\,k_2-1]} \lambda_{2,i}A^i b_2 \in W_1\ .$$

Ist $k_1 + k_2 = n$, so brich das Verfahren ab.

Schritt 3. Wähle $b_3 \in K^n \smallsetminus W_2$. Bestimme $k_3 \geqslant 1$ maximal so, daß

$$(A^0 b_1,\ \ldots,\ A^{k_1-1}b_1,\ A^0 b_2,\ \ldots,\ A^{k_2-1}b_2,\ A^0 b_3,\ \ldots,\ A^{k_3-1}b_3)$$

linear unabhängig ist. Sei W_3 der von diesem Tupel erzeugte Unterraum in K^n. Merke die Koeffizienten $\lambda_{3,i}$ in

$$A^{k_3}b_3 + \sum_{i\in[0,\,k_3-1]} \lambda_{3,i}A^i b_3 \in W_1\ .$$

Ist $k_1 + k_2 + k_3 = n$, so brich das Verfahren ab.

Und so fort, bis in *Schritt t* schließlich $\sum_{i\in[1,t]} k_i = n$ erreicht ist.

Sei nun $T \in \mathrm{GL}_n(K)$ die Matrix, deren Spaltentupel durch

$$(A^0 b_1,\ \ldots,\ A^{k_1-1}b_1,\ A^0 b_2,\ \ldots,\ A^{k_2-1}b_2,\ \ldots,\ A^0 b_t,\ \ldots,\ A^{k_t-1}b_t)$$

gegeben ist. Dann ist

$$T^{-1}AT \;=\; \left(\begin{array}{c|c|c|c}
\begin{matrix} 0 & & & & -\lambda_{1,1} \\ 1 & 0 & & & -\lambda_{1,2} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -\lambda_{1,\,k_1-1} \end{matrix} & \begin{matrix} * \\ * \\ \vdots \\ \vdots \\ * \end{matrix} & & \begin{matrix} * \\ * \\ \vdots \\ \vdots \\ * \end{matrix} \\ \hline
 & \begin{matrix} 0 & & & & -\lambda_{2,1} \\ 1 & 0 & & & -\lambda_{2,2} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -\lambda_{2,\,k_2-1} \end{matrix} & & \begin{matrix} * \\ * \\ \vdots \\ \vdots \\ * \end{matrix} \\ \hline
 & & \begin{matrix} \ddots & \\ & \ddots \end{matrix} & \begin{matrix} \vdots \\ \vdots \end{matrix} \\ \hline
 & & & \begin{matrix} 0 & & & & -\lambda_{t,1} \\ 1 & 0 & & & -\lambda_{t,2} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -\lambda_{t,\,k_t-1} \end{matrix}
\end{array}\right) \;=:\; \tilde{A}\ ,$$

wobei alle nicht erwähnten Einträge verschwinden, und alle mit $*$ markierten Einträge nicht spezifiziert sind. Dies erkennt man durch Vergleich von AT mit $T\tilde{A}$. Da das charakteristische Polynom unter Konjugation invariant ist, ist $\chi_A(X) = \chi_{\tilde{A}}(X) = \det(X \cdot E_n - \tilde{A})$. Diese Determinante einer oberen Blockdreiecksmatrix kann diagonalblockweise ausgerechnet werden. Mit vorstehendem Lemma erhalten wir

$$\chi_A(X) \;=\; \chi_{\tilde{A}}(X) \;=\; \prod_{j\in[1,k]} \left(X^{k_j} + \sum_{i\in[0,\,k_j-1]} \lambda_{j,i} X^i \right) .$$

Bemerkung. Für die Bestimmung der k_i bringe man die aus dem bislang erhaltenen Tupel gebildete Matrix in Spaltenstufenform (d.h. die transponierte Matrix in Zeilenstufenform).

4.2.2 Ein Beispiel

Sei $K = \mathbf{C}$. Sei

$$A := \begin{pmatrix} 3 & 2 & 1 & 0 & -2 & -2 \\ 2 & 3 & 0 & -1 & -1 & -2 \\ 1 & 1 & 2 & 0 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 0 \\ 2 & 1 & 0 & -1 & 1 & -2 \\ 1 & 1 & 1 & 0 & -1 & 0 \end{pmatrix} \;\in\; \mathbf{C}^{6\times 6} .$$

Schritt 1. Sei $b_1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Es wird $Ab_1 = \begin{pmatrix} 3 \\ 2 \\ 1 \\ 1 \\ 2 \\ 1 \end{pmatrix}$. Die Matrix $(A^0 b_1,\, A^1 b_1)$ bringen wir in die Spaltenstufenform

$$\left(\begin{array}{cc} 1 & 3 \\ 0 & 2 \\ 0 & 1 \\ 0 & 1 \\ 0 & 2 \\ 0 & 1 \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right) \;\rightsquigarrow\; \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \\ 0 & 1/2 \\ 0 & 1/2 \\ 0 & 1 \\ 0 & 1/2 \\ \hline 1 & -3/2 \\ 0 & 1/2 \end{array}\right) ,$$

wobei wir noch unterhalb des Querstrichs die Information mitführen, wie die Spalten entstanden sind. So z.B. ist die zweite Spalte gleich $-3/2 \cdot A^0 b_1 + 1/2 \cdot A^1 b_1$.

Es wird $A^2 b_1 = A(Ab_1) = \begin{pmatrix} 8 \\ 7 \\ 4 \\ 3 \\ 7 \\ 4 \end{pmatrix}$. Unter Verwendung der vorhergehenden Spaltenstufenform bringen wir nun auch die Matrix $(A^0 b_1,\, A^1 b_1,\, A^2 b_1)$ in die Spaltenstufenform

$$\left(\begin{array}{ccc} 1 & 0 & 8 \\ 0 & 1 & 7 \\ 0 & 1/2 & 4 \\ 0 & 1/2 & 3 \\ 0 & 1 & 7 \\ 0 & 1/2 & 4 \\ \hline 1 & -3/2 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1 \end{array}\right) \;\rightsquigarrow\; \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & -4 & 5 \\ 0 & 4 & -7 \\ 0 & -1 & 2 \end{array}\right) .$$

Es wird $A^3b_1 = A(A^2b_1) = \begin{pmatrix} 20\\19\\12\\7\\19\\12 \end{pmatrix}$. Unter Verwendung der vorhergehenden Spaltenstufenform bringen wir nun auch die Matrix $(A^0b_1,\, A^1b_1,\, A^2b_1,\, A^3b_1)$ in die Spaltenstufenform

$$\left(\begin{array}{rrrr} 1 & 0 & 0 & 20\\ 0 & 1 & 0 & 19\\ 0 & 0 & 1 & 12\\ 0 & 1 & -1 & 7\\ 0 & 1 & 0 & 19\\ 0 & 0 & 1 & 12\\ \hline 1 & -4 & 5 & 0\\ 0 & 4 & -7 & 0\\ 0 & -1 & 2 & 0\\ 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{rrrr} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & -1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ \hline 1 & -4 & 5 & -4\\ 0 & 4 & -7 & 8\\ 0 & -1 & 2 & -5\\ 0 & 0 & 0 & 1 \end{array}\right) .$$

Wir entnehmen der letzten Spalte der mitgeführten Matrix, daß

$$A^3b_1 - 5A^2b_1 + 8A^1b_1 - 4A^0b_1 \;=\; 0\,.$$

Schritt 2. Sei $b_2 := \begin{pmatrix} 0\\1\\0\\0\\0\\0 \end{pmatrix}$. Unter Verwendung der vorletzten Spaltenstufenform in Schritt 1 bringen wir nun auch die Matrix $(A^0b_1,\, A^1b_1,\, A^2b_1,\; A^0b_2)$ in die Spaltenstufenform

$$\left(\begin{array}{rrrr} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & -1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ \hline 1 & -4 & 5 & 0\\ 0 & 4 & -7 & 0\\ 0 & -1 & 2 & 0\\ 0 & 0 & 0 & 1 \end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ \\ \end{array} \rightsquigarrow \left(\begin{array}{rrrr} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0\\ \hline 1 & 0 & 1 & -4\\ 0 & 0 & -3 & 4\\ 0 & 0 & 1 & -1\\ 0 & 1 & -1 & -1 \end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ \\ \end{array} .$$

Würde uns nur das charakteristische Polynom, und nicht auch die Matrix $T^{-1}AT$ interessieren, so wären die mit $*$ markierten Zeilen überflüssig und müßten nicht mitgeführt werden.

Es wird $Ab_2 = \begin{pmatrix} 2\\3\\1\\1\\1\\1 \end{pmatrix}$. Unter Verwendung der vorhergehenden Spaltenstufenform bringen wir nun auch die Matrix $(A^0b_1,\, A^1b_1,\, A^2b_1,\; A^0b_2,\, A^1b_2)$ in die Spaltenstufenform

$$\left(\begin{array}{rrrrr} 1 & 0 & 0 & 0 & 2\\ 0 & 1 & 0 & 0 & 3\\ 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\\ 0 & 0 & 1 & 0 & 1\\ \hline 1 & 0 & 1 & -4 & 0\\ 0 & 0 & -3 & 4 & 0\\ 0 & 0 & 1 & -1 & 0\\ 0 & 1 & -1 & -1 & 0\\ 0 & 0 & 0 & 0 & 1 \end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ \\ \\ \end{array} \rightsquigarrow \left(\begin{array}{rrrrr} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 & 0\\ \hline 1 & 0 & 2 & -3 & -1\\ 0 & 0 & -4 & 3 & 1\\ 0 & 0 & 1 & -1 & 0\\ 0 & 1 & -2 & -2 & 1\\ 0 & 0 & 1 & 1 & -1 \end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ \\ \\ \end{array} .$$

Es wird $A^2b_2 = A(Ab_2) = \begin{pmatrix} 9\\9\\5\\4\\5\\5 \end{pmatrix}$. Unter Verwendung der vorhergehenden Spaltenstufenform bringen wir nun auch die Matrix $(A^0b_1,\, A^1b_1,\, A^2b_1,\; A^0b_2,\, A^1b_2)$ in die Spaltenstufenform

$$\left(\begin{array}{rrrrrr}
1 & 0 & 0 & 0 & 0 & 9 \\
0 & 1 & 0 & 0 & 0 & 9 \\
0 & 0 & 1 & 0 & 0 & 5 \\
0 & 0 & 0 & 1 & 0 & 4 \\
0 & 0 & 0 & 0 & 1 & 5 \\
0 & 0 & 1 & 0 & 0 & 5 \\
\hline
1 & 0 & 2 & -3 & -1 & 0 \\
0 & 0 & -4 & 3 & 1 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 \\
0 & 1 & -2 & -2 & 1 & 0 \\
0 & 0 & 1 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ \\ \\ \\ \end{array}
\rightsquigarrow
\left(\begin{array}{rrrrrr}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
\hline
1 & 0 & 2 & -3 & -1 & -2 \\
0 & 0 & -4 & 3 & 1 & 3 \\
0 & 0 & 1 & -1 & 0 & -1 \\
0 & 1 & -2 & -2 & 1 & 4 \\
0 & 0 & 1 & 1 & -1 & -4 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ \\ \\ \\ \end{array} .$$

Wir entnehmen der letzten Spalte der mitgeführten Matrix, daß

$$A^2b_1 - 4A^1b_2 + 4A^0b_2 - A^2b_1 + 3A^1b_1 - 2A^0b_1 \;=\; 0 \,,$$

und also insbesondere, daß

$$A^2b_1 - 4A^1b_2 + 4A^0b_2 \in W_1 \,.$$

Schritt 3. Sei $b_3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Zufälligerweise konnten wir als Anfangsvektoren die ersten drei Standardbasisvektoren wählen. Man kann immer Standardbasisvektoren wählen, muß aber gegebenenfalls welche auslassen, falls sie im bereits erreichten Erzeugnis liegen. Läge z.B. b_3 im bereits erreichten Erzeugnis W_2, so hätten wir b_3 nicht nehmen können, und hätten dann untersucht, ob b_4 nicht in W_2 liegt. Usf.

Unter Verwendung der vorletzten Spaltenstufenform in Schritt 1 bringen wir nun auch die Matrix $(A^0b_1,\ A^1b_1,\ A^2b_1,\ A^0b_2,\ A^1b_2,\ A^0b_3)$ in die Spaltenstufenform

$$\left(\begin{array}{rrrrrr}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
\hline
1 & 0 & 2 & -3 & -1 & 0 \\
0 & 0 & -4 & 3 & 1 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 \\
0 & 1 & -2 & -2 & 1 & 0 \\
0 & 0 & 1 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ * \\ * \\ \\ \end{array}
\rightsquigarrow
\left(\begin{array}{rrrrrr}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & -3 & -1 & 2 \\
0 & 0 & 0 & 3 & 1 & -4 \\
0 & 0 & 0 & -1 & 0 & 1 \\
0 & 1 & 0 & -2 & 1 & -2 \\
0 & 0 & 0 & 1 & -1 & 1 \\
0 & 0 & 1 & 0 & 0 & -1
\end{array}\right)\begin{array}{c} \\ \\ \\ \\ \\ \\ * \\ * \\ * \\ * \\ * \\ \\ \end{array} .$$

Würde uns nur das charakteristische Polynom, und nicht auch die Matrix $T^{-1}AT$ interessieren, so wären die mit $*$ markierten Zeilen überflüssig und müßten nicht mitgeführt werden.

Es wird $Ab_3 = \begin{pmatrix} 1 \\ 0 \\ 2 \\ -1 \\ 0 \\ 1 \end{pmatrix}$. Unter Verwendung der vorhergehenden Spaltenstufenform bringen wir nun auch die Matrix $(A^0b_1,\ A^1b_1,\ A^2b_1,\ A^0b_2,\ A^1b_2,\ A^0b_3,\ A^1b_3)$ in die Spaltenstufenform

$$\left(\begin{array}{ccccccc} 1&0&0&0&0&0&1\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&2\\ 0&0&0&1&0&0&-1\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&1\\ \hline 1&0&0&-3&-1&2&0\\ 0&0&0&3&1&-4&0\\ 0&0&0&-1&0&1&0\\ 0&1&0&-2&1&-2&0\\ 0&0&0&1&-1&1&0\\ 0&0&1&0&0&-1&0\\ 0&0&0&0&0&0&1 \end{array}\right)\begin{array}{c}\\ \\ \\ \\ \\ \\ *\\ *\\ *\\ *\\ *\\ \\ \\ \end{array} \rightsquigarrow \left(\begin{array}{ccccccc} 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ \hline 1&0&0&-3&-1&2&-6\\ 0&0&0&3&1&-4&7\\ 0&0&0&-1&0&1&-2\\ 0&1&0&-2&1&-2&0\\ 0&0&0&1&-1&1&0\\ 0&0&1&0&0&-1&-1\\ 0&0&0&0&0&0&1 \end{array}\right)\begin{array}{c}\\ \\ \\ \\ \\ \\ *\\ *\\ *\\ *\\ *\\ \\ \\ \end{array} .$$

Wir entnehmen der letzten Spalte der mitgeführten Matrix, daß

$$A^1b_3 - A^0b_3 + 0A^1b_2 + 0A^0b_2 - 2A^2b_1 + 7A^1b_1 - 6A^0b_1 \;=\; 0\;,$$

und also insbesondere, daß

$$A^1b_3 - A^0b_3 \in W_2\;.$$

Das charakteristische Polynom ergibt sich also zu

$$\chi_A(X) \;=\; (X^3 - 5X^2 + 8X^1 - 4X^0)(X^2 - 4X^1 + 4X^0)(X^1 - X^0) = (X-2)^4(X-1)^2\;,$$

wobei der Faktor dritten Grades nur durch Erraten einer Nullstelle zerlegt wurde – Teiler des konstanten Terms sind gute Kandidaten.

Ist nun

$$T \;=\; (A^0b_1,\ A^1b_1,\ A^2b_1,\ A^0b_2,\ A^1b_2,\ A^0b_3) \;=\; \begin{pmatrix} 1&3&8&0&2&0\\ 0&2&7&1&3&0\\ 0&1&4&0&1&1\\ 0&1&3&0&1&0\\ 0&2&7&0&1&0\\ 0&1&4&0&1&0 \end{pmatrix} \;\in\; \mathrm{GL}_6(\mathbf{C})\;,$$

so erkennen wir auch ohne langwierige Berechnung von T^{-1}, daß

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

Bemerkung. Für die Bestimmung der Jordanform von A im folgenden Kapitel kann anstelle von A auch die hier gefundene Matrix $\tilde{A} = T^{-1}AT$ verwandt werden. Beides führt zur Jordanform von A. Dies kann insbesondere dann von Nutzen sein, wenn die hier angeführte Methode zur Berechnung von $\chi_A(X)$ ohnehin durchgeführt wurde.

4.3 Die Jordanform

Ein Endomorphismus $V \xrightarrow{f} V$ eines endlichdimensionalen Vektorraums V über K kann auf verschiedene Weisen durch Matrizen beschrieben werden – für jede Basis $\underline{y}$ von V erhalten wir eine Matrix $A = A(f)_{\underline{y},\underline{y}}$. Ein Basiswechsel von $\underline{y}$ nach $\underline{z}$ gibt uns alternativ eine Matrix $S^{-1}AS$ zur Beschreibung, wobei $S = A(1_V)_{\underline{y},\underline{z}}$. Wir fragen, ob für $V \xrightarrow{f} V$ eine Basis $\underline{z}$

existiert, zu welcher sich die beschreibende Matrix $A(f)_{\underline{z},\underline{z}}$ in besonders einfacher Gestalt ergibt. Optimal wäre eine Diagonalmatrix, nur ist dies im allgemeinen nicht möglich. So etwa ist dies für $x \longmapsto \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) x$ unmöglich. (Allgemeiner ist für $f \neq 0$ mit $f^m = 0$ für ein $m \geqslant 2$ eine diagonale Beschreibung unmöglich, da die beschreibende Matrix diese Eigenschaft dann ebenfalls haben müßte, und eine Diagonalmatrix diese Eigenschaft nicht haben kann.) Wir werden eine um eine Nebendiagonale ergänzte Diagonalmatrix konstruieren, die sogenannte Jordanform.

4.3.1 Zerlegung in Haupträume

Gegeben sei $A \in K^{n\times n}$. Für ein Polynom $f(X) = \sum_{i\geqslant 0} a_i X^i \in K[X]$ schreiben wir $f(A) := \sum_{i\geqslant 0} a_i A^i \in K^{n\times n}$. Hierbei schreiben wir gelegentlich auch einfach μ anstelle von $\mu A^0 = \mu E$ für $\mu \in K$.

Lemma von Schur (einfache Version). *Sei $\chi_A(X) = \prod_{i\in[1,n]}(X - \lambda_i)$ in Linearfaktoren zerlegt, wobei die Reihenfolge der Eigenwerte beliebig gewählt werden kann. Dann gibt es eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ so, daß $S^{-1}AS$ eine obere Dreiecksmatrix bildet, mit den Eigenwerten in dieser Reihenfolge auf der Diagonalen. D.h. schreiben wir $S^{-1}AS = (c_{j,k})_{j,k}$, so ist $c_{j,k} = 0$ für $j, k \in [1, n]$ mit $j > k$, und $c_{j,j} = \lambda_j$ für $j \in [1, n]$.*

Beweis. Es genügt zu zeigen, daß wir eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ so finden können, daß mit $S^{-1}AS = (c_{j,k})_{j,k}$ zumindest $c_{j,1} = 0$ ist für $j \in [2, n]$, und $c_{1,1} = \lambda_1$, d.h. so, daß die erste Spalte bis auf den Diagonaleintrag λ_1 verschwindet.

Sei dann nämlich $B := (c_{j,k})_{j,k\in[2,n]}$. Da $\prod_{i\in[1,n]}(X - \lambda_i) = \chi_{S^{-1}AS}(X) = (X - \lambda_1)\chi_B(X)$, folgt $\chi_B(X) = \prod_{i\in[2,n]}(X - \lambda_i)$. Also können wir mit Induktion eine invertierbare Matrix $T \in \mathrm{GL}_{n-1}(K)$ finden, die die Matrix $B := (c_{j,k})_{j,k\in[2,n]}$ in obere Dreiecksform mit der Diagonalen $(\lambda_2, \ldots, \lambda_n)$ konjugiert. Schreiben wir $U \in K^{n\times n}$ für die Blockdiagonalmatrix mit den Blöcken $E_1 = (1)$ und T, so ist auch SU invertierbar, und $(SU)^{-1}A(SU) = U^{-1}(S^{-1}AS)U$ ist in oberer Dreiecksform mit der geforderten Diagonalen.

Wir schreiben nun dazu $S = (s_{j,k})_{j,k}$ und setzen als erste Spalte $s_{*,1}$ einen Eigenvektor von A zum Eigenwert λ_1 ein. Sodann ergänzen wir diese Spalte mit Basisergänzung zu einer invertierbaren Matrix S. Nun ist die erste Spalte von $S^{-1}AS$ gegeben durch

$$S^{-1}As_{*,1} \;=\; S^{-1}(\lambda s_{*,1}) \;=\; \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix} .$$

□

Satz 12 (Cayley-Hamilton) *Es ist $\chi_A(A) = 0$.*

Beweis. Mit Schurs Lemma in einfacher Version dürfen wir annehmen, daß sich A in oberer Dreiecksform befindet. Denn für S invertierbar ist $S^{-1}\chi_A(A)S = \chi_A(S^{-1}AS) = \chi_{S^{-1}AS}(S^{-1}AS)$, und mithin $\chi_A(A) = 0$ äquivalent zu $\chi_{S^{-1}AS}(S^{-1}AS) = 0$.

Wir schreiben $A = (a_{i,j})_{i,j}$. Wir führen eine Induktion über n. Die Behauptung trifft zu für $n = 1$, da das charakteristische Polynom $X - a_{1,1}$ von $(a_{1,1})$ diese Matrix annulliert.

Sei $n \geqslant 2$. Sei $B = (a_{i,j})_{i,j \in [2,n]} \in K^{(n-1)\times(n-1)}$ die Matrix im rechten unteren Eck von A, so daß also $A = \left(\begin{smallmatrix} a_{1,1} & * \\ 0 & B \end{smallmatrix}\right)$. Nach Induktionsvoraussetzung ist $\chi_B(B) = 0$, und damit $\chi_B(A) = \left(\begin{smallmatrix} * & * \\ 0 & 0 \end{smallmatrix}\right)$, unter Beibehaltung der Blockeinteilung. Nun ist $\chi_A(X) = (X - a_{1,1})\chi_B(X)$ nach dem Lemma über Determinanten von Blockdreiecksmatrizen. Es wird somit

$$\chi_A(A) \;=\; (A - a_{1,1}E)\chi_B(A) \;=\; \left(\begin{smallmatrix} 0 & * \\ 0 & * \end{smallmatrix}\right)\left(\begin{smallmatrix} * & * \\ 0 & 0 \end{smallmatrix}\right) \;=\; 0\,.$$

□

Hauptraum. Sei λ ein Eigenwert von A. Der *Hauptraum* von A zum Eigenwert λ sei gegeben durch

$$H_A(\lambda) \;:=\; \{x \in K^n \mid \text{es gibt ein } m \geqslant 1 \text{ mit } (\lambda E - A)^m x = 0\}\,.$$

Dies ist ein Unterraum von K^n, da mit $(\lambda E - A)^r y = 0$, $(\lambda E - A)^s z = 0$ und $\mu, \nu \in K$ auch $(\lambda E - A)^{\max\{r,s\}}(\mu y + \nu z) = 0$ gilt. Unter Verwendung von $m = 1$ sieht man $E_A(\lambda) \leqslant H_A(\lambda)$. Genauso wie für den Eigenraum sieht man, daß $S \cdot H_{S^{-1}AS}(\lambda) = H_A(\lambda)$.

Beispiel. Sei $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in \mathbf{C}^{2\times 2}$. Dann ist $E_A(0) = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle$ und $H_A(0) = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \rangle$.

Lemma. *Sei λ ein Eigenwert von A mit algebraischer Vielfachheit m. Folgendes gilt.*

(i) *Es ist* $H_A(\lambda) = \operatorname{Kern}(A - \lambda E)^m$.

(ii) *Es ist* $\dim H_A(\lambda) = m$.

Beweis. Da für S invertierbar $H_{S^{-1}AS}(\lambda) = S^{-1}H_A(\lambda)$ und $\operatorname{Kern}(S^{-1}AS - \lambda E)^m = \operatorname{Kern} S^{-1}(A - \lambda E)^m S = S^{-1}\operatorname{Kern}(A - \lambda E)^m$ sind, sind die Aussagen (i, ii) für A äquivalent zu den Aussagen (i, ii) für $S^{-1}AS$. Also dürfen wir mit Schurs Lemma in einfacher Version annehmen, daß sich A in oberer Dreiecksform befindet, und zwar mit den Eigenwerten in beliebig gewählter Reihenfolge auf der Diagonalen. So können wir etwa annehmen, daß links oben in A die Diagonaleinträge in den Positionen (j,j) für $j \in [1,m]$ gleich λ sind.

Da $n-m$ Diagonaleinträge von A ungleich λ sind, ist für alle $l \geqslant 1$ der Rang $\operatorname{rk}(A - \lambda E)^l \geqslant n - m$, d.h. $\dim \operatorname{Kern}(A - \lambda E)^l \leqslant m$.

Schreiben wir $B = (a_{i,j})_{i,j \in [1,m]}$ für den $m \times m$-Block im linken oberen Eck von A, so ist $B - \lambda E$ eine obere Dreiecksmatrix mit Nullen auf der Diagonalen, und mithin $(B - \lambda E)^m = 0$. Somit ist $\dim \operatorname{Kern}(A - \lambda E)^m = m$. Wegen $\operatorname{Kern}(A - \lambda E)^m \leqslant \operatorname{Kern}(A - \lambda E)^l$ für $m \leqslant l$ folgt aus der Gleichheit der Dimensionen die Gleichheit der Unterräume, und also $H_A(\lambda) = \operatorname{Kern}(A - \lambda E)^m$. Dessen Dimension ist, wie eben festgestellt, gleich m. □

Bemerkung. Aus (ii) und aus $E_A(\lambda) \leqslant H_A(\lambda)$ folgt, daß die geometrische Vielfachheit eines Eigenwertes λ von A kleiner oder gleich seiner algebraischen Vielfachheit ist, wobei Gleichheit genau dann eintritt, wenn $E_A(\lambda) = H_A(\lambda)$.

Lemma. *Sei $f(X) \in K[X] \smallsetminus \{0\}$ so, daß $f(A) = 0$. Sei $f(X) = \prod_{i \in [1,k]} g_i(X)$ in Faktoren von Grad $\geqslant 1$ ohne gemeinsame Nullstelle in K zerlegt; d.h. ist $g_i(\lambda) = 0$ und $g_j(\lambda) = 0$ für ein $\lambda \in K$, so ist notwendig bereits $i = j$. Dann ist*

$$K^n \;=\; \bigoplus_{i \in [1,k]} \operatorname{Kern} g_i(A)\,.$$

Beweis. Wir können $k \geqslant 2$ annehmen. Für $j \in [1,k]$ schreiben wir $\tilde{g}_j(X) := \prod_{i\in[1,k]\smallsetminus\{j\}} g_i(X)$.

Jedes Ideal in $K[X]$ ungleich $\{0\}$ ist von der Form $h(X)K[X]$ für ein normiertes Polynom $h(X)$; und so finden wir auch

$$\left\{ \sum_{i\in[1,k]} u_i(X)\tilde{g}_i(X) \;\middle|\; u_i(X) \in K[X] \right\} \;=\; h(X)K[X]\;.$$

Da sich insbesondere $\tilde{g}_i(X) = v_i(X)h(X)$ schreiben lassen für $i \in [1,k]$, wäre jede Nullstelle von $h(X)$ eine gemeinsame Nullstelle aller Polynome $\tilde{g}_i(X)$ und damit auch eine gemeinsame Nullstelle wenigstens zweier Polynome $g_i(X)$, $g_j(X)$ für $i,j \in [1,k]$ mit $i \neq j$. Da dies ausgeschlossen ist, muß $h(X) = 1$ sein. Mithin können wir auch Polynome $u_i(X) \in K[X]$ so finden, daß $\sum_{i\in[1,k]} u_i(X)\tilde{g}_i(X) = 1$. Einen Vektor $x \in K^n$ können wir also schreiben als

$$x \;=\; Ex \;=\; \sum_{i\in[1,k]} \tilde{g}_i(A)u_i(A)x \;\in\; \sum_{i\in[1,k]} \operatorname{Im}\tilde{g}_i(A)\;,$$

woraus wir $K^n = \sum_{i\in[1,k]} \operatorname{Im}\tilde{g}_i(A)$ ersehen.

Wir behaupten, daß $\operatorname{Kern} g_j(A) = \operatorname{Im}\tilde{g}_j(A)$. Wegen $g_j(A)\tilde{g}_j(A) = f(A) = 0$ ist $\operatorname{Im}\tilde{g}_j(A) \leqslant \operatorname{Kern} g_j(A)$. Für die umgekehrte Inklusion finden wir mangels gemeinsamer Nullstelle zunächst wie oben $v(X), w(X) \in K[X]$ mit $v(X)g_j(X) + w(X)\tilde{g}_j(X) = 1$. Ist nun $x \in \operatorname{Kern} g_j(A)$, so wird

$$x \;=\; (v(A)g_j(A) + w(A)\tilde{g}_j(A))x \;=\; w(A)\tilde{g}_j(A)x \;=\; \tilde{g}_j(A)w(A)x \;\in\; \operatorname{Im}\tilde{g}_j(A)\;.$$

Nun behaupten wir, daß $\sum_{i\in[1,k]} \operatorname{Im}\tilde{g}_j(A) = \bigoplus_{i\in[1,k]} \operatorname{Im}\tilde{g}_j(A)$, d.h. daß diese Summe direkt ist. Sei $j \in [1,k]$, und sei

$$x \;\in\; \operatorname{Im}\tilde{g}_j(A) \cap \sum_{i\in[1,k]\smallsetminus\{j\}} \operatorname{Im}\tilde{g}_i(A)\;.$$

Dann ist zum einen $x \in \operatorname{Kern} g_j(A)$, so daß wir wie oben ein $w(X) \in K[X]$ mit $x = w(A)\tilde{g}_j(A)x$ finden können. Dazuhin können wir noch $x = \sum_{i\in[1,k]\smallsetminus\{j\}} \tilde{g}_i(A)x_i$ mit gewissen $x_i \in K^n$ schreiben. Insgesamt wird

$$x \;=\; w(A)\tilde{g}_j(A)x \;=\; w(A)\tilde{g}_j(A) \sum_{i\in[1,k]\smallsetminus\{j\}} \tilde{g}_i(A)x_i \;=\; 0\;,$$

da $f(X)$ die Produkte $\tilde{g}_j(X)\tilde{g}_i(X)$ teilt, und somit aus $f(A) = 0$ auch $\tilde{g}_j(A)\tilde{g}_i(A) = 0$ folgt.

Insgesamt haben wir $K^n = \bigoplus_{i\in[1,k]} \operatorname{Kern} g_i(A)$ gezeigt. $\square$

Wir fassen zusammen. Dazu sei zunächst vereinbart, daß eine lineare Abbildung $V \xrightarrow{f} V$ eines Vektorraums V in sich *nilpotent* heiße, falls es ein $m \geqslant 1$ mit $f^m = 0$ gibt. Analog heiße eine Matrix $N \in K^{n\times n}$ *nilpotent,* falls es ein $m \geqslant 1$ mit $N^m = 0$ gibt. Eine nilpotente Matrix N hat 0 als einzigen Eigenwert, da $Nx = \lambda x$ mit $x \in K^n \smallsetminus \{0\}$ zur Folge hat, daß $0 = N^m x = \lambda^m x$, und somit $\lambda = 0$.

Hauptzerlegungslemma. *Sei $\chi_A(X) = \prod_{i\in[1,k]}(X-\lambda_i)^{m_i}$, wobei $\lambda_i \neq \lambda_j$ für $i \neq j$ und $m_i \geqslant 1$ stets. Dann ist*

$$K^n \;=\; \bigoplus_{i\in[1,k]} H_A(\lambda_i)$$

Dabei ist $H_A(\lambda_j) = \mathrm{Kern}(A-\lambda_j)^{m_j}$, sowie $\dim H_A(\lambda_j) = m_j$ die algebraische Vielfachheit des Eigenwertes λ_j, für $j \in [1,k]$.

Insbesondere gibt es eine Basiswechselmatrix $S \in \mathrm{GL}_n(\mathbf{C})$, mit Spaltentupel einer aus Hauptraumbasen zusammengesetzten Basis, derart, daß $S^{-1}AS = \mathrm{diag}(A_1,\ldots,A_k)$ eine Hauptdiagonalblockmatrix ist, und derart, daß $A_j \in K^{m_j\times m_j}$ das charakteristische Polynom $\chi_{A_j}(X) = (X-\lambda_j)^{m_j}$ besitzt für $j \in [1,k]$.

Beweis. Die direkte Zerlegung folgt mit vorigem Lemma unter Verwendung von $g_j(X) = (X-\lambda_j)^{m_j}$, da mit vorvorigem Lemma $\mathrm{Kern}(A-\lambda_j)^{m_j} = H_A(\lambda_j)$.

Die Blockzerlegung einer konjugierten Matrix $S^{-1}AS$ erhält man durch Einstellen der Basisvektoren der Haupträume in die Spalten einer Matrix S.

Die eingeschränkte lineare Abbildung $H_A(\lambda_j) \longrightarrow H_A(\lambda_j)$, $x \longmapsto (A-\lambda_j E)x$, ist nilpotent, da zunächst $x \longmapsto (A-\lambda_j E)x$ den Hauptraum $H_A(\lambda_j)$ in sich überführt, und dazuhin jeder Vektor in $H_A(\lambda_j)$ von einer Potenz von $A-\lambda_j E$ annulliert wird. Die beschreibende Matrix dieser eingeschränkten Abbildung bezüglich der in die Spalten von S eingestellten Basis von $H_A(\lambda_j)$ ist gegeben durch $A_j - \lambda_j E \in K^{m_j\times m_j}$. Diese Matrix $A_j - \lambda_j E$ hat als nilpotente Matrix das charakteristische Polynom X^{m_j}, und somit hat A_j selbst das charakteristische Polynom

$$\chi_{A_j}(X) \;=\; \det(XE-A_j) \;=\; \det((X-\lambda_j)E-(A_j-\lambda_j E)) \;=\; \chi_{A_j-\lambda_j E}(X-\lambda_j) \;=\; (X-\lambda_j)^{m_j}\ .$$

(Durch $\prod_{j\in[1,k]} \chi_{A_j}(X) = \chi_{S^{-1}AS}(X) = \chi_A(X)$ wird der Exponent in $\chi_{A_j}(X) = (X-\lambda_j)^{m_j}$ abermals bestätigt.) □

4.3.2 Jordanform nilpotenter Matrizen

Mit dem Hauptzerlegungslemma können wir eine Matrix in Hauptdiagonalblockgestalt konjugieren, und dies derart, daß die Hauptdiagonalblöcke minus einem gewissen Vielfachen der Einheitsmatrix nilpotent sind. Bleibt uns also, nilpotente Matrizen in Form zu bringen.

Der für das folgenden Lemma dargelegte Beweis enthält bereits den wesentlichen Teil des Konstruktionsverfahrens der Jordanform.

Wir fassen die auftretenden Tupel von Vektoren in der Notation wie gehabt zusammen. So z.B. sei $y_{3;2}$ der 2te Vektor des Tupels $\underline{y}_3$. Ist ferner $\underline{z} = (z_1,\ldots,z_l)$ ein Tupel von Vektoren in K^n, und ist $B \in K^{n\times n}$, so sei $B\underline{z} := (Bz_1, \dots, Bz_l)$. Ist schließlich $\underline{z}' = (z'_1, \dots, z'_{l'})$ ein weiteres Tupel von Vektoren in K^n, dann bezeichne $(\underline{z}, \underline{z}') = (z_1, \dots, z_l, z'_1, \dots, z'_{l'})$ das zusammengesetzte Tupel.

Nilpotenzlemma. *Sei* $N \in K^{n\times n}$ nilpotent, *d.h. gebe es ein* $m \geqslant 1$ *mit* $N^m = 0$. *Wähle* m *minimal mit dieser Eigenschaft.*

Es gibt ein linear unabhängiges Tupel $\underline{x}_m = (x_{m;1}, \dots, x_{m;g_m})$ *in* $\mathrm{Kern}(N^m)$ $(= K^n)$ *mit*

$$\mathrm{Kern}(N^{m-1}) \oplus \underbrace{\langle x_{m;1}, \dots, x_{m;g_m}\rangle}_{=:\, U_m} \;=\; \mathrm{Kern}(N^m)\ (= K^n)\ .$$

Es gibt ein linear unabhängiges Tupel $\underline{x}_{m-1} = (x_{m-1;1}, \dots, x_{m-1;g_{m-1}})$ *in* $\mathrm{Kern}(N^{m-1})$ *mit*

$$\mathrm{Kern}(N^{m-2}) \oplus \underbrace{NU_m \oplus \langle x_{m-1;1}, \dots, x_{m-1;g_{m-1}}\rangle}_{=:\, U_{m-1}} \;=\; \mathrm{Kern}(N^{m-1})\ .$$

Es gibt ein linear unabhängiges Tupel $\underline{x}_{m-2} = (x_{m-2;1}, \dots, x_{m-2;g_{m-2}})$ *in* $\mathrm{Kern}(N^{m-2})$ *mit*

$$\mathrm{Kern}(N^{m-3}) \oplus \underbrace{NU_{m-1} \oplus \langle x_{m-2;1}, \dots, x_{m-2;g_{m-2}}\rangle}_{=:\, U_{m-2}} \;=\; \mathrm{Kern}(N^{m-2})\ .$$

Und so fort, bis zu $g_1 \geqslant 0$ *und zum Tupel* $\underline{x}_1 = (x_{1;1}, \dots, x_{1;g_1})$ *in* $\mathrm{Kern}(N^1)$ *mit*

$$\underbrace{\mathrm{Kern}(N^0)}_{=\,0} \oplus \underbrace{NU_2 \oplus \langle x_{1;1}, \dots, x_{1;g_1}\rangle}_{=:\, U_1} \;=\; \mathrm{Kern}(N^1)\ .$$

Das Tupel aller hierbei in Erscheinung tretenden Vektoren

$$(N^i x_{j;s} \mid j \in [1, m],\ s \in [1, g_j],\ i \in [0, j-1])$$

ist eine Basis von K^n.

Beweis. Zugleich mit der Auswahl der Tupel $\underline{x}_j$ in der velangten Form behaupten wir, daß das erzeugende Tupel $(N^{m-j}\underline{x}_m, N^{m-j-1}\underline{x}_{m-1}, \dots, N^0\underline{x}_j)$ von U_j linear unabhängig ist für alle $j \in [1, m]$.

Wir bemerken zunächst, daß

$$0 \;=\; \mathrm{Kern}(N^0) \;\leqslant\; \mathrm{Kern}(N^1) \;\leqslant\; \mathrm{Kern}(N^2) \;\leqslant\; \cdots \;\leqslant\; \mathrm{Kern}(N^m) \;=\; K^n\ .$$

Wir wählen eine Basis $\underline{y}_1$ von $\mathrm{Kern}(N^1)$, ergänzen diese zu einer Basis $(\underline{y}_1, \underline{y}_2)$ von $\mathrm{Kern}(N^2)$, und so fort, bis zu einer Basis

$$(\underline{y}_1, \underline{y}_2,\ \dots,\ \underline{y}_m)$$

von $\mathrm{Kern}(N^m) = K^n$.

Wir zählen die folgenden Schritte rückwärts, dementsprechend, in welchem *Level* wir uns gerade befinden. Die Konstruktion bricht ab, sobald Level 1 abgearbeitet ist. Befinden wir uns also in Level j, so hat dies $j \geqslant 1$ zur Voraussetzung.

Level m. Wir wählen $\underline{x}_m = \underline{y}_m$ und erhalten so die Zerlegung

$$\mathrm{Kern}(N^{m-1}) \oplus \underbrace{\langle \underline{x}_m \rangle}_{= U_m} \;=\; \mathrm{Kern}(N^m)\,.$$

Level $m-1$. Die Abbildung $U_m \longrightarrow NU_m : u \longmapsto Nu$ ist ein Isomorphismus, da Elemente im Kern dieser Surjektion in $\mathrm{Kern}(N) \,\cap\, U_m \;\leqslant\; \mathrm{Kern}(N^{m-1}) \,\cap\, U_m = 0$ liegen. Auch ist die Summe $\mathrm{Kern}(N^{m-2}) + NU_m$ direkt, da $u \in U_m$ mit $Nu \in \mathrm{Kern}(N^{m-2})$ notwendig $u \in \mathrm{Kern}(N^{m-1}) \cap U_m = 0$ nach sich zieht.

In $\mathrm{Kern}(N^{m-1})$ liefert nun Basisergänzung des mithin linear unabhängigen Tupels

$$(\underline{y}_1, \underline{y}_2, \ldots, \underline{y}_{m-2}, N^1\underline{x}_m)$$

um ein Tupel $\underline{x}_{m-1}$, welches aus $\underline{y}_{m-1}$ ausgewählt werden kann, zu einer Basis

$$(\underline{y}_1, \underline{y}_2, \ldots, \underline{y}_{m-2}, N^1\underline{x}_m, N^0\underline{x}_{m-1})$$

von $\mathrm{Kern}(N^{m-1})$ die Zerlegung

$$\mathrm{Kern}(N^{m-2}) \oplus \underbrace{NU_m \oplus \langle \underline{x}_{m-1} \rangle}_{= U_{m-1}} \;=\; \mathrm{Kern}(N^{m-1})\,.$$

Das erzeugende Tupel $(N^1\underline{x}_m, N^0\underline{x}_{m-1})$ von U_{m-1} ist ein Teiltupel dieser ergänzten Basis, und damit linear unabhängig.

Level $m-2$. Die Abbildung $U_{m-1} \longrightarrow NU_{m-1} : u \longmapsto Nu$ ist ein Isomorphismus, da Elemente im Kern dieser Surjektion in $\mathrm{Kern}(N) \cap U_{m-1} \;\leqslant\; \mathrm{Kern}(N^{m-2}) \cap U_{m-1} = 0$ liegen. Auch ist die Summe $\mathrm{Kern}(N^{m-3}) + NU_{m-1}$ direkt, da $u \in U_{m-1}$ mit $Nu \in \mathrm{Kern}(N^{m-3})$ notwendig $u \in \mathrm{Kern}(N^{m-2}) \cap U_{m-1} = 0$ nach sich zieht.

In $\mathrm{Kern}(N^{m-2})$ liefert nun Basisergänzung des mithin linear unabhängigen Tupels

$$(\underline{y}_1, \underline{y}_2, \ldots, \underline{y}_{m-3}, N^2\underline{x}_m, N^1\underline{x}_{m-1})$$

um ein Tupel $\underline{x}_{m-2}$, welches aus $\underline{y}_{m-2}$ ausgewählt werden kann, zu einer Basis

$$(\underline{y}_1, \underline{y}_2, \ldots, \underline{y}_{m-3}, N^2\underline{x}_m, N^1\underline{x}_{m-1}, N^0\underline{x}_{m-2})$$

von $\mathrm{Kern}(N^{m-2})$ die Zerlegung

$$\mathrm{Kern}(N^{m-3}) \oplus \underbrace{NU_{m-1} \oplus \langle \underline{x}_{m-2} \rangle}_{= U_{m-2}} \;=\; \mathrm{Kern}(N^{m-2})\,.$$

Das erzeugende Tupel $(N^2\underline{x}_m, N^1\underline{x}_{m-1}, N^0\underline{x}_{m-2})$ von U_{m-2} ist ein Teiltupel dieser ergänzten Basis, und damit linear unabhängig.

Level zwischen $m-3$ *und* 2. Wir setzen so fort.

Level 1. Die Abbildung $U_2 \longrightarrow NU_2 : u \longmapsto Nu$ ist ein Isomorphismus, da Elemente im Kern dieser Surjektion in $\mathrm{Kern}(N^1) \cap U_2 = 0$ liegen. Die Summe $\mathrm{Kern}(N^0) + NU_2$ ist hier schon deshalb direkt, weil $\mathrm{Kern}(N^0) = 0$ ist.

In $\mathrm{Kern}(N^1)$ liefert nun Basisergänzung des mithin linear unabhängigen Tupels

$$(N^{m-1}\underline{x}_m, N^{m-2}\underline{x}_{m-1}, \ldots, N^1\underline{x}_2)$$

um ein Tupel $\underline{x}_1$, welches aus $\underline{y}_1$ ausgewählt werden kann, zu einer Basis

$$(N^{m-1}\underline{x}_m, N^{m-2}\underline{x}_{m-1}, \ldots, N^1\underline{x}_2, N^0\underline{x}_1)$$

von $\mathrm{Kern}(N^{m-2})$ die Zerlegung

$$\mathrm{Kern}(N^0) \oplus \underbrace{NU_2 \oplus \langle \underline{x}_1 \rangle}_{= U_1} \;=\; \mathrm{Kern}(N^1)\ .$$

Das erzeugende Tupel $(N^{m-1}\underline{x}_m, N^{m-2}\underline{x}_{m-1}, \ldots, N^1\underline{x}_2, N^0\underline{x}_1)$ von U_1 ist hier nun als Basis insbesondere linear unabhängig.

Basis. Bleibt zu zeigen, daß $(N^d\underline{x}_{j+d} \mid j \in [1,m],\ d \in [0, m-j])$ eine Basis des Vektorraums K^n ist. Eben wurde eingesehen, daß für jedes $j \in [1,m]$ das Tupel $(N^d\underline{x}_{j+d} \mid d \in [0, m-j])$ eine Basis von U_j ist. Die Behauptung folgt nun mit der direkten Summenzerlegung

$$K^n \;=\; \mathrm{Kern}\, N^{m-1} \oplus U_m \;=\; \mathrm{Kern}\, N^{m-2} \oplus U_{m-1} \oplus U_m \;=\; \cdots \;=\; U_1 \oplus \cdots \oplus U_{m-1} \oplus U_m\ .$$

□

Bemerkung. Zur bequemen Berechnung der Basis $(\underline{y}_1, \underline{y}_2, \ldots, \underline{y}_m)$ von K^n bedienen wir uns folgender Vereinfachung.

Zur Bestimmung des Kerns von N bringen wir die Matrix N durch Zeilenumformungen auf Zeilenstufenform $G_1 N = Z_1$, mit $G_1 \in \mathrm{GL}_n(K)$. Dann ist $\mathrm{Kern}\, Z_1 = \mathrm{Kern}(G_1 N) = \mathrm{Kern}\, N$.

Zur Bestimmung des Kerns von N^2 bringen wir die Matrix $Z_1 N$ durch Zeilenumformungen auf Zeilenstufenform $G_2 Z_1 N = Z_2$, mit $G_2 \in \mathrm{GL}_n(K)$. Dann ist $\mathrm{Kern}\, Z_2 = \mathrm{Kern}(G_2 Z_1 N) = \mathrm{Kern}((G_2 G_1) N^2) = \mathrm{Kern}(N^2)$.

Zur Bestimmung des Kerns von N^3 bringen wir die Matrix $Z_2 N$ durch Zeilenumformungen auf Zeilenstufenform $G_3 Z_2 N = Z_3$, mit $G_3 \in \mathrm{GL}_n(K)$. Dann ist $\mathrm{Kern}\, Z_3 = \mathrm{Kern}(G_3 Z_2 N) = \mathrm{Kern}((G_3 G_2 G_1) N^3) = \mathrm{Kern}(N^3)$.

Und so fort. Solange $\mathrm{Kern}\, N^j < K^n$, ist übrigens auch $\mathrm{Kern}\, N^j < \mathrm{Kern}\, N^{j+1}$, oder äquivalent, $\mathrm{rk}\, Z_j > \mathrm{rk}\, Z_{j+1}$ — solange man noch nicht fertig ist, kommen in *jedem* Schritt Vektoren dazu. Das ist eine gute Probe für den jeweils gerade durchgeführten Schritt.

Schließlich können noch in jedem Schritt die Nullzeilen unterschlagen werden.

Die jeweilige Zeilenstufenform nur unvollständig zu berechnen, d.h. die Spalten nur teilweise zu säubern, ist hier keine gute Idee.

Folgerung. Sei

$$\mathrm{Kette}(x_{j;s}) := (N^{j-1}x_{j;s}, N^{j-2}x_{j;s}, \ldots, N^0 x_{j;s})$$

für $j \in [1,m]$ und $s \in [1,g_j]$. Bezüglich der im Nilpotenzlemma konstruierten und wie folgt sortierten *Kettenbasis*

$$\Big(\mathrm{Kette}(x_{m;1}),\ldots,\mathrm{Kette}(x_{m;g_m}),\mathrm{Kette}(x_{m-1;1}),\ldots,\mathrm{Kette}(x_{m-1;g_{m-1}}),\ldots,\mathrm{Kette}(x_{1;1}),\ldots,\mathrm{Kette}(x_{1;g_1})\Big)$$

von K^n hat die Abbildung $x \longmapsto Nx$ die beschreibende Matrix

$$\begin{pmatrix} N_{b_1} & & \\ & \ddots & \\ & & N_{b_t} \end{pmatrix}$$

mit Blöcken der Gestalt

$$N_b \;:=\; \begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & \ddots & \ddots & \\ & & & & 0 & 1 \\ & & & & & 0 \end{pmatrix} \;\in\; K^{b\times b}\,,$$

wobei die leergelassenen Einträge mit Nullen zu ergänzen sind. Hierbei ist das Tupel $(b_1,\ldots,b_t)$ absteigend geordnet, wobei der Eintrag $j \in [1,m]$ in diesem Tupel gerade g_j-fach auftritt. Insbesondere ist die Zahl der Nilpotenzblöcke gleich der Zahl der Ketten, d.h. $t = \sum_{j\in[1,m]} g_j$.

In anderen Worten, es gibt ein $S \in \mathrm{GL}_n(K)$ so, daß $S^{-1}NS$ von Hauptdiagonalblockgestalt ist, mit Blöcken der Form N_b. Die Basiswechselmatrix S hat als Spalteneinträge die Basisvektoren der eben angeführten Basis.

4.3.3 Beispiel und Erläuterung zum Nilpotenzlemma

Beispiel. Sei $K = \mathbf{C}$, sei $n = 5$ und sei

$$N \;=\; \begin{pmatrix} 1 & -1 & 1 & -1 & 1 \\ 0 & -1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & -1 \\ 1 & 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 & 1 \end{pmatrix}\;.$$

Berechnung der Kerne der Potenzen von N liefert

$$(y_{1;1}, y_{1;2}, y_{2;1}, y_{2;2}, y_{3;1}) \;=\; \left(\begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}\right)\;.$$

Sei also $x_{3;1} := y_{3;1} = \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}$. Wir können im zweiten Schritt $x_{2;1} := y_{2;1}$ verwenden, um eine Basis

$$(y_{1;1}, y_{1;2}, Nx_{3;1}, x_{2;1}) \;=\; \left(\begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}-1\\-1\\1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}\right)$$

von Kern N^2 zu erhalten. (Alternativ hätte man auch $y_{2;2}$ nehmen können). Im dritten und letzten Schritt sind keine Vektoren $x_{1;i}$ auszuwählen, d.h. es ist $g_1 = 0$, da

$$(N^2 x_{3;1}, N x_{2;1}) \;=\; \left(\begin{pmatrix} 0\\1\\0\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\1\\1 \end{pmatrix} \right)$$

bereits eine Basis von Kern N ist. Das Nilpotenzlemma gibt uns nun die Kettenbasis

$$(N^2 x_{3;1}, N x_{3;1}, x_{3;1}, N x_{2;1}, x_{2;1}) \;=\; \left(\begin{pmatrix} 0\\1\\0\\0\\1 \end{pmatrix}, \begin{pmatrix} -1\\-1\\1\\0\\-1 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\0\\0 \end{pmatrix} \right)$$

von $\mathbf{C}^5$. Bezüglich dieser erhalten wir die beschreibende Matrix

$$S^{-1} N S \;=\; \left(\begin{array}{ccc|cc} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

von $x \longmapsto Nx$, wobei

$$S \;=\; \begin{pmatrix} 0 & -1 & 0 & 1 & 0 \\ 1 & -1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 1 & 0 \end{pmatrix} .$$

Erläuterung. Aus der Konstruktion zum Nilpotenzlemma kann sich zum Beispiel eine Basis der folgenden Form ergeben.

$x_{4;1}$ $\quad x_{4;2}$				U_4
$N x_{4;1}$ $\quad N x_{4;2}$		$x_{3;1}$		U_3
$N^2 x_{4;1}$ $\quad N^2 x_{4;2}$		$N x_{3;1}$		U_2
$N^3 x_{4;1}$ $\quad N^3 x_{4;2}$		$N^2 x_{3;1}$	$x_{1;1}$	U_1

In Schritt 1 wurde mit $(x_{4;1}, x_{4;2}) = (y_{4;1}, y_{4;2})$ ergänzt. In Schritt 2 wurde aus $(y_{3;1}, y_{3;2}, y_{3;3})$ das Tupel $(x_{3;1})$ ausgewählt, um NU_4 zu U_3 zu ergänzen. In Schritt 3 gab es nichts zu ergänzen, aus $(y_{2;1}, y_{2;2}, y_{2;3})$ wurde also kein Vektor ausgewählt. In Schritt 4 wurde aus $(y_{1;1}, y_{1;2}, y_{1;3}, y_{1;4})$ das Tupel $(x_{1;1})$ ausgewählt, um NU_2 zu U_1 zu ergänzen. Somit ist $g_4 = 2$, $g_3 = 1$, $g_2 = 0$ und $g_1 = 1$.

Es ist Kern $N^1 = U_1$ das Erzeugnis der untersten Zeile obiger Tabelle, Kern $N^2 = U_1 \oplus U_2$ das Erzeugnis der unteren beiden Zeilen, Kern $N^3 = U_1 \oplus U_2 \oplus U_3$ das Erzeugnis der unteren drei Zeilen, und schließlich Kern $N^4 = K^{12}$ der gesamte Vektorraum.

Bezüglich der Kettenbasis

$$(\underbrace{N^3 x_{4;1}, N^2 x_{4;1}, N^1 x_{4;1}, N^0 x_{4;1},}_{\text{Kette}(x_{4;1})} \underbrace{N^3 x_{4;2}, N^2 x_{4;2}, N^1 x_{4;2}, N^0 x_{4;2},}_{\text{Kette}(x_{4;2})} \underbrace{N^2 x_{3;1}, N^1 x_{3;1}, N^0 x_{3;1},}_{\text{Kette}(x_{3;1})} \underbrace{N^0 x_{1;1}}_{\text{Kette}(x_{1;1})}) ,$$

für welche wir also die Spalten der Tabelle von unten nach oben durchlaufen, hat $x \longmapsto Nx$ die Blockgestalt

$$\begin{pmatrix} \boxed{\begin{matrix}0&1&&\\&0&1&\\&&0&1\\&&&0\end{matrix}} &&& \\ & \boxed{\begin{matrix}0&1&&\\&0&1&\\&&0&1\\&&&0\end{matrix}} && \\ && \boxed{\begin{matrix}0&1&\\&0&1\\&&0\end{matrix}} & \\ &&& \boxed{0} \end{pmatrix} .$$

In der obigen Bezeichnung ist also $t = 4$, und $(b_1, b_2, b_3, b_4) = (4, 4, 3, 1)$.

4.3.4 Jordanform allgemeiner quadratischer Matrizen

Mit dem Hauptzerlegungslemma blieb uns noch, die auf einem Hauptraum den Endomorphismus $x \longmapsto Ax$ beschreibende Matrix in Form zu bekommen. Dies können wir nun mit dem Nilpotenzlemma erledigen.

Satz 13 *Sei $A \in K^{n\times n}$.*

(i) *Es gibt (wenigstens) ein $S \in \mathrm{GL}_n(K)$ so, daß $S^{-1}AS$ eine Hauptdiagonalblockmatrix ist, mit* Jordanblöcken *von der Form $\lambda E_b + N_b \in K^{b\times b}$, wobei λ ein Eigenwert von A ist. Wir sagen, $S^{-1}AS$ ist in* Jordanscher Normalform, *oder kurz, in* Jordanform.

(ii) *Sei λ ein Eigenwert von A, und sei $(b_1, \ldots, b_t)$ das Tupel der in $S^{-1}AS$ auftretenden Kantenlängen b von Blöcken der Form $\lambda E_b + N_b$. Dann ist $\dim E_A(\lambda) = t$ und $\dim H_A(\lambda) = \sum_{i\in[1,t]} b_i$. Genauer, es ist*

$$\dim \mathrm{Kern}(\lambda E - A)^s - \dim \mathrm{Kern}(\lambda E - A)^{s-1} \;=\; \#\{i \mid b_i \geqslant s\}$$

für $s \geqslant 1$. Insbesondere legt A die Jordanform von $S^{-1}AS$ bis auf die Reihenfolge der Jordanblöcke fest, unabhängig von der zur Konjugation in Jordanform gewählten Matrix S.

Beweis. Zu (i). Sei $\chi_A(X) = \prod_{i\in[1,k]}(X - \lambda_i)^{m_i}$, mit $\lambda_i \neq \lambda_j$ für $i \neq j$ und $m_i \geqslant 1$ stets. Mit dem Hauptzerlegungslemma gibt es ein $S \in \mathrm{GL}_n(K)$ mit $S^{-1}AS = \mathrm{diag}(A_1, \ldots, A_k)$, wobei $A_j \in K^{m_j\times m_j}$ das charakteristische Polynom $\chi_{A_j}(X) = (X - \lambda_j)^{m_j}$ besitzt für $j \in [1, k]$. Diese Hauptdiagonalblockmatrix kann nun blockweise weiter konjugiert werden.

Wir dürfen also annehmen, daß A nur einen Eigenwert λ hat, daß mithin $K^n = H_A(\lambda)$. Speziell ist mit Cayley-Hamilton $(A - \lambda E_n)^n = 0$. Mit dem Nilpotenzlemma finden wir nun ein $S \in \mathrm{GL}_n(K)$ so, daß $S^{-1}(A - \lambda E_n)S$ eine Blockdiagonalmatrix mit Blöcken der Form N_b ist. Dann ist $S^{-1}AS$ eine Blockdiagonalmatrix mit Blöcken der Form $\lambda E_b + N_b$.

Zu (ii). Da $\dim \operatorname{Kern}(\lambda E - A)^s = \dim \operatorname{Kern} S^{-1}(\lambda E - A)^s S = \dim \operatorname{Kern}(\lambda E - S^{-1}AS)^s$, dürfen wir mit (i) die Matrix A als in Jordanform gegeben annehmen. Nun ist für $b \geqslant 1$

$$\dim \operatorname{Kern} N_b^s \;=\; \begin{cases} s & \text{für } s \leqslant b \\ b & \text{für } s \geqslant b\,, \end{cases}$$

und die behauptete Formel folgt, da ein Nilpotenzblock der Form N_b zur Dimensionsdifferenz der Kerne genau dann einen Beitrag 1 leistet, wenn $s \leqslant b$, und er sonst keinen Beitrag liefert.

Verfahren. Die Jordanform einer gegebenen Matrix $A \in K^{n\times n}$ kann in den folgenden Schritten berechnet werden.

(1) Berechne und zerlege das charakteristische Polynom $\chi_A(X) = \det(XE - A) = \prod_{i\in[1,k]}(X - \lambda_i)^{m_i}$, wobei $\lambda_i \neq \lambda_j$ für $i \neq j$.

$\forall\, i$ {

(2) Berechne eine Basis von $\operatorname{Kern}(A - \lambda_i E)$, ergänze diese zu einer Basis von $\operatorname{Kern}((A - \lambda_i E)^2)$, ergänze diese zu einer Basis von $\operatorname{Kern}((A - \lambda_i E)^3)$, und so fort, bis zu einer Basis von $\operatorname{Kern}((A - \lambda_i E)^{m_i}) = H_A(\lambda_i)$. Breche ab, sobald $\dim \operatorname{Kern}((A - \lambda_i E)^m) = m_i$, spätestens also bei $m = m_i$.

(3) Berechne die im Nilpotenzlemma bezüglich des nilpotenten Endomorphismus $x \longmapsto (A - \lambda_i E)x$ von $H_A(\lambda_i)$ konstruierte Kettenbasis dieses Hauptraumes. Der dort zu verwendende Exponent m ist gerade der Abbruchwert aus (2).

(4) Setze die in (3) gefundenen Basistupel für $i \in [1, k]$ nebeneinander zu einer Basis von K^n und beschreibe $x \longmapsto Ax$ in dieser Basis.

4.3.5 Beispiel und Erläuterung zur Jordanform

Beispiel. Sei $K = \mathbf{C}$, sei

$$A \;=\; \begin{pmatrix} 0 & 2 & 1 & 1 & -1 & -2 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 1 \end{pmatrix}\;.$$

Zu (1). Wir berechnen zunächst $\chi_A(X) = \det(XE - A) = X^2(X-1)^4$, und erhalten so die Eigenwerte $\lambda_1 = 0$ (mit algebraischer Vielfachheit $m_1 = 2$) und $\lambda_2 = 1$ (mit algebraischer Vielfachheit $m_2 = 4$).

Die Vektoren $y_{j;k}$ sind nur 'lokal bezeichnet', d.h. ist der jeweilige Eigenwert abgearbeitet, vergessen wir diese Bezeichnung wieder.

Zu (2, λ_1). Wir berechnen (in den Bezeichnungen des Nilpotenzlemmas, angewandt auf den Endomorphismus $H_A(0) \longrightarrow H_A(0) : x \longmapsto (A - 0 \cdot E)x)$

$$\mathrm{Kern}(A - 0E) \;=\; \langle \underbrace{\begin{pmatrix} 0\\1\\0\\0\\0\\1 \end{pmatrix}}_{=:\, y_{1;1}} \rangle \quad (\, = E_A(0)\,)$$

und

$$\mathrm{Kern}(A - 0E)^2 \;=\; \langle \begin{pmatrix} 0\\1\\0\\0\\0\\1 \end{pmatrix}, \underbrace{\begin{pmatrix} 1\\0\\1\\0\\1\\0 \end{pmatrix}}_{=:\, y_{2;1}} \rangle \quad (\, = H_A(0)\,)\ .$$

Zu (3, λ_1). Wir nehmen nun $x_{1;2;1} := y_{2;1}$, der erste Index (= 1) stehe hierbei für die Nummer des Eigenwerts, die weiteren beiden (= 2; 1) entstammen dem Nilpotenzlemma. Da bereits $\langle (A - 0 \cdot E)x_{1;2;1} \rangle = \mathrm{Kern}(A - 0 \cdot E)$ ist, sind keine weiteren Elemente zu wählen. Wir haben so die Basis

$$(\underbrace{Ax_{1;2;1}, x_{1;2;1}}_{\mathrm{Kette}(x_{1;2;1})})$$

von $H_A(0)$ konstruiert.

Zu (2, λ_2). Wir berechnen (in den Bezeichnungen des Nilpotenzlemmas, angewandt auf den Endomorphismus $H_A(1) \longrightarrow H_A(1) : x \longmapsto (A - 1 \cdot E)x)$

$$\mathrm{Kern}(A - 1 \cdot E) \;=\; \langle \underbrace{\begin{pmatrix} 1\\1\\0\\0\\1\\0 \end{pmatrix}}_{=:\, y_{1;1}}, \underbrace{\begin{pmatrix} 1\\0\\0\\1\\0\\0 \end{pmatrix}}_{=:\, y_{1;2}} \rangle \quad (\, = E_A(1)\,)\ ,$$

$$\mathrm{Kern}(A - 1 \cdot E)^2 \;=\; \langle \begin{pmatrix} 1\\1\\0\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\0\\1\\0\\0 \end{pmatrix}, \underbrace{\begin{pmatrix} 0\\0\\0\\0\\1\\0 \end{pmatrix}}_{=:\, y_{2;1}} \rangle$$

und

$$\mathrm{Kern}(A - 1 \cdot E)^3 \;=\; \langle \begin{pmatrix} 1\\1\\0\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\0\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\0\\1\\0 \end{pmatrix}, \underbrace{\begin{pmatrix} 0\\0\\1\\0\\0\\0 \end{pmatrix}}_{=:\, y_{3;1}} \rangle \quad (\, = H_A(1)\,)\ .$$

Zu (3, λ_2). Wir nehmen nun $x_{2;3;1} = y_{3;1}$. Da bereits $(y_{1;1}, y_{1;2}, (A - 1 \cdot E)x_{2;3;1})$ eine Basis von $\mathrm{Kern}(A - 1 \cdot E)^2$ darstellt, ist an dieser Stelle kein Vektor aus $(y_{2;1})$ auszuwählen, und das Tupel $\underline{x}_2$ bleibt leer. Im nächsten Schritt ist dann mit $x_{2;1;1} := y_{1;2}$ die Ergänzung zu einer Basis

$$((A - 1 \cdot E)^2 x_{2;3;1}, x_{2;1;1})$$

von Kern$(A - 1 \cdot E)$ erreicht. Wir haben so insgesamt die Kettenbasis

$$(\underbrace{(A-E)^2 x_{2;3;1}, (A-E)x_{2;3;1}, x_{2;3;1}}_{\text{Kette}(x_{2;3;1})}, \underbrace{x_{2;1;1}}_{\text{Kette}(x_{2;1;1})})$$

von $H_A(1)$ konstruiert.

Zu (4). Insgesamt hat der Endomorphismus $x \longmapsto Ax$ von K^n bezüglich der Basis

$$\begin{array}{rcc|cccc|c}
 & (Ax_{1;2;1}, & x_{1;2;1}, & (A-E)^2 x_{2;3;1}, & (A-E)x_{2;3;1}, & x_{2;3;1}, & & x_{2;1;1}) \\
= & (\begin{pmatrix}0\\1\\0\\0\\0\\1\end{pmatrix}, & \begin{pmatrix}1\\0\\1\\0\\1\\0\end{pmatrix}, & \begin{pmatrix}1\\1\\0\\0\\1\\0\end{pmatrix}, & \begin{pmatrix}1\\1\\0\\0\\0\\0\end{pmatrix}, & \begin{pmatrix}0\\0\\1\\0\\0\\0\end{pmatrix}, & & \begin{pmatrix}1\\0\\0\\1\\0\\0\end{pmatrix})
\end{array}$$

die Blockdiagonalform

$$B := \begin{pmatrix} \boxed{\begin{matrix}0 & 1\\ & 0\end{matrix}} & & \\ & \boxed{\begin{matrix}1 & 1 & \\ & 1 & 1\\ & & 1\end{matrix}} & \\ & & \boxed{1} \end{pmatrix} .$$

In anderen Worten, mit

$$S := \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

wird $S^{-1}AS = B$, oder auch, was einfacher zu verifizieren ist, $AS = SB$. Wobei bei letzterer Gleichung auch noch auf die Invertierbarkeit von S zu achten ist, um eine vollkommen sichere Probe zu haben.

Erläuterung. Wir gehen noch einmal auf den dritten Schritt des Jordanverfahrens ein. Sei $A \in \mathbf{C}^{n \times n}$ gegeben, und sei λ ein Eigenwert von A. Wir schreiben $C = A - \lambda E$.

Angenommen (was in der Praxis natürlich etwas groß wäre), wir hätten einen zehndimensionalen Hauptraum $H_A(\lambda)$, der sich wie folgt zusammensetzt.

$$\begin{array}{r|lllll}
\text{Kern}\, C & y_{1;1} & y_{1;2} & y_{1;3} & y_{1;4} & y_{1;5} \\
\text{Kern}\, C^2 & y_{2;1} & y_{2;2} & y_{2;3} & & \\
H_A(\lambda) = \text{Kern}\, C^3 & y_{3;1} & y_{3;2} & & &
\end{array}$$

Dies ist zu lesen als

$$\begin{array}{lcl}
\text{Kern}\, C & = & \langle y_{1;1}, y_{1;2}, y_{1;3}, y_{1;4}, y_{1;5} \rangle \\
\text{Kern}\, C^2 & = & \langle y_{1;1}, y_{1;2}, y_{1;3}, y_{1;4}, y_{1;5}, y_{2;1}, y_{2;2}, y_{2;3} \rangle \\
\text{Kern}\, C^3 & = & \langle y_{1;1}, y_{1;2}, y_{1;3}, y_{1;4}, y_{1;5}, y_{2;1}, y_{2;2}, y_{2;3}, y_{3;1}, y_{3;2} \rangle \, .
\end{array}$$

Wir setzen nun $x_{3;1} := y_{3;1}$ und $x_{3;2} := y_{3;2}$. Nach Anwendung von C auf die Vektoren im dritten Level landen wir im nächstunteren Level:

$$\begin{array}{r|ccccc}
\text{Kern}\, C & y_{1;1} & y_{1;2} & y_{1;3} & y_{1;4} & y_{1;5} \\
\text{Kern}\, C^2 & Cx_{3;1} & Cx_{3;2} & y_{2;1} & y_{2;2} & y_{2;3} \\
H_A(\lambda) = \text{Kern}\, C^3 & x_{3;1} & x_{3;2} & & &
\end{array}$$

Für eine Basis des achtdimensionalen Unterraums $\operatorname{Kern} C^2$ sind die in den ersten beiden Zeilen verzeichneten Vektoren nun zwei zuviel. Man wähle nun aus $(y_{2;1}, y_{2;2}, y_{2;3})$ einen Vektor so aus, daß sich nach Streichung der beiden anderen in den ersten beiden Zeilen eine Basis von $\operatorname{Kern} C^2$ ergibt. Sei dies etwa für $x_{2;1} := y_{2,2}$ der Fall, d.h. seien damit in den ersten beiden Zeilen von

$$\begin{array}{r|ccccc} \operatorname{Kern} C & y_{1;1} & y_{1;2} & y_{1;3} & y_{1;4} & y_{1;5} \\ \operatorname{Kern} C^2 & Cx_{3;1} & Cx_{3;2} & x_{2;1} & & \\ H_A(\lambda) = \operatorname{Kern} C^3 & x_{3;1} & x_{3;2} & & & \end{array}$$

acht Vektoren eingetragen, die ein linear unabhängiges Tupel bilden. (Der dafür aus $(y_{2;1}, y_{2;2}, y_{2;3})$ auszuwählende Vektor $x_{2;1}$ ist i.a. nicht eindeutig festgelegt.) Nach Anwendung von C auf die jetzigen Vektoren des zweiten Levels landen wir im nächstunteren Level:

$$\begin{array}{r|cccccccc} \operatorname{Kern} C & C^2x_{3;1} & C^2x_{3;2} & Cx_{2;1} & y_{1;1} & y_{1;2} & y_{1;3} & y_{1;4} & y_{1;5} \\ \operatorname{Kern} C^2 & Cx_{3;1} & Cx_{3;2} & x_{2;1} & & & & & \\ H_A(\lambda) = \operatorname{Kern} C^3 & x_{3;1} & x_{3;2} & & & & & & \end{array}$$

Für eine Basis des fünfdimensionalen Unterraums $\operatorname{Kern} C$ sind die in der ersten Zeile verzeichneten Vektoren nun drei zuviel. Man wähle nun aus $(y_{1;1}, y_{1;2}, y_{1;3}, y_{1;4}, y_{1;5})$ zwei Vektoren so aus, daß sich nach Streichung der drei anderen in der ersten Zeile eine Basis von $\operatorname{Kern} C$ ergibt. Sei dies etwa für $x_{1;1} := y_{1,2}$ und $x_{1;2} := y_{1;4}$ der Fall, d.h. seien damit in der ersten Zeile von

$$\begin{array}{r|ccccc} \operatorname{Kern} C & C^2x_{3;1} & C^2x_{3;2} & Cx_{2;1} & x_{1;1} & x_{1;2} \\ \operatorname{Kern} C^2 & Cx_{3;1} & Cx_{3;2} & x_{2;1} & & \\ H_A(\lambda) = \operatorname{Kern} C^3 & x_{3;1} & x_{3;2} & & & \end{array}$$

fünf Vektoren eingetragen, die ein linear unabhängiges Tupel bilden. (Die dafür aus $(y_{1;1}, y_{1;2}, y_{1;3}, y_{1;4}, y_{1;5})$ auszuwählenden Vektoren $x_{1;1}$ und $x_{1;2}$ sind i.a. nicht eindeutig festgelegt.)

Fertig. Die in die Matrix S für den Hauptraum $H_A(\lambda)$ einzutragenden Ketten finden sich in den Spalten der Tabelle.

4.3.6 Minimalpolynom

Sei $A \in K^{n\times n}$. Wir betrachten das Ideal

$$I \;:=\; \{f(X) \in K[X] \mid f(A) = 0\} \;\subseteq\; K[X]\,.$$

Mit Cayley-Hamilton ist $\chi_A(X) \in I$, und somit $I \neq \{0\}$. Damit gibt es ein eindeutiges normiertes Polynom $\mu_A(X)$, für welches $I = \mu_A(X)K[X]$ ist, genannt das *Minimalpolynom* von A. In anderen Worten, $\mu_A(X) \in K[X]$ ist normiert, erfüllt selbst $\mu_A(A) = 0$ und teilt dazuhin jedes Polynom, das ebenfalls A annulliert. Zum Beispiel teilt das Minimalpolynom $\mu_A(X)$ das charakteristische Polynom $\chi_A(X)$, d.h. es gibt ein $g(X) \in K[X]$ mit $\mu_A(X)g(X) = \chi_A(X)$.

Aus dieser Teilbarkeitseigenschaft folgt, daß das Minimalpolynom auch das eindeutig bestimmte normierte Polynom minimalen Grades ist, welches A annulliert. Man könnte also durch Testen aller Teiler von $\chi_A(X)$ das Minimalpolynom ermitteln.

Eine bessere Möglichkeit ist die folgende. Sei $S \in \mathrm{GL}_n(K)$ eine invertierbare Matrix. Aus $\mu_A(S^{-1}AS) = S^{-1}\mu_A(A)S = 0$ folgt, daß $\mu_{S^{-1}AS}(X)$ ein Teiler von $\mu_A(X)$ ist. Aus $\mu_{S^{-1}AS}(A) = SS^{-1}\mu_{S^{-1}AS}(A)SS^{-1} = S\mu_{S^{-1}AS}(S^{-1}AS)S^{-1} = 0$ folgt, daß $\mu_A(X)$ ein Teiler von $\mu_{S^{-1}AS}(X)$ ist. Insgesamt ist also $\mu_{S^{-1}AS}(X) = \mu_A(X)$, und wir können zur Bestimmung des Minimalpolynoms die Jordanform von A heranziehen.

Für $b \geqslant 1$ hat nun ein Jordanblock $\lambda E_b + N_b$ das Minimalpolynom $(X-\lambda)^b$. Wenn also $\chi_A(X) = \prod_{i\in[1,k]}(X-\lambda_i)^{m_i}$ das charakteristische Polynom von A ist, $\lambda_i \neq \lambda_j$ für $i \neq j$ und $m_i \geqslant 1$ stets, so ist das Minimalpolynom von A gegeben durch

$$\mu_A(X) \;=\; \prod_{i\in[1,k]} (X-\lambda_i)^{c_i}\;,$$

wobei c_i die maximale Kantenlänge eines Jordanblocks zum Eigenwert λ_i in der Jordanform von A ist.

So hat etwa die Matrix A im Beispiel nach Satz 13 das Minimalpolynom $\mu_A(X) = X^2(X-1)^3$.

4.3.7 Diagonalisierbarkeit

Sei $A \in K^{n\times n}$. Gibt es ein $S \in \mathrm{GL}_n(K)$ so, daß $S^{-1}AS$ eine Diagonalmatrix ist, so heißt *A diagonalisierbar.*

Satz 14 *Eine Matrix $A \in K^{n\times n}$ ist diagonalisierbar genau dann, wenn für jeden Eigenwert λ von A die geometrische mit der algebraischen Vielfachheit übereinstimmt, d.h. wenn stets $E_A(\lambda) = H_A(\lambda)$ ist.*

Beweis. Ist A diagonalisierbar, so dürfen wir mit der Invarianz der geometrischen und algebraischen Vielfachheit unter Konjugation annehmen, daß A eine Diagonalmatrix ist. Für eine Diagonalmatrix stimmen aber geometrische und algebraische Vielfachheit eines jeden Eigenwertes überein.

Ist umgekehrt $E_A(\lambda) = H_A(\lambda)$ für alle Eigenwerte λ von A, so ist nach Satz 13.(ii) in dortiger Notation

$$t \;=\; \dim E_A(\lambda) \;=\; \dim H_A(\lambda) \;=\; \sum_{i\in[1,t]} b_i\;,$$

woraus $(b_1,\ldots,b_t) = (1,\ldots,1)$ folgt. Also haben alle Jordanblöcke Kantenlänge 1, d.h. A ist diagonalisierbar. $\square$

Bemerkung. Ist $A \in K^{n\times n}$ diagonalisierbar, so bricht das im Nilpotenzlemma geschilderte Verfahren bereits nach dem ersten Schritt ab. Die Punkte (2) und (3) im oben angegebenen Verfahren zur Berechnung der Jordanform reduzieren sich also auf die Erstellung einer Basis von $E_A(\lambda_i)$ für $i \in [1, k]$.

Bemerkung. Hat $A \in K^{n\times n}$ nun n verschiedene Eigenwerte, so ist A diagonalisierbar. In der Tat, für jeden dieser Eigenwerte λ_i folgt aus $1 \leqslant \dim E_A(\lambda_i) \leqslant \dim H_A(\lambda_i) = m_i$ und aus $\sum_{i\in[1,n]} m_i = n$, daß $1 = \dim E_A(\lambda_i) = \dim H_A(\lambda_i)$.

4.4 $*$ Jordanformen nach Frobenius und Böge

Wir stellen alternativ zum oben gezeigten Verfahren die Frobenius-Böge-Methode vor [**10,** IX, §2]. Diese ist geeignet zur Berechnung von Jordanformen über beliebigen Körpern. Dieser Abschnitt ist nicht prüfungs- oder klausurrelevant.

4.4.1 $*$ Euklidsche Ringe

Wir werden nun etwas ausholen, und die Theorie der euklidschen Ringe nachholen, die wir in den Kapiteln über $\mathbf{Z}$ und $K[X]$ umgangen hatten.

Sei R ein kommutativer Ring. Sei R *nullteilerfrei,* d.h. sei $ab \neq 0$ für alle $a,\, b \in R \smallsetminus \{0\}$.

Sei ferner eine Abbildung $d : R \smallsetminus \{0\} \longrightarrow \mathbf{N}$ mit folgender Eigenschaft gegeben ([3]).

Für alle $x \in R$ und alle $y \in R \smallsetminus \{0\}$ gibt es ein $t \in R$ und ein $r \in R$ mit

$$x \;=\; yt + r \tag{$*$}$$

und mit entweder $r = 0$ oder $d(r) < d(y)$.

Der Ring R zusammen mit der Funktion d heißt auch *euklidscher Ring.* Für $x \in R$ heiße $d(x)$ der *Grad* von x. Ein Element $y \in R$ heißt *Teiler* eines Elementes $x \in R$, falls es ein $t \in R$ gibt mit $x = yt$. Wir erinnern an die Definition des Ideals $xR := \{xt \;:\; t \in R\} \subseteq R$ für ein gegebenes $x \in R$. Zwei Elemente x und y in R heißen *assoziiert,* falls $xR = yR$. Äquivalent, x und y sind assoziiert, falls ein $u \in \mathrm{Inv}(R)$ existiert mit $x = yu$. Die Assoziiertheit ist eine Äquivalenzrelation.

Ein Element x in R heißt *irreduzibel,* wenn jeder Teiler von x entweder zu x oder zu 1 assoziiert ist. In jeder Assoziiertenklasse eines irreduziblen Elements wählen wir einen Repräsentanten. Die Menge dieser Repräsentanten werde mit $\mathrm{Irr}(R)$ bezeichnet.

Beispiel. Der Ring $R = \mathbf{Z}$ der ganzen Zahlen bildet zusammen mit der Funktion $d(z) = |z|$ für $z \in \mathbf{Z}\smallsetminus\{0\}$ einen euklidschen Ring, wie Division mit Rest zeigt. Hier ist der Grad eines Elementes also durch den Betrag gegeben. Zwei Elemente sind assoziiert, falls sie bis auf Vorzeichen übereinstimmen. Ein Element ist irreduzibel genau dann, wenn es prim ist. Wir wählen jeweils eine positive Primzahl als Repräsentanten.

Beispiel. Sei K ein Körper. Der Ring $R = K[X]$ der Polynome mit Koeffizienten in K bildet zusammen mit der Funktion $d(f) = \deg(f)$ für $f(X) \in K[X] \smallsetminus \{0\}$ einen euklidschen Ring, wie Polynomdivision mit Rest zeigt. Hier ist der Grad eines Elementes im Sinne der eben getroffenen Sprachregelung also der Grad eines Polynoms im bisherigen Sinne. Zwei Elemente sind assoziiert, falls sie bis auf nichtverschwindenden skalaren Faktor übereinstimmen. Ein Element ist irreduzibel genau dann, wenn es bis auf Multiplikation mit einem nichtverschwindenden Skalar im bisherigen Sinne ein irreduzibles Polynom ist. Als Repräsentanten wählten wir die irreduziblen Polynome im bisherigen Sinne, welche qua Definition normiert sind.

[3]Nicht mit der gleichnamigen Abbildung aus §3.4.2 zu verwechseln.

Beispiel. Der Ring $R = \mathbf{Z}[i] := \{a + bi \in \mathbf{C} \mid a,\, b \in \mathbf{Z}\}$ der Gaußschen Zahlen bildet zusammen mit der Funktion $d(a + bi) = a^2 + b^2$ für $a + bi \in \mathbf{Z}[i] \smallsetminus \{0\}$ einen euklidschen Ring. In der Tat findet sich in einem Kreis mit Radius 1 um jeden Punkt der Gaußschen Zahlenebene, die $\mathbf{C}$ repräsentiert, wenigstens eine Zahl mit ganzem Real- und Imaginärteil. Gegeben x und y wie in $(*)$, findet sich eine solche Zahl q im Abstand kleiner als 1 von x/y. Somit ist $d(r) = d(x - yq) < d(y)$.

Der Begriff des euklidschen Ringes hätte es erlaubt, §1.4.3 und §1.4.5 zu einem einzigen Abschnitt zusammenzufassen. Wir holen dies nach.

Lemma. *Jedes Ideal in R ist von der Form xR für ein $x \in R$. Wir sagen auch, R ist ein* Hauptidealbereich.

Beweis. Sei $I \neq 0R$ ein Ideal in R. Sei x ein Element kleinsten Grades in $I \smallsetminus \{0\}$. Es ist $xR \subseteq I$, und wir wollen die Gleichheit zeigen. Sei uns ein $y \in I$ vorgegeben. Da R euklidsch ist, erhalten wir $y = xt + r$, mit $t,\, r \in R$ und mit entweder $d(r) \in [0, d(x) - 1]$ oder aber $r = 0$. Es ist $r = y - xt \in I$. Wegen der Minimalität von $d(x)$ kann r nicht ungleich Null sein. Also ist $r = 0$ und $y = xt \in xR$. ▫

Ist $T \subseteq R$ eine Teilmenge, so können wir das von ihr *erzeugte* Ideal

$$I \;:=\; \left\{ \sum_{t \in T} r_t t \;\middle|\; r_t \in R, \text{ nur endlich viele } r_t \text{ ungleich } 0 \right\}$$

bilden. Es ist $T = gR$ für ein $g \in R$, und das Element g liegt bis auf Assoziation fest. Es heißt g der *größte gemeinsame Teiler* von T.

Lemma. *Sei $x \in R \smallsetminus \{0\}$. Genau dann ist R/xR ein Körper, wenn x irreduzibel ist.*

Beweis. Ist x nicht irreduzibel, so gibt es eine Zerlegung $x = yz$ derart, daß x weder y noch z teilt. Also ist $yz \equiv_{xR} 0$, wohingegen $y \not\equiv_{xR} 0$ und $z \not\equiv_{xR} 0$. Damit ist R/xR kein Körper.

Ist $x =: q$ irreduzibel, so haben wir zu zeigen, daß R/qR ein Körper ist. Zu jedem $y \not\equiv_{qR} 0$ haben wir ein $s \in R$ mit $ys \equiv_{qR} 1$ zu finden. Sei u der größte gemeinsame Teiler von $\{q, y\}$. Nun teilt u insbesondere das irreduzible Element q. Wäre u assoziiert zu q, so wäre $y \in uR = qR$, was nicht der Fall ist. Also ist u assoziiert zu 1, und somit $1 \in 1R = uR = \{qs + yt \mid s,\, t \in R\}$. Somit gibt es s und t in R mit $qs + yt = 1$. Dann ist $yt \equiv_{qR} 1$. ▫

Lemma. *Ist $q \in R$ irreduzibel, und teilt q das Produkt ab der Elemente $a,\, b \in \mathbf{R}$, so teilt q das Element a oder das Element b.*

Beweis. Es ist R/qR ein Körper. Nach Voraussetzung ist darin $ab \equiv_{qR} 0$, und folglich entweder $a \equiv_{qR} 0$ oder $b \equiv_{qR} 0$. ▫

Lemma. *Jedes Element $x \in R$ läßt sich schreiben als*

$$(**) \qquad x \;=\; a \cdot \prod_{q \in \mathrm{Irr}(R)} q^{\mathrm{v}_q(x)}\,,$$

wobei $a \in \mathrm{Inv}(R)$. Die Zahlen $\mathrm{v}_q(x)$ sind nur für endlich viele $q \in \mathrm{Irr}(R)$ ungleich Null, so daß ein endliches Produkt entsteht (engl. v*aluation, dt. Bewertung). Sie sind durch die Gleichung $(**)$ eindeutig festgelegt. Es heißt $(**)$ die* Primfaktorzerlegung *von x.*

Beweis. Wir wollen zeigen, daß jede nichtleere Teilmenge der Menge der Ideale von R ein bezüglich der Inklusion maximales Element besitzt, d.h. ein Ideal, welches in keinem anderen Ideal dieser gegebenen Teilmenge echt enthalten ist. Ein solcher Ring heißt auch *noethersch.*

Wäre dem nicht so, so könnten wir darin eine unendliche Folge von Idealen I_j von R bilden, $j \geqslant 1$, in welcher $I_j \subsetneq I_{j+1}$ für $j \geqslant 1$ ist. Es ist nun $\bigcup_{j \geqslant 1} I_j$ ebenfalls ein Ideal von R, und somit gibt es mit vorigem Lemma ein $z \in R$ so, daß $\bigcup_{j \geqslant 1} I_j = zR$. Insbesondere ist $z \in \bigcup_{j \geqslant 1} I_j$, es gibt also ein $j_0 \geqslant 1$

mit $z \in I_{j_0}$. Dann ist

$$zR \subseteq I_{j_0} \subsetneq I_{j_0+1} \subseteq \bigcup_{j \geqslant 1} I_j = zR\,,$$

Widerspruch.

Betrachte nun die Menge der Ideale yR, für die y keine Primfaktorzerlegung hat. Diese Aussage ist vom gewählten Erzeuger y unabhängig. Sei angenommen, diese Menge sei nicht leer. Sei y_0R darin maximal. Dann ist y_0 nicht invertierbar und auch nicht irreduzibel. Folglich gibt es eine Zerlegung $y_0 = y_1y_2$ mit $y_0R \subsetneq y_1R$ und $y_0R \subsetneq y_2R$. Also haben y_1 und y_2 je eine Primfaktorzerlegung, und somit auch deren Produkt $y = y_1y_2$. Widerspruch.

Die Eindeutigkeit der Darstellung (∗∗) folgt durch Vergleich zweier solcher Darstellungen wie folgt. Sei

$$x \;=\; a \cdot \prod_{q \in \mathrm{Irr}(R)} q^{\mathrm{v}_q(x)} \;=\; a' \cdot \prod_{q \in \mathrm{Irr}(R)} q^{\mathrm{v}'_q(x)}\,.$$

Sei $\mathrm{v}_{q_0}(x) < \mathrm{v}'_{q_0}(x)$ angenommen. Nach Division durch $q^{\mathrm{v}_{q_0}(x)}$ ersehen wir, daß q_0 das Produkt $\prod_{q \in \mathrm{Irr}(R) \smallsetminus \{q_0\}} q^{\mathrm{v}_q(x)}$ teilt. Mit obigem Lemma teilt q_0 also einen der Faktoren, sagen wir q_1, mit q_1 nicht assoziiert zu q_0. Wegen q_1 irreduzibel muß q_0 assoziiert zu 1, also invertierbar sein, Widerspruch. ▫

4.4.2 ∗ Die Smithsche Normalform

Seien $m, n \geqslant 1$. Ist $l \leqslant \min(m,n)$, und sind $r_1, \ldots, r_l \in R$, so schreiben wir

$$\mathrm{diag}_{m,n}(r_1,\ldots,r_l) \;:=\; \begin{pmatrix} r_1 & 0 & \cdots & & & \cdots & 0 \\ 0 & r_2 & 0 & \cdots & & \cdots & 0 \\ & & \ddots & & & & \\ 0 & \cdots & 0 & r_l & 0 & \cdots & 0 \\ 0 & \cdots & & \cdots & & \cdots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & & \cdots & & \cdots & 0 \end{pmatrix} \;\in\; R^{m\times n}\,.$$

Wir schreiben $\mathrm{GL}_m(R) = \mathrm{Inv}(R^{m\times m}) = \{S \in R^{m\times m} \mid \text{es gibt ein } T \in R^{m\times m} \text{ mit } ST = E \text{ und } TS = E\}$.

Lemma. *Seien m, $n \geqslant 1$. Sei $C \in R^{m\times n}$ gegeben. Es gibt Matrizen $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ und Elemente $d_1, d_2, \ldots, d_l \in R$ derart, daß d_i ein Teiler von d_{i+1} ist für $i \in [1, l-1]$ und daß*

$$PCQ \;=\; \mathrm{diag}_{m,n}(d_1,\ldots,d_l)\,.$$

Die Matrix $\mathrm{diag}_{m,n}(d_1,\ldots,d_l)$ *heißt* Smithsche Normalform *oder kurz* Smithform *von C.*

Beweis. Mit Induktion genügt es zu zeigen, daß Matrizen $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ so existieren, daß

$$PCQ \;=\; \begin{pmatrix} d_1 & 0 \\ 0 & C' \end{pmatrix}$$

mit $C' \in R^{(m-1)\times(n-1)}$ und mit $d_1 \in R$ einem Teiler jedes Elementes von C'. Denn diese Eigenschaft geht bei nachfolgender Multiplikation von C' von links oder von rechts mit invertierbaren Matrizen mit Einträgen in R nicht verloren.

Wir werden im folgenden mit Zeilen- und Spaltenoperationen argumentieren. Eine Zeilenoperation entspricht hierbei der Multiplikation mit einer invertierbaren Matrix von links, eine Spaltenoperation der Multiplikation mit einer invertierbaren Matrix von rechts.

Wir geben einen Algorithmus an. Unter dem *Eck* der Matrix verstehen wir die Position $(1,1)$. Unter dem *Rand* verstehen wir die Menge der Matrixpositionen $(\{1\}\times[2,n]) \cup ([2,m]\times\{1\})$, d.h. die erste Zeile und die erste Spalte, ausgenommen das Eck.

(1) Sind alle Einträge des Randes gleich null, so gehe zu (4).

(2) Bringe, falls erforderlich, ein Element ungleich null kleinsten Grades der Matrix durch eine Zeilen- und eine Spaltenvertauschung in das Eck.

(3) Addiere unter Zuhilfenahme von $(*)$ ein geeignetes Vielfaches der ersten Spalte auf jede weitere Spalte so, daß an oberster Stelle dieser weiteren Spalte entweder eine Null oder aber ein Element kleineren Grades als im Eck resultiert. Addiere unter Zuhilfenahme von $(*)$ ein geeignetes Vielfaches der ersten Zeile auf jede weitere Zeile so, daß an vorderster Stelle dieser weiteren Zeile entweder eine Null oder aber ein Element kleineren Grades als im Eck resultiert. Gehe zu (1).

(4) Teilt der Eintrag im Eck jedes Element der Matrix, so ist der Algorithmus beendet.

(5) Addiere eine Zeile mit einem vom Eintrag im Eck nicht geteilten Eintrag zur ersten Zeile. Gehe zu (1).

Die Schleife (1-3) bricht ab, da bei jedem Durchlauf der Grad des Eintrags im Eck echt kleiner wird.

Die Schleife (1-5) bricht ab, da bei jedem Durchlauf der Grad des Eintrags im Eck echt kleiner wird.

Befindet sich der Algorithmus bei (4), so sind alle Einträge des Randes gleich Null. Wird er in (4) dann auch beendet, so ist die Matrix in der verlangten Form. □

Seien $m, n \geqslant 1$, und sei $C = (c_{i,j}) \in R^{m\times n}$. Sei $k \in [1, \min\{m,n\}]$. Ein *$k \times k$-Minor* von C ist die Determinante einer $k\times k$-Untermatrix $(c_{i_s,j_t})_{s,t} \in R^{k\times k}$ von C, wobei $i_s < i_{s+1}$ und $j_t < j_{t+1}$ stets. Sei $D_k(C)$ der größte gemeinsame Teiler aller $k \times k$-Minoren von C.

Lemma. *Seien $d_1, \ldots, d_l$ Elementarteiler von C. Es ist*

$$D_k(C) \;=\; \begin{cases} a_k \prod_{j\in[1,k]} d_j \text{ mit einem } a_k \in \mathrm{Inv}(R) & \text{falls } k \in [1,l] \\ 0 & \text{sonst .} \end{cases}$$

Insbesondere bestimmt die Matrix C ihre Elementarteiler bis auf Assoziation.

Beweis. Sei $k \in [1,n]$. Da die Formel für $D_k(C)$ für eine Smithform von C zutrifft, genügt es zu zeigen, daß für $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ gilt, daß $D_k(C)$ und $D_k(PCQ)$ assoziiert sind. Mit Transposition genügt es zu zeigen, daß $D_k(C)$ und $D_k(CQ)$ assoziiert sind. Da ferner Q invertierbar ist, genügt es zu zeigen, daß $D_k(C)$ ein Teiler von $D_k(CQ)$ ist.

Zeigen wir dies für eine beliebige Matrix $Q \in R^{n\times n}$. Wegen der Multilinearität der Minoren in den Spalten von CQ dürfen wir hierzu annehmen, es sei jede Spalte von Q ein Standardbasisvektor. Denn die Minoren im allgemeinen Fall sind R-Linearkombinationen dieses Spezialfalls.

Diesenfalls ist ein $k \times k$-Minor von CQ aber entweder gleich Null, oder aber bis auf Vorzeichen bereits als $k \times k$-Minor von C aufgetreten. □

4.4.3 $*$ Jordanformen über beliebigen Körpern

Sei K ein beliebiger Körper, nicht notwendig algebraisch abgeschlossen. Wir spezialisieren die Situation des vorigen Abschnitts nun zum Polynomring $(R =)\ K[X]$.

Für ein Polynom $f(X) \in K[X] \smallsetminus \{0\}$ und ein $m \geqslant 1$ schreiben wir

$$\Delta_m(f) \;:=\; \mathrm{diag}(1,\ldots,1,f(X)) \;\in\; K[X]^{m\times m}\,.$$

Lemma A. *Seien $n \geqslant 1$. Sei $C \in K[X]^{n\times n}$ mit $\deg(\det C) = n$ gegeben. Es gibt Matrizen $P \in \mathrm{GL}_m(K[X])$ und $Q \in \mathrm{GL}_n(K[X])$, irreduzible Polynome $q_1(X), \ldots, q_k(X)$ in $\mathrm{Irr}(K[X])$ und Exponenten $b_1, \ldots, b_k \geqslant 1$ derart, daß*

$$PCQ \;=\; \mathrm{diag}\Big(\Delta_{b_1\cdot\deg(q_1)}(q_1^{b_1}), \Delta_{b_2\cdot\deg(q_2)}(q_2^{b_2}), \ldots, \Delta_{b_k\cdot\deg(q_k)}(q_k^{b_k})\Big)\;,$$

wobei hier diag *das Bilden der Blockdiagonalmatrix bezeichne. Die Polynome $q_i(X)$ sind hierbei i.a.* nicht *paarweise verschieden. Eine Matrix dieser Form heiße* in sortierter Smithform. *Die Polynome q_i und die Exponenten b_i sind durch Angabe von C bis auf Reihenfolge festgelegt.*

Beweis. Wir dürfen C als in Smithform gegeben annehmen. Ferner dürfen wir annehmen, daß alle Diagonaleinträge Produkte gewisser Potenzen von Polynomen in $\mathrm{Irr}(K[X])$ sind, da wir gegebenenfalls noch mit einer invertierbaren Diagonalmatrix in $K^{n\times n}$ multiplizieren dürfen. Sei $g(X) := \det C \in K[X]$. Nach Voraussetzung ist $\deg(g) = n$.

Wir behaupten, daß eine Diagonalmatrix mit Determinante $g(X)$ und wenigstens einem Diagonaleintrag, der von zwei verschiedenen irreduziblen Polynomen geteilt wird, noch einen Diagonaleintrag assoziiert zu 1 besitzt. Nehmen wir hierzu an, dies sei nicht der Fall. Dann hat jeder Diagonaleintrag einen Grad $\geqslant 1$, und wenigstens einer einen Grad > 1. Insgesamt hat die Determinante dieser Diagonalmatrix einen Grad $> n = \deg g(X)$. Widerspruch.

Wir behaupten, daß wir erreichen können, daß alle Diagonaleinträge Potenzen eines einzigen irreduziblen Polynoms sind. Da wir Diagonaleinträge beliebig vertauschen dürfen, genügt es dafür, für $h_1(X)$ und $h_2(X)$ in $K[X] \smallsetminus \{0\}$ mit größtem gemeinsamen Teiler 1 von $\{h_1(X), h_2(X)\}$, die Matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & h_1h_2 \end{smallmatrix}\right)$ mit invertierbaren Matrizen von links und von rechts so zu multiplizieren, daß wir $\left(\begin{smallmatrix} h_1 & 0 \\ 0 & h_2 \end{smallmatrix}\right)$ erhalten. Denn dann können wir zu einem Faktor, der nicht Potenz eines einzigen irreduziblen Polynoms ist, oben eine 1 hintauschen und diese Tatsache anwenden, um eine Potenz eines irreduziblen Polynoms abzuspalten. Nun gibt es $r_1(X)$ und $r_2(X)$ in $K[X]$ mit $h_1r_1 + h_2r_2 = 1$. Damit wird in der Tat

$$\left(\begin{smallmatrix} h_1 & -r_2 \\ h_2 & r_1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & h_1h_2 \end{smallmatrix}\right)\left(\begin{smallmatrix} h_1r_1 & h_2r_2 \\ -1 & 1 \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} h_1 & 0 \\ 0 & h_2 \end{smallmatrix}\right) .$$

Sind schließlich k Diagonaleinträge gleich $q_i^{b_i}$ mit einem $b_i \geqslant 1$ und mit $q_i(X) \in \mathrm{Irr}(K[X])$, und die übrigen $n-k$ Einträge gleich 1, so bleibt uns für die behauptete zu erreichende Form der Matrix nachzuweisen, daß dann $n - k \overset{!}{=} \sum_{i\in[1,k]}(b_i \cdot \deg(q_i) - 1)$. Nun ist aber $\sum_{i\in[1,k]} b_i \cdot \deg(q_i) = \deg(g) = n$. Somit können wir eine Matrix in sortierter Smithform erreichen.

Die Faktoren $q_i(X)^{b_i}$ sind dabei gerade die Potenzen irreduzibler Polynome, die in den Primfaktorzerlegungen der Elementarteiler von C auftreten, wie uns obiges Argument zeigt, wenn wir es rückwärts lesen und $\left(\begin{smallmatrix} h_1 & 0 \\ 0 & h_2 \end{smallmatrix}\right)$ in $\left(\begin{smallmatrix} 1 & 0 \\ 0 & h_1h_2 \end{smallmatrix}\right)$ umformen. Da C seine Elementarteiler bis auf Assoziation festlegt, und diese ihre Primfaktorzerlegungen festlegen, ist insgesamt die sortierte Smithform bis auf die Reihenfolge der Blöcke ebenfalls eindeutig von C festgelegt. ▫

Seien $n \geqslant 1$ und $A, B \in K^{n\times n}$ gegeben. Die Matrix $XE - A \in K[X]^{n\times n}$ heißt *charakteristische Matrix* von A. Wir erinnern uns daran, daß A und B *konjugiert* heißen, falls ein $S \in \mathrm{GL}_n(K)$ existiert mit $S^{-1}AS = B$. Konjugiertheit ist eine Äquivalenzrelation. Die zugehörigen Äquivalenzklassen heißen auch *Konjugationsklassen.*

Lemma B. *Es sind A und B genau dann konjugiert, wenn es $P, Q \in \mathrm{GL}_n(K[X])$ gibt mit $P(XE - A)Q = XE - B$. In anderen Worten, A und B sind genau dann konjugiert, wenn ihre charakteristischen Matrizen dieselbe Smithform besitzen.*

Beweis. Zum einen, sind A und B konjugiert, ist also etwa $AS = SB$ mit $S \in \mathrm{GL}_n(K)$, so folgt $(XE - A)S = S(XE - B)$, und wir sind fertig wegen $S \in \mathrm{GL}_n(K) \leqslant \mathrm{GL}_n(K[X])$.

Zum anderen, seien $P, Q \in \mathrm{GL}_n(K[X])$ gegeben mit $P(XE - A) = (XE - B)Q^{-1}$. Schreiben wir

$$\begin{array}{rcl} P &=& \sum_{i\geqslant 0} P_i X^i \\ Q &=& \sum_{i\geqslant 0} Q_i X^i \\ Q^{-1} &=& \sum_{i\geqslant 0} \check{Q}_i X^i \end{array}$$

mit $P_i, Q_i, \check{Q}_i \in K^{n\times n}$, und für jeweils nur endlich viele Indizes i ungleich 0, und setzen wir dazuhin

$P_{-1} = \check{Q}_{-1} := 0_{n,n}$, so wird

$$P(XE - A) \;=\; \left(\sum_{i\geqslant 0} P_i X^{i+1}\right) - \left(\sum_{i\geqslant 0} P_i A X^i\right) \;=\; \sum_{i\geqslant 0}(P_{i-1} - P_i A)X^i\;,$$

und analog

$$(XE - B)Q^{-1} \;=\; \left(\sum_{i\geqslant 0} \check{Q}_i X^{i+1}\right) - \left(\sum_{i\geqslant 0} B\check{Q}_i X^i\right) \;=\; \sum_{i\geqslant 0}(\check{Q}_{i-1} - B\check{Q}_i)X^i\;,$$

Koeffizientenvergleich zeigt nun, daß $P_{i-1} - P_i A = \check{Q}_{i-1} - B\check{Q}_i$ für alle $i \geqslant 0$. Sei

$$T \;:=\; \sum_{i\geqslant 0} \check{Q}_i A^i \;\in\; K^{n\times n}\;.$$

Dann ist

$$\begin{array}{rcl}
TA & = & \left(\sum_{i\geqslant 0} \check{Q}_i A^i\right) A \\
& = & \sum_{i\geqslant 0}(B\check{Q}_{i+1} + P_i - P_{i+1}A)A^{i+1} \\
& = & \left(\sum_{i\geqslant 0} B\check{Q}_{i+1}A^{i+1}\right) + \left(\sum_{i\geqslant 0} P_i A^{i+1}\right) - \left(\sum_{i\geqslant 0} P_{i+1}A^{i+2}\right) \\
& = & \left(\sum_{i\geqslant 0} B\check{Q}_{i+1}A^{i+1}\right) + P_0 A \\
& = & \left(\sum_{i\geqslant 0} B\check{Q}_{i+1}A^{i+1}\right) + B\check{Q}_0 \\
& = & B\left(\sum_{i\geqslant 0} \check{Q}_i A^i\right) \\
& = & BT\;.
\end{array}$$

Wir haben noch zu zeigen, daß $T \in \mathrm{GL}_n(K)$ liegt. Es ist

$$\begin{array}{rcl}
E & = & QQ^{-1} \\
& = & \sum_{l\geqslant 0} X^l \left(\sum_{i+j\,=\,l} Q_j\check{Q}_i\right)\;,
\end{array}$$

so daß Koeffizientenvergleich $Q_0\check{Q}_0 = E$ und $\sum_{i+j=l} Q_j\check{Q}_i = 0$ für $l \geqslant 1$ ergibt. Sei

$$S \;:=\; \sum_{j\geqslant 0} Q_j B^j \;\in\; K^{n\times n}\;.$$

Es wird

$$\begin{array}{rcl}
ST & = & \sum_{j\geqslant 0} Q_j B^j T \\
& = & \sum_{j\geqslant 0} Q_j T A^j \\
& = & \sum_{i,\,j\,\geqslant\,0} Q_j(\check{Q}_i A^i)A^j \\
& = & \sum_{l\geqslant 0}\left(\sum_{i+j\,=\,l} Q_j\check{Q}_i\right) A^l \\
& = & E\;.
\end{array}$$

□

Folgerung. *Sei $\mathcal{J} \subseteq K^{n\times n}$ eine Teilmenge derart, daß es für jede Matrix der Form*

$$\mathrm{diag}\Big(\Delta_{b_1\cdot\deg(q_1)}(q_1^{b_1}),\,\Delta_{b_2\cdot\deg(q_2)}(q_2^{b_2}),\,\ldots,\,\Delta_{b_k\cdot\deg(q_k)}(q_k^{b_k})\Big)$$

mit $q_i(X) \in \mathrm{Irr}(K[X])$, mit $b_i \geqslant 1$ und mit $\sum_{i\in[1,k]} b_i \cdot \deg(q_i) = n$ genau ein $J \in \mathcal{J}$ gibt, dessen charakteristische Matrix $XE - J$ diese sortierte Smithform besitzt. Dann ist $\mathcal{J}$ ein Repräsentantensystem für die Konjugationsklassen von $K^{n\times n}$. □

Um nun Normalformen, d.h. eben solche Repräsentantensysteme $\mathcal{J}$, zu konstruieren, genügt es, von gewissen ausgesuchten Matrizen die sortierte Smithform ihrer charakteristischen Matrix auszurechnen. Notieren wir uns hierbei aufgetretene Transformationsmatrizen, so haben wir auch gleich einen Algorithmus, um den Repräsentanten einer gegebenen Matrix samt der zur Konjugation benötigten Matrix zu bestimmen. Siehe §4.4.4.2.

Sei $f(X) = X^l + \sum_{i\in[0,l-1]} a_i X^i \in K[X]$ ein normiertes Polynom von Grad $l \geqslant 1$. Die *Begleitmatrix* zu f ist gegeben durch

$$B_f \;:=\; \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \\ 0 & \cdots & & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & & \cdots & -a_{l-1} \end{pmatrix} \;\in\; K^{l\times l}\,.$$

So ist etwa für $\lambda \in K$ die Begleitmatrix $B_{X-\lambda} = (\,\lambda\,) \in K^{1\times 1}$.

Sei ferner, bei gegebenem $l \geqslant 1$,

$$L_l \;=\; \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \;\in\; K^{l\times l}\,.$$

So ist etwa $L_1 = (\,1\,) \in K^{1\times 1}$.

Sei $q(X) \in \mathrm{Irr}(K[X])$, und sei $b \geqslant 1$. Wir bilden den folgenden (verallgemeinerten) *Jordanblock*

$$\mathrm{J}(q,b) \;:=\; \begin{pmatrix} B_q & L_{\deg(q)} & 0 & \cdots & \cdots & 0 \\ 0 & B_q & L_{\deg(q)} & 0 & \cdots & 0 \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \\ 0 & \cdots & \cdots & 0 & B_q & L_{\deg(q)} \\ 0 & \cdots & & \cdots & 0 & B_q \end{pmatrix} \;\in\; K^{(b\cdot\deg(q))\times(b\cdot\deg(q))}\,.$$

Die erste obere Nebendiagonale ist also durchgehend mit 1en belegt.

So zum Beispiel ergibt sich, in der Notation von Satz 13, der Jordanblock $\mathrm{J}(X-\lambda, b) = \lambda E_b + N_b$, also ein dort bereits aufgetretener Jordanblock der Kantenlänge b mit Eigenwert λ. Ist nun K *nicht* algebraisch abgeschlossen, so können außer Polynomen von Grad 1 noch weitere irreduzible Polynome auftreten, und also auch etwas allgemeinere Jordanblöcke als die in Satz 13 bereits in Erscheinung getretenen.

Lemma C. *Sei $q(X) \in \mathrm{Irr}(K[X])$ von Grad $r := \deg(q)$, und sei $b \geqslant 1$. Die sortierte Smithform der charakteristischen Matrix von $\mathrm{J}(q,b)$ ist gegeben durch $\mathrm{diag}(1,\ldots,1,q^b) \in K[X]^{br\times br}$. Genauer, es gibt ein $\tilde{P} \in \mathrm{GL}_{br}(K[X])$ derart, daß mit*

$$v \;=\; (\; q^0X^0 \;\; q^0X^1 \;\ldots\; q^0X^{r-1} \;\; q^1X^0 \;\; q^1X^1 \;\ldots\; q^1X^{r-1} \;\;\ldots\;\; q^{b-1}X^0 \;\; q^{b-1}X^1 \;\ldots\; q^{b-1}X^{r-1} \;)^{\mathrm{t}} \;\in\; K[X]^{br}$$

und der durch ihr Spaltentupel definierten Matrix

$$\mathrm{Q}(q,b) \;:=\; (e_2, e_3, \ldots, e_{br}, v) \;\in\; \mathrm{GL}_{br}(K[X])$$

wir

$$(XE - \mathrm{J}(q,b))\cdot \mathrm{Q}(q,b) \;=\; \tilde{P}\cdot \mathrm{diag}(1,\ldots,1,q^b)$$

erhalten.

Beweis. Es genügt zu zeigen, daß $(XE - \mathrm{J}(q,b))\,\mathrm{Q}(q,b)$ eine untere Dreiecksmatrix mit Diagonale $(-1,\ldots,-1,q^b)$ ist. Denn dann ergibt sich $\tilde{P} := (\ (XE - \mathrm{J}(q,b))\,\mathrm{Q}(q,b)\ ) \cdot \mathrm{diag}(1,\ldots,1,q^{-b})$, welche als untere Dreiecksmatrix mit Diagonale $(-1,\ldots,-1,+1)$ in der Tat in $\mathrm{GL}_n(K[X])$ liegt. Wegen der Gestalt von $XE - \mathrm{J}(q,b)$ und $\mathrm{Q}(q,b)$ genügt dafür aber bereits $(XE - \mathrm{J}(q,b))v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ q^b \end{pmatrix}$, was wir direkt ersehen. $\square$

Beispiel. Für $\lambda \in K$ ist $\mathrm{Q}(X-\lambda,1) = (\ 1\ )$. Oder, es ergibt sich zum Beispiel im Falle $K = \mathbf{R}$ die Matrix

$$\mathrm{Q}(X^2+1,2) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & X \\ 0 & 1 & 0 & X^2{+}1 \\ 0 & 0 & 1 & X(X^2{+}1) \end{pmatrix} \in \mathbf{R}[X]^{4\times 4}\,.$$

Bemerkung. Seien m, $n \geqslant 1$. Ist $D \in K[X]^{m\times m}$ die sortierte Smithform der charakteristischen Matrix von $A \in K^{m\times m}$, und ist $D' \in K[X]^{n\times n}$ die sortierte Smithform der charakteristischen Matrix von $A' \in K^{n\times n}$, so ist $\left(\begin{smallmatrix} D & 0 \\ 0 & D' \end{smallmatrix}\right) \in K[X]^{(m+n)\times(m+n)}$ die sortierte Smithform der charakteristischen Matrix von $\left(\begin{smallmatrix} A & 0 \\ 0 & A' \end{smallmatrix}\right) \in K^{(m+n)\times(m+n)}$. Kurz, wir dürfen die sortierte Smithform blockweise berechnen.

Damit haben wir zu jeder in obiger Folgerung geforderten sortierten Smithform einen Konjugationsrepräsentanten gefunden, der sich als Blockdiagonalmatrix aus Jordanblöcken zusammensetzt. Wir fassen nun zu einem theoretischen Ergebnis zusammen. Mit diag werden dabei jeweils Blockdiagonalmatrizen gebildet.

Satz über die Jordanform, nach Frobenius und Böge. *Sei $n \geqslant 1$, sei K ein beliebiger Körper. Jede Matrix $A \in K^{n\times n}$ ist konjugiert zu einer Matrix in* Jordanscher Normalform, *oder kurz* Jordanform,

$$\mathrm{diag}(\mathrm{J}(q_1,b_1),\mathrm{J}(q_2,b_2),\ldots,\mathrm{J}(q_k,b_k))\ ,$$

wobei die irreduziblen Polynome q_1, …, q_k und die positiven ganzen Zahlen b_1, …, b_k (bis auf Reihenfolge) durch die sortierte Smithform

$$\mathrm{diag}\Big(\Delta_{b_1\cdot\deg(q_1)}(q_1^{b_1}),\Delta_{b_2\cdot\deg(q_2)}(q_2^{b_2}),\ldots,\Delta_{b_k\cdot\deg(q_k)}(q_k^{b_k})\Big)$$

der charakteristischen Matrix von A festgelegt sind. $\square$

Minimalpolynom. Das Minimalpolynom von $\mathrm{J}(q,b)$ für $q \in \mathrm{Irr}(K[X])$ und $b \geqslant 0$ ist gegeben durch $q(X)^b$.

Dazu behaupten wir, daß die Matrix $\mathrm{J}(q,b)$ von $q(X)^b$, nicht aber von $q(X)^{b-1}$ annulliert wird. Es ist $q(\mathrm{J}(q,b))$ eine obere Blockdreiecksmatrix mit verschwindenden Hautptdiagonalblöcken der Größe $\deg(q)\times\deg(q)$; und Blöcken in der ersten oberen Blocknebendiagonalen, welche allesamt untere Dreiecksmatrizen mit Einsen auf der Hauptdiagonalen sind; was wiederum aus der Tatsache folgt, daß $\mathrm{J}(q,b)$ auf der ersten oberen Nebendiagonalen Einsen stehen hat, und darüber nur noch Nullen.

Da das Minimalpolynom unter Konjugation einer Matrix invariant bleibt, ist, in der Notation des vorstehenden Satzes, das Minimalpolynom von A das kleinste gemeinsame Vielfache in $K[X]$ der Polynome $q_1^{b_1}$, …, $q_k^{b_k}$. In anderen Worten, das Minimalpolynom von A ist der Elementarteiler größten Grades der charakteristischen Matrix von A, zu finden im rechten unteren Eck der Smithform.

4.4.4 $*$ Algorithmus

4.4.4.1 $*$ Vorbemerkungen

Bemerkung a. Wir werden vor der Aufgabe stehen, eine Matrix $C \in K[X]^{n\times n}$ in sortierte Smithform $P'CQ'$ zu bekommen, mit P' und Q' in $\mathrm{GL}_n(K[X])$, und uns dabei Q' zu behalten. Dazu schreiben wir die Einheitsmatrix unter die Matrix C und wenden alle *Spalten*umformungen, die auf C angewandt werden, simultan auf die unten angefügte Matrix an.

Um zur sortierten Smithform zu gelangen, bilden wir zunächst die Smithform und spalten dann Diagonaleinträge, die noch verschiedene irreduzible Teiler haben, auf. Dazu hilft folgende Bemerkung.

Bemerkung b. Sind $h_1(X)$ und $h_2(X)$, so können wir zur Berechnung des größten gemeinsamen Teilers von $\{h_1, h_2\}$ den Euklidschen Algorithmus anwenden. Sei iterativ für $i \geqslant 1$

$$h_i \;=\; h_{i+1}u_{i+1} + h_{i+2}\;,$$

mit entweder $h_{i+2} = 0$ oder $\deg(h_{i+2}) < \deg(h_{i+1})$. Breche ab, falls $h_{i+2} = 0$. Das von h_i und h_{i+1} erzeugte Ideal stimmt mit dem von h_{i+1} und h_{i+2} erzeugten Ideal überein, da h_i in letzerem und h_{i+2} in ersterem enthalten ist. Insbesondere, sind $h_m \neq 0$ und $h_{m+1} = 0$, so ist das von h_1 und h_2 erzeugte Ideal gleich $h_m(X)K[X]$, in anderen Worten, h_m ist der größte gemeinsame Teiler von h_1 und h_2.

Damit muß es Polynome $s_1(X)$ und $t_1(X)$ geben mit $h_1s_1 + h_2t_1 = h_m$. Rechnerisch erhalten wir diese, indem wir iterativ $\binom{s_m}{t_m} = \binom{1}{0}$ und

$$\binom{s_{i-1}}{t_{i-1}} \;=\; \begin{pmatrix} 0 & 1 \\ 1 & -u_i \end{pmatrix}\binom{s_i}{t_i}$$

setzen. Denn es ist $h_m = h_m s_m + h_{m+1}t_m$, und induktiv folgt

$$\begin{array}{rcl} h_m & = & h_i s_i + h_{i+1}t_i \\ & = & h_i s_i + (h_{i-1} - h_i u_i)t_i \\ & = & h_{i-1}t_i + h_i(s_i - u_i t_i) \\ & = & h_{i-1}s_{i-1} + h_i t_{i-1} \end{array}$$

Ist h_m ein Skalar, so wird schließlich

$$h_1(s_1/h_m) + h_2(t_1/h_m) \;=\; 1\;.$$

Dies können wir verwenden, um aus der Smithform zur sortierten Smithform zu gelangen; vgl. den Beweis zu Lemma A.

Bemerkung c. Sei $q(X) \in \mathrm{Irr}(K[X])$ von Grad $r := \deg(q)$, und sei $b \geqslant 1$. Schreibe

$$w \;=\; (\; -q^0X^1 \;\; -q^0X^2 \;\; \ldots \;\; -q^0X^{r-1} \;\; -q^1X^0 \;\; -q^1X^1 \;\; \ldots \;\; -q^1X^{r-1} \;\; \ldots \;\; -q^{b-1}X^0 \;\; -q^{b-1}X^1 \;\; \ldots \;\; -q^{b-1}X^{r-1} \;\; 1\;)^{\mathrm{t}} \;\in\; K[X]^{br}\;.$$

Die Inverse zu $\mathrm{Q}(q,b)$ ist wie folgt durch ihr Spaltentupel gegeben.

$$\mathrm{Q}(q,b)^{-1} \;=\; (w, e_1, e_2, \ldots, e_{br-1}) \;\in\; \mathrm{GL}_{br}(K[X])\;.$$

Beispiel. Für $\lambda \in K$ ist $\mathrm{Q}(X-\lambda,1)^{-1} = (\;1\;)$. Oder, es ergibt sich zum Beispiel im Falle $K = \mathbf{R}$ die Matrix $\mathrm{Q}(X^2+1,2)^{-1} = \begin{pmatrix} -X & 1 & 0 & 0 \\ -(X^2+1) & 0 & 1 & 0 \\ -(X^2+1)X & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathbf{R}[X]^{4\times 4}$.

4.4.4.2 $*$ Verfahren

Sei $n \geqslant 1$, und sei $A \in K^{n\times n}$ gegeben. Seien P', $Q' \in \mathrm{GL}_n(K[X])$ so, daß

$$P'(XE-A)Q' \;=\; \mathrm{diag}\Big(\Delta_{b_1\cdot\deg(q_1)}(q_1^{b_1}), \Delta_{b_2\cdot\deg(q_2)}(q_2^{b_2}), \ldots, \Delta_{b_k\cdot\deg(q_k)}(q_k^{b_k})\Big)$$

in sortierter Smithform ist, mit $q_i \in \mathrm{Irr}(K[X])$ und $b_i \geqslant 1$, vgl. Lemma A und Bemerkungen a, b. Nun hat mit Lemma C

$$J \;:=\; \mathrm{diag}(\mathrm{J}(q_1, b_1), \mathrm{J}(q_2, b_2), \ldots, \mathrm{J}(q_k, b_k))$$

ebenfalls diese Smithform, und die für die Umformung in diese Smithform nötige Matrix von rechts können wir wie folgt spezifizieren. Es gibt mit Lemma C eine Matrix $\tilde{P} \in \mathrm{GL}_n(K[X])$ derart, daß

$$\tilde{P}\big(P'(XE - A)Q'\big) \;=\; (XE - J)\,\mathrm{diag}(\mathrm{Q}(q_1, b_1), \mathrm{Q}(q_2, b_2), \ldots, \mathrm{Q}(q_k, b_k)) \;.$$

Setzen wir

$$\begin{array}{rcl} P & := & \tilde{P}P' \\ Q & := & Q' \cdot \mathrm{diag}(\mathrm{Q}(q_1, b_1)^{-1}, \mathrm{Q}(q_2, b_2)^{-1}, \ldots, \mathrm{Q}(q_k, b_k)^{-1}) \;, \end{array}$$

so folgt

$$P(XE - A) \;=\; (XE - J)Q^{-1} \;.$$

Schreiben wir nun $Q =: \sum_{i \geqslant 0} Q_i X^i$ mit $Q_i \in K^{n\times n}$, so ist gemäß Beweis von Lemma B mit $S := \sum_{i\geqslant 0} Q_i J^i$ eine Matrix gefunden, die wie gewünscht

$$S^{-1}AS \;=\; J$$

liefert. Zur Berechnung von Q ist Bemerkung c von Nutzen.

Wir fassen die Rechenschritte zusammen.

Die Jordanform J einer Matrix $A \in K^{n\times n}$ und die Transformationsmatrix $S \in \mathrm{GL}_n(K)$, für die $S^{-1}AS = J$ ist, kann in den folgenden Schritten berechnet werden.

(1) Berechne die sortierte Smithform der charakteristischen Matrix $XE - A$ von A.
Ist mit P', $Q' \in \mathrm{GL}_n(K[X])$ erreicht, daß sich

$$P'(XE - A)Q' \;=\; \mathrm{diag}\Big(\Delta_{b_1\cdot\deg(q_1)}(q_1^{b_1}), \Delta_{b_2\cdot\deg(q_2)}(q_2^{b_2}), \ldots, \Delta_{b_k\cdot\deg(q_k)}(q_k^{b_k})\Big) \;,$$

in sortierter Smithform ergibt, so behalten wir Q'.

(2) Berechne die Matrix

$$Q \;=\; \sum_{i\geqslant 0} Q_i X^i \;:=\; Q' \cdot \mathrm{diag}(\mathrm{Q}(q_1, b_1)^{-1}, \mathrm{Q}(q_2, b_2)^{-1}, \ldots, \mathrm{Q}(q_k, b_k)^{-1}) \;,$$

wobei $Q_i \in K^{n\times n}$.

(3) Sei $J := \mathrm{diag}(\mathrm{J}(q_1, b_1), \mathrm{J}(q_2, b_2), \ldots, \mathrm{J}(q_k, b_k))$. Bilde

$$S \;:=\; \sum_{i\geqslant 0} Q_i J^i \;.$$

Nun ist $S^{-1}AS = J$.

(4) Zur Probe verifizieren wir $AS \overset{!}{=} SJ$. Ist dazuhin S tatsächlich regulär, so ist das Resultat sicher korrekt.

Wie jeder (mir bekannte) Algorithmus, so hat auch dieser einen Haken. Schritt (1), die 'verfeinerte Berechnung des charakteristischen Polynoms', kann zu länglichen Polynomen als Matrixeinträgen in der Transformationsmatrix Q' führen.

4.4.4.3 $*$ Beispiele

4.4.4.3.1 $*$ Ein Beispiel über R und C

(I) Sei $K = \mathbf{R}$, und sei $A = \left(\begin{smallmatrix} -3 & 2 & -3 \\ 0 & 1 & -1 \\ 5 & -3 & 4 \end{smallmatrix}\right) \in \mathbf{R}^{3\times 3}$. Wir formen die charakteristische Matrix $XE - A$ von A in Smithform um. Dabei führen wir die Spaltenumformungen simultan auf der unten angefügten Matrix durch, die zu anfangs gleich E sei. Zeilenumformungen lassen die unten angefügte Matrix unverändert.

$$\left(\begin{array}{ccc} X+3 & -2 & 3 \\ 0 & X-1 & 1 \\ -5 & 3 & X-4 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc} 3 & -2 & X+3 \\ 1 & X-1 & 0 \\ X-4 & 3 & -5 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc} 1 & X-1 & 0 \\ 3 & -2 & X+3 \\ X-4 & 3 & -5 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1-3X & X+3 \\ 0 & -X^2+5X-1 & -5 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1-X & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & -X^2+5X-1 \\ 0 & -(X+3)/5 & 1-3X \\ \hline 0 & -1/5 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1-X \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-2)(X^2+1) \\ \hline 0 & -1/5 & -X^2/5+X-1/5 \\ 0 & 0 & 1 \\ 1 & 0 & 1-X \end{array}\right).$$

Um diese Matrix nun in sortierte Smithform zu bekommen, stellen wir zunächst einmal fest, daß

$$(1/5)(X^2 + 1) + (-(X + 2)/5)(X - 2) \;=\; 1\,.$$

Also multiplizieren wir ihren unteren rechten 2×2-Block von links mit $\left(\begin{smallmatrix} X^2+1 & (X+2)/5 \\ X-2 & 1/5 \end{smallmatrix}\right)$ und von rechts mit $\left(\begin{smallmatrix} (X^2+1)/5 & -(X-2)(X+2)/5 \\ -1 & 1 \end{smallmatrix}\right)$, und erhalten

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & X^2+1 & 0 \\ 0 & 0 & X-2 \\ \hline 0 & \frac{4X^2}{25}-X+\frac{4}{25} & -\frac{4X^2}{25}+X-\frac{9}{25} \\ 0 & -1 & 1 \\ 1 & X-1 & 1-X \end{array}\right).$$

Die untenstehende Matrix ist unsere Matrix Q'.

Somit wird

$$\begin{aligned} Q &= Q' \cdot \mathrm{diag}(\mathrm{Q}(X^2+1,1)^{-1}, \mathrm{Q}(X-2,1)^{-1}) \\ &= Q' \cdot \left(\begin{smallmatrix} -X & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \\ &= \begin{pmatrix} \frac{4X^2}{25}-X+\frac{4}{25} & 0 & -\frac{4X^2}{25}+X-\frac{9}{25} \\ -1 & 0 & 1 \\ -1 & 1 & 1-X \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} \frac{4}{25} & 0 & -\frac{9}{25} \\ -1 & 0 & 1 \\ -1 & 1 & 1 \end{pmatrix}}_{Q_0} \cdot X^0 + \underbrace{\begin{pmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{Q_1} \cdot X^1 + \underbrace{\begin{pmatrix} \frac{4}{25} & 0 & -\frac{4}{25} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{Q_2} \cdot X^2\,. \end{aligned}$$

Mit $J = \operatorname{diag}(\mathrm{J}(X^2+1,1), \mathrm{J}(X-2,1)) = \left(\begin{smallmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 2 \end{smallmatrix}\right)$ wird

$$\begin{array}{rcl} S & = & Q_0 J^0 + Q_1 J^1 + Q_2 J^2 \\ & = & \left(\begin{smallmatrix} 4/25 & 0 & -9/25 \\ -1 & 0 & 1 \\ -1 & 1 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & -1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{smallmatrix}\right) + \left(\begin{smallmatrix} -4/25 & 0 & -16/25 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \\ & = & \left(\begin{smallmatrix} 0 & -1 & 1 \\ -1 & 0 & 1 \\ -1 & 1 & -1 \end{smallmatrix}\right) . \end{array}$$

In der Tat ist nun $S^{-1}AS = J$.

(II) Sei nun $K = \mathbf{C}$, und sei weiterhin $A = \left(\begin{smallmatrix} -3 & 2 & -3 \\ 0 & 1 & -1 \\ 5 & -3 & 4 \end{smallmatrix}\right)$, nur jetzt gesehen in $\mathbf{C}^{3\times 3}$. Nun sind wir im Falle eines algebraisch abgeschlossenen Körpers $\mathbf{C}$, müßten also nicht unbedingt das Frobenius-Böge-Verfahren anwenden. Wir wollen dies trotzdem tun. Zur Unterscheidung der in den verschiedenen Berechnungen auftretenden Matrizen verwenden wir obere Indizes in Klammern.

Unter Zuhilfenahme von (I) genügt es, den Block $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ aus der Jordanform über $\mathbf{R}$ nun über $\mathbf{C}$ in Jordanform zu bringen, und danach die Transformationsmatrizen zu multiplizieren. Seine charakteristische Matrix wird unter Verwendung von Lemma C umgeformt zu

$$\left(\begin{array}{cc} X & -1 \\ 1 & X \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc} 1 & 0 \\ 0 & X^2+1 \\ \hline 0 & 1 \\ 1 & X \end{array}\right) \rightsquigarrow \left(\begin{array}{cc} X+i & 0 \\ 0 & X-i \\ \hline -1 & 1 \\ (-1-\frac{i}{2})X+\frac{1}{2} & (1+\frac{i}{2})X+\frac{1}{2} \end{array}\right) ,$$

unter Verwendung der Tatsache, daß $(-\frac{i}{2})(X+i)+\frac{i}{2}(X-i) = 1$. Es ist $\operatorname{diag}(\mathrm{Q}(X+i,1)^{-1}, \mathrm{Q}(X-i,1)^{-1}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, und daher erhalten wir direkt, mit $J^{(1)} = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right)$,

$$S^{(1)} \;=\; Q_0^{(1)}(J^{(1)})^0 + Q_1^{(1)}(J^{(1)})^1 \;=\; \left(\begin{smallmatrix} -1 & 1 \\ 1/2 & 1/2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ -1-i/2 & 1+i/2 \end{smallmatrix}\right) \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} -1 & 1 \\ i & i \end{smallmatrix}\right) .$$

In der Tat ist nun $(S^{(1)})^{-1} \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) S^{(1)} = J^{(1)}$.

Insgesamt wird mit $S^{(2)} = S \cdot \operatorname{diag}(S^{(1)}, 1) = \left(\begin{smallmatrix} -i & -i & 1 \\ 1 & -1 & 1 \\ 1+i & -1+i & -1 \end{smallmatrix}\right)$ dann

$$(S^{(2)})^{-1} A S^{(2)} = \operatorname{diag}(J^{(1)}, 2) = \left(\begin{smallmatrix} -i & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & 2 \end{smallmatrix}\right) \;=:\; J^{(2)} ,$$

und dies ist eine Transformation in die Jordanform über $\mathbf{C}$.

Wir hätten auch über $\mathbf{C}$ direkt das Frobenius-Böge-Verfahren für A ansetzen können; wir sind nicht darauf angewiesen, zunächst die Jordanform über $\mathbf{R}$ zu berechnen.

4.4.4.3.2 $*$ Ein Beispiel über $\mathbf{F}_3$ und $\mathbf{F}_9$

(I) Sei $K = \mathbf{F}_3$, und sei $A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ -1 & -1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix} \in \mathbf{F}_3^{6\times 6}$. Wir formen ihre charakteristische Matrix um.

$$
\left(\begin{array}{cccccc}
X-1 & 0 & -1 & 0 & -1 & 1 \\
0 & X & 0 & 1 & 1 & -1 \\
1 & 1 & X & 1 & 0 & 0 \\
-1 & 0 & 0 & X+1 & -1 & -1 \\
0 & -1 & -1 & 1 & X-1 & 1 \\
1 & 1 & -1 & 1 & -1 & X+1 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
\rightsquigarrow
\left(\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & -X+1 & -X^2+X-1 & -X+1 & -1 & 1 \\
0 & X & 0 & 1 & 1 & -1 \\
0 & 1 & X & X-1 & -1 & -1 \\
0 & -1 & -1 & 1 & X-1 & 1 \\
0 & 0 & -X-1 & 0 & -1 & X+1 \\
\hline
1 & -1 & -X & -1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

$$
\rightsquigarrow
\left(\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & -X^2-X+1 & X-1 & -X^2-X+1 & -X-1 \\
0 & 0 & -X & X+1 & X^2-X+1 & X-1 \\
0 & 0 & X-1 & X & X+1 & 0 \\
0 & 0 & -X-1 & 0 & -1 & X+1 \\
\hline
1 & -1 & -X+1 & 1 & -X+1 & -1 \\
0 & 1 & -1 & 1 & X-1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
\rightsquigarrow
\left(\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & X^2+X-1 & -X \\
0 & 0 & 0 & -1 & -X^2-X+1 & -X^2+1 \\
0 & 0 & 0 & X^2+X & X^2+X-1 & X^2-1 \\
\hline
1 & -1 & -X+1 & X^2-X+1 & X^2+X+1 & X^2+1 \\
0 & 1 & -1 & X+1 & -X-1 & X-1 \\
0 & 0 & 1 & -X & -X & -X-1 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

$$
\rightsquigarrow
\left(\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & (X^2+X-1) \\
0 & 0 & 0 & 0 & (X^2+X-1)^2 & -(X+1)(X^2+X-1) \\
\hline
1 & -1 & -X+1 & X^2-X+1 & -X^4-X^2-X-1 & X^3+X+1 \\
0 & 1 & -1 & X+1 & -X^3+X^2-X & X^2-X-1 \\
0 & 0 & 1 & -X & X^3+X^2+X & -X^2-X-1 \\
0 & 0 & 0 & 1 & -X^2-X+1 & X \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

$$
\rightsquigarrow
\left(\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & (X^2+X-1)^2 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & (X^2+X-1) \\
\hline
1 & -1 & -X+1 & -X^4-X^2-X-1 & X^2-X+1 & X^3+X+1 \\
0 & 1 & -1 & -X^3+X^2-X & X+1 & X^2-X-1 \\
0 & 0 & 1 & X^3+X^2+X & -X & -X^2-X-1 \\
0 & 0 & 0 & -X^2-X+1 & 1 & X \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{array}\right) .
$$

Die untenstehende Matrix ist Q'. Ferner ist

$$\operatorname{diag}(\mathrm{Q}(X^2+X-1,2)^{-1}, \mathrm{Q}(X^2+X-1,1)^{-1}) \;=\; \begin{pmatrix} -X & 1 & 0 & 0 & 0 & 0 \\ -(X^2{+}X{-}1) & 0 & 1 & 0 & 0 & 0 \\ -(X^2{+}X{-}1)X & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -X & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Somit wird

$$\begin{aligned} Q \;&=\; Q' \cdot \operatorname{diag}(\mathrm{Q}(X^2+X-1,2)^{-1}, \mathrm{Q}(X^2+X-1,1)^{-1}) \\ &=\; \begin{pmatrix} X^2{+}1 & 1 & -1 & -X{+}1 & X^2{+}1 & X^2{-}X{+}1 \\ X^2{+}1 & 0 & 1 & -1 & X{-}1 & X{+}1 \\ -X & 0 & 0 & 1 & -X{-}1 & -X \\ -X^2{-}X{+}1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ &=\; \underbrace{\begin{pmatrix} 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}}_{Q_0} \cdot X^0 + \underbrace{\begin{pmatrix} 0 & 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & -1 & -1 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}}_{Q_1} \cdot X^1 + \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}}_{Q_2} \cdot X^2 . \end{aligned}$$

Mit $J = \operatorname{diag}(\mathrm{J}(X^2+X-1,2), \mathrm{J}(X^2+X-1,1)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$ wird mithin

$$S \;=\; Q_0 J^0 + Q_1 J^1 + Q_2 J^2 \;=\; \begin{pmatrix} -1 & 0 & -1 & -1 & 0 & 0 \\ -1 & -1 & -1 & -1 & 0 & 1 \\ 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Und in der Tat ist $S^{-1}AS = J$.

(II) Sei $K = \mathbf{F}_9$, und sei weiterhin $A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ -1 & -1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}$, nur jetzt gesehen in $\mathbf{F}_9^{6\times 6}$. Unter Zuhilfenahme von (I) genügt es, die Blöcke $\mathrm{J}(X^2+X-1,1)$ und $\mathrm{J}(X^2+X-1,2)$ über $\mathbf{F}_9$ in Jordanform zu bringen.

Wir beginnen mit $\mathrm{J}(X^2+X-1,1)$. Seine charakteristische Matrix wird unter Verwendung von Lemma C umgeformt zu

$$\left(\begin{array}{cc} X & -1 \\ -1 & X{+}1 \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right) \;\rightsquigarrow\; \left(\begin{array}{cc} 1 & 0 \\ 0 & (X{-}(1{+}\iota))(X{-}(1{-}\iota)) \\ \hline 0 & 1 \\ 1 & X \end{array}\right) \;\rightsquigarrow\; \left(\begin{array}{cc} X{-}(1{+}\iota) & 0 \\ 0 & X{-}(1{-}\iota) \\ \hline -1 & 1 \\ (-1{-}\iota)X{+}(\iota{-}1) & (1{+}\iota)X{+}(-\iota{-}1) \end{array}\right).$$

Mit $J^{(1)} = \left(\begin{smallmatrix} 1+\iota & 0 \\ 0 & 1-\iota \end{smallmatrix}\right)$ bekommen wir

$$S^{(1)} \;=\; Q_0^{(1)}(J^{(1)})^0 + Q_1^{(1)}(J^{(1)})^1 \;=\; \left(\begin{smallmatrix} -1 & 1 \\ \iota-1 & -\iota-1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ -1-\iota & 1+\iota \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1+\iota & 0 \\ 0 & 1-\iota \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} -1 & 1 \\ -1-\iota & 1-\iota \end{smallmatrix}\right) \;,$$

und in der Tat ist $(S^{(1)})^{-1}\,\mathrm{J}(X^2+X-1,1)S^{(1)} = J^{(1)}$.

Wir setzen fort mit $\mathrm{J}(X^2+X-1,2)$. Seine charakteristische Matrix wird unter Verwendung von Lemma C umgeformt zu

$$\left(\begin{array}{cccc} X & -1 & 0 & 0 \\ -1 & X+1 & -1 & 0 \\ 0 & 0 & X & -1 \\ 0 & 0 & -1 & X+1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (X^2+X-1)^2 \\ \hline 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & X \\ 0 & 1 & 0 & (X^2+X-1) \\ 0 & 0 & 1 & (X^2+X-1)X \end{array}\right) \rightsquigarrow \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & (X-(\iota+1))^2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (X-(-\iota+1))^2 \\ \hline 0 & -1 & 0 & 1 \\ 1 & -X & 0 & X \\ 0 & \iota X^3-X^2-X-\iota & 0 & -\iota X^3+X^2+X+\iota+1 \\ 0 & -X^3-X^2+X & 1 & X^3+X^2-X \end{array}\right).$$

Wegen $J^{(2)} = \left(\begin{smallmatrix} 1+\iota & 1 & 0 & 0 \\ 0 & 1+\iota & 0 & 0 \\ 0 & 0 & 1-\iota & 1 \\ 0 & 0 & 0 & 1-\iota \end{smallmatrix}\right)$, wegen $\mathrm{Q}(X-(\iota+1),2)^{-1} = \left(\begin{smallmatrix} -X+(\iota+1) & 1 \\ 1 & 0 \end{smallmatrix}\right)$ und wegen $\mathrm{Q}(X-(-\iota+1),2)^{-1} = \left(\begin{smallmatrix} -X+(-\iota+1) & 1 \\ 1 & 0 \end{smallmatrix}\right)$ wird

$$Q = \begin{pmatrix} -1 & 0 & 1 & 0 \\ X+1+\iota & 1 & X & 0 \\ \iota X^3-X^2-X-\iota & 0 & -\iota X^3+X^2+X+\iota+1 & 0 \\ -X^3-X^2+X & 0 & X^3+X^2+X+1-\iota & 1 \end{pmatrix},$$

und somit

$$\begin{aligned} S^{(2)} &= Q_0\cdot(J^{(2)})^0 + Q_1\cdot(J^{(2)})^1 + Q_2\cdot(J^{(2)})^2 + Q_3\cdot(J^{(2)})^3 \\ &= \left(\begin{smallmatrix} -1 & 0 & 1 & 0 \\ \iota+1 & 1 & 0 & 0 \\ -\iota & 0 & \iota+1 & 0 \\ 0 & 0 & -\iota+1 & 1 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0&0&0&0 \\ 1&0&1&0 \\ -1&0&1&0 \\ 1&0&1&0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 1+\iota & 1 & 0 & 0 \\ 0 & 1+\iota & 0 & 0 \\ 0 & 0 & 1-\iota & 1 \\ 0 & 0 & 0 & 1-\iota \end{smallmatrix}\right) \\ &+ \left(\begin{smallmatrix} 0&0&0&0 \\ 0&0&0&0 \\ -1&0&1&0 \\ -1&0&1&0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} -\iota & -1-\iota & 0 & 0 \\ 0 & -\iota & 0 & 0 \\ 0 & 0 & \iota & -1+\iota \\ 0 & 0 & 0 & \iota \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0&0&0&0 \\ 0&0&0&0 \\ \iota&0&-\iota&0 \\ -1&0&1&0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 1-\iota & 0 & 0 & 0 \\ 0 & 1-\iota & 0 & 0 \\ 0 & 0 & 1+\iota & 0 \\ 0 & 0 & 0 & 1+\iota \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} -1 & 0 & 1 & 0 \\ -\iota-1 & -1 & 1-\iota & 1 \\ 0 & \iota & 0 & \iota \\ 0 & \iota-1 & 0 & \iota+1 \end{smallmatrix}\right). \end{aligned}$$

In der Tat ist $(S^{(2)})^{-1}\,\mathrm{J}(X^2+X-1,2)S^{(2)} = J^{(2)}$. Zusammen ist also mit

$$S^{(3)} = S\cdot\mathrm{diag}(S^{(2)},S^{(1)}) = \left(\begin{smallmatrix} 1 & 1+\iota & -1 & -1+\iota & 0 & 0 \\ -1+\iota & -1+\iota & 1+\iota & 1+\iota & -1-\iota & 1-\iota \\ 1+\iota & \iota & -1+\iota & \iota & -1 & 1 \\ 0 & -\iota & 0 & -\iota & -1-\iota & 1-\iota \\ -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{smallmatrix}\right)$$

die Jordanform

$$(S^{(3)})^{-1}AS^{(3)} = \left(\begin{smallmatrix} 1+\iota & 1 & 0 & 0 & 0 & 0 \\ 0 & 1+\iota & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\iota & 1 & 0 & 0 \\ 0 & 0 & 0 & 1-\iota & 0 & 0 \\ 0 & 0 & 0 & 0 & 1+\iota & 0 \\ 0 & 0 & 0 & 0 & 0 & 1-\iota \end{smallmatrix}\right) =: J^{(3)}$$

über $\mathbf{F}_9$ erreicht.

4.5 Unitäres Diagonalisieren

In diesem Abschnitt sei der Skalarkörper der Körper $K = \mathbf{C}$ der komplexen Zahlen.

Bemerkung. Die *komplexe Konjugation* $\mathbf{C} \longrightarrow \mathbf{C} : \zeta = \xi + i\eta \longmapsto \bar{\zeta} = \xi - i\eta$, wobei $\xi, \eta \in \mathbf{R}$, erfüllt

$$\begin{array}{rcl} \overline{\zeta + \zeta'} & = & \bar{\zeta} + \bar{\zeta}' \\ \overline{\zeta \cdot \zeta'} & = & \bar{\zeta} \cdot \bar{\zeta}' \end{array}$$

für alle $\zeta, \zeta' \in \mathbf{C}$. Wir schreiben auch $|\zeta| = \sqrt{\zeta\bar{\zeta}} = \sqrt{\xi^2 + \eta^2}$ für den *Betrag* von ζ.

Seien $m, n, r \geqslant 1$. Für $A = (a_{j,k})_{j,k} \in \mathbf{C}^{m \times n}$ sei die *konjugierte* Matrix gegeben durch

$$\bar{A} \;:=\; (\bar{a}_{j,k})_{j,k} \;\in \mathbf{C}^{m \times n} \;.$$

Dann werden

$$\begin{array}{rcl} \bar{\bar{A}} & = & A \\ \overline{\lambda A + \lambda' A'} & = & \bar{\lambda}\bar{A} + \bar{\lambda}'\bar{A}' \\ \overline{A \cdot B} & = & \bar{A} \cdot \bar{B} \end{array}$$

für $A, A' \in \mathbf{C}^{m,n}$, $B \in \mathbf{C}^{n,r}$ und $\lambda,\ \lambda' \in \mathbf{C}$. Denn für $j \in [1, m]$ und $l \in [1, r]$ ist der Eintrag von $\bar{A} \cdot \bar{B}$ an Position (j, l) gleich $\sum_{k \in [1,n]} \bar{a}_{j,k}\bar{b}_{k,l} = \overline{\sum_{k \in [1,n]} a_{j,k}b_{k,l}}$, also gleich dem Eintrag von $\overline{A \cdot B}$ an dieser Position.

4.5.1 Orthonormalisierung nach Gram-Schmidt

Sei $n \geqslant 1$. Wir betrachten den Vektorraum $\mathbf{C}^n$.

Skalarprodukt. Sei auf $\mathbf{C}^n$ das *Skalarprodukt* gegeben durch

$$\begin{array}{rcl} \mathbf{C}^n \times \mathbf{C}^n & \longrightarrow & \mathbf{C} \\ (\ x = (\xi_j)_j\ ,\ y = (\eta_j)_j\ ) & \longmapsto & \bar{x}^{\mathrm{t}} y \;=\; \sum_{j \in [1,n]} \bar{\xi}_j \eta_j \;. \end{array}$$

Ist $\bar{x}^{\mathrm{t}} y = 0$, so heißen die Vektoren x und y *orthogonal.*

Es ist $\bar{x}^{\mathrm{t}} x$ stets eine reelle Zahl $\geqslant 0$. Wir schreiben $\|x\| := \sqrt{\bar{x}^{\mathrm{t}} x}$ für die *Norm* von x. Mit $x = (\xi_j)_j$ ist ausgeschrieben also $\|x\| = \sqrt{\sum_{j \in [1,n]} |\xi_j|^2}$.

Es ist $\|x\| = 0$ genau dann, wenn $x = 0$. Falls $x \neq 0$, so schreiben wir $x^0 := \|x\|^{-1} x$ für den zugehörigen *normierten* Vektor. Es wird so $\|x^0\| = 1$.

Lemma (Cauchy-Schwarzsche Ungleichung). *Seien $x, y \in \mathbf{C}^n$. Es ist*

$$|\bar{x}^{\mathrm{t}} y| \;\leqslant\; \|x\| \cdot \|y\| \;,$$

wobei die Gleichheit genau dann gilt, wenn (x, y) linear abhängig ist.

Beweis. Wir dürfen $x \neq 0$ annehmen. Für beliebiges $\lambda \in \mathbf{C}$ wird

$$0 \;\leqslant\; \|\lambda x - y\|^2 \;=\; \bar{\lambda}\lambda \bar{x}^{\mathrm{t}} x + \bar{y}^{\mathrm{t}} y - \bar{\lambda}\bar{x}^{\mathrm{t}} y - \lambda \bar{y}^{\mathrm{t}} x \;.$$

Für $\lambda := (\bar{x}^{\mathrm{t}}y)(\bar{x}^{\mathrm{t}}x)^{-1}$ ergibt sich

$$0 \;\leqslant\; (\bar{y}^{\mathrm{t}}x)(\bar{x}^{\mathrm{t}}y)(\bar{x}^{\mathrm{t}}x)^{-1} + (\bar{y}^{\mathrm{t}}y) - (\bar{y}^{\mathrm{t}}x)(\bar{x}^{\mathrm{t}}x)^{-1}(\bar{x}^{\mathrm{t}}y) - (\bar{x}^{\mathrm{t}}y)(\bar{x}^{\mathrm{t}}x)^{-1}(\bar{y}^{\mathrm{t}}x)\;.$$

Nach Multiplikation mit $\bar{x}^{\mathrm{t}}x > 0$ erhalten wir

$$0 \;\leqslant\; (\bar{x}^{\mathrm{t}}x)(\bar{y}^{\mathrm{t}}y) - (\bar{x}^{\mathrm{t}}y)(\bar{y}^{\mathrm{t}}x)\;.$$

Gilt hierin die Gleichheit, so ist $\|\lambda x - y\|^2 = 0$, und mithin auch $\lambda x - y = 0$. Es ist (x, y) also linear abhängig.

Ist umgekehrt (x, y) linear abhängig, so gibt es wegen $x \neq 0$ ein $\mu \in \mathbf{C}$ mit $y = \mu x$, und wir erhalten

$$(\bar{x}^{\mathrm{t}}x)(\bar{y}^{\mathrm{t}}y) \;=\; |\mu|^2(\bar{x}^{\mathrm{t}}x)^2 \;=\; (\bar{y}^{\mathrm{t}}x)(\bar{x}^{\mathrm{t}}y)\;.$$

□

Orthonormalbasis. Ein Tupel $(x_1, \ldots, x_m)$ heißt *orthonormal,* falls $\|x_j\| = 1$ für $j \in [1, m]$ und $\bar{x}_j^{\mathrm{t}}x_k = 0$ für $j, k \in [1, m]$ mit $j < k$ (was wegen $\bar{y}^{\mathrm{t}}z = \overline{\bar{z}^{\mathrm{t}}y}$ für $y, z \in \mathbf{C}^n$ auch $\bar{x}_j^{\mathrm{t}}x_k = 0$ für $i, j \in [1, m]$ mit $j > k$ zur Folge hat). Ein orthonormales Tupel ist linear unabhängig. In der Tat, ist $\sum_{j\in[1,m]} \lambda_j x_j = 0$, so folgt $\lambda_k = \bar{x}_k^{\mathrm{t}}\left(\sum_{j\in[1,m]} \lambda_j x_j\right) = 0$ für alle $k \in [1, m]$. Wir sagen auch, $(x_1, \ldots, x_m)$ ist eine *Orthonormalbasis* von $\langle x_1, \ldots, x_m\rangle \leqslant \mathbf{C}^n$.

Der Beweis des folgenden Lemmas besteht aus dem Gram-Schmidtschen Orthonormalisierungsverfahren.

Lemma. *Sei $U \leqslant \mathbf{C}^n$ ein Unterraum, und sei $(x_1, \ldots, x_k)$ ein orthonormales Tupel von Vektoren in U. Dann läßt sich dieses Tupel ergänzen zu einer Orthonormalbasis $(x_1, \ldots, x_m)$ von U. Mit $k = 0$ sehen wir insbesondere, daß jeder Unterraum $U \leqslant \mathbf{C}^n$ eine Orthonormalbasis besitzt.*

Beweis. Sei ein orthonormales Tupel $(x_1, \ldots, x_k)$ in U gegeben. Mit Induktion genügt es, im Falle $\langle x_1, \ldots, x_k\rangle < U$ dieses orthonormale Tupel um einen Vektor zu einem orthonormalen Tupel $(x_1, \ldots, x_{k+1})$ zu ergänzen.

Sei $y \in U \smallsetminus \langle x_1, \ldots, x_k\rangle$. Setze

$$z \;:=\; y - \sum_{j\in[1,k]} (\bar{x}_j^{\mathrm{t}}y)x_j\;.$$

Wegen $y \notin \langle x_1, \ldots, x_k\rangle$ ist $z \neq 0$, und wir können

$$x_{k+1} \;:=\; z^0 \;=\; \left(y - \sum_{j\in[1,k]} (\bar{x}_j^{\mathrm{t}}y)x_j\right)^0$$

nehmen. Für $l \in [1, k]$ ist dann

$$\bar{x}_l^{\mathrm{t}}x_{k+1} \;=\; \|z\|^{-1}\left(\bar{x}_l^{\mathrm{t}}y - \sum_{j\in[1,k]} (\bar{x}_j^{\mathrm{t}}y)\bar{x}_l^{\mathrm{t}}x_j\right) \;=\; \|z\|^{-1}\Big(\bar{x}_l^{\mathrm{t}}y - (\bar{x}_l^{\mathrm{t}}y)\bar{x}_l^{\mathrm{t}}x_l\Big) \;=\; 0\;,$$

so daß wir mit $\|x_{k+1}\| = 1$ sehen, daß $(x_1, \ldots, x_{k+1})$ ein orthonormales Tupel ist. ▫

Beispiel. Wir wollen eine Orthonormalbasis von $U := \langle \begin{pmatrix} 2i \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ i \end{pmatrix} \rangle \leqslant \mathbf{C}^4$ bestimmen. Sei hierzu

$$x_1 \;:=\; \begin{pmatrix} 2i \\ 0 \\ 0 \\ 0 \end{pmatrix}^0 = \begin{pmatrix} i \\ 0 \\ 0 \\ 0 \end{pmatrix} .$$

Sei ferner

$$x_2 \;:=\; \left[\begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} - \left(\begin{pmatrix} -i & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} \right) \begin{pmatrix} i \\ 0 \\ 0 \\ 0 \end{pmatrix} \right]^0 \;=\; \begin{pmatrix} 0 \\ 0 \\ i \\ 0 \end{pmatrix} ,$$

und schließlich

$$x_3 \;:=\; \left[\begin{pmatrix} 0 \\ 1 \\ 2 \\ i \end{pmatrix} - \left(\begin{pmatrix} -i & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ i \end{pmatrix} \right) \begin{pmatrix} i \\ 0 \\ 0 \\ 0 \end{pmatrix} - \left(\begin{pmatrix} 0 & 0 & -i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ i \end{pmatrix} \right) \begin{pmatrix} 0 \\ 0 \\ i \\ 0 \end{pmatrix} \right]^0 \;=\; 2^{-1/2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ i \end{pmatrix} .$$

Dann ist $(x_1, x_2, x_3) = (\begin{pmatrix} i \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ i \\ 0 \end{pmatrix}, 2^{-1/2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ i \end{pmatrix})$ eine Orthonormalbasis von U.

4.5.2 Normal, unitär, hermitesch

Definition. Sei $A \in \mathbf{C}^{n \times n}$.

(i) Die Matrix A heißt *normal,* falls $\bar{A}^{\mathrm{t}} A = A \bar{A}^{\mathrm{t}}$.

(ii) Die Matrix A heißt *hermitesch,* falls $\bar{A}^{\mathrm{t}} = A$ (nach Charles Hermite).

(iii) Die Matrix A heißt *unitär,* falls $\bar{A}^{\mathrm{t}} A = E$ (und folglich $\bar{A}^{\mathrm{t}} = A^{-1}$).

Bemerkung. Eine hermitesche Matrix ist normal. Eine unitäre Matrix ist normal.

Bemerkung. Eine Matrix $A \in \mathbf{C}^{n \times n}$ ist genau dann unitär, wenn ihre Spalten ein orthonormales Tupel bilden. Denn $\bar{A}^{\mathrm{t}} A = E$ ist gleichbedeutend damit, daß $\bar{a}^{\mathrm{t}}_{*,j} a_{*,k} = 1$ für $j = k$ und $\bar{a}^{\mathrm{t}}_{*,j} a_{*,k} = 0$ für $j \neq k$, wobei $j, k \in [1, n]$.

Bemerkung. Für $A \in \mathbf{C}^{n \times n}$ sind $\bar{A}^{\mathrm{t}} A$ und $A \bar{A}^{\mathrm{t}}$ beide hermitesch. Folglich genügt es für die Überprüfung der Normalität von A, die Einträge von $\bar{A}^{\mathrm{t}} A$ mit denen von $A \bar{A}^{\mathrm{t}}$ an den Positionen (i, j) mit $i, j \in [1, n]$ und $i \leqslant j$ zu vergleichen.

Beispiel. Die Matrix $(2i) \in \mathbf{C}^{1 \times 1}$ ist normal, aber weder unitär noch hermitesch. Die Matrix $(i) \in \mathbf{C}^{1 \times 1}$ ist unitär, aber nicht hermitesch. Die Matrix $(2) \in \mathbf{C}^{1 \times 1}$ ist hermitesch, aber nicht unitär. Allgemeiner ist $A = \operatorname{diag}(d_1, \ldots, d_n)$ für beliebige $d_j \in \mathbf{C}$ normal; unitär aber nur, falls $|d_j| = 1$ für alle $j \in [1, n]$; und hermitesch nur, falls $d_j \in \mathbf{R}$ für alle $j \in [1, n]$.

Mit einer unitären Matrix U können wir *unitär konjugieren*, d.h. die Operation $\mathbf{C}^{n \times n} \longrightarrow \mathbf{C}^{n \times n}$, $A \longmapsto \bar{U}^{\mathrm{t}} A U = U^{-1} A U$ ausführen.

Lemma. *Sei $A \in \mathbf{C}^{n\times n}$. Für eine unitäre Matrix $U \in \mathbf{C}^{n\times n}$ gelten die folgenden Implikationen.*

(i) *Ist A normal, so sind es auch $\bar{A}$, A^{t} und $\bar{U}^{\mathrm{t}}AU$.*

(ii) *Ist A hermitesch, so sind es auch $\bar{A}$, A^{t} und $\bar{U}^{\mathrm{t}}AU$.*

(iii) *Ist A unitär, so auch $\bar{A}$, A^{t} und $\bar{U}^{\mathrm{t}}AU$. Allgemeiner ist das Produkt zweier unitärer Matrizen unitär. Insbesondere bilden die unitären Matrizen eine Untergruppe $\mathrm{U}_n(\mathbf{C}) \leqslant \mathrm{GL}_n(\mathbf{C})$, die* unitäre Gruppe.

Beweis. Zu (i). Ist $\bar{A}^{\mathrm{t}}A = A\bar{A}^{\mathrm{t}}$, so auch $A^{\mathrm{t}}\bar{A} = \bar{A}A^{\mathrm{t}}$, woraus wir $\bar{A}$ und A^{t} normal ersehen. Ferner ist

$$\begin{array}{rcl} \left(\overline{\bar{U}^{\mathrm{t}}AU}\right)^{\mathrm{t}}\left(\bar{U}^{\mathrm{t}}AU\right) & = & \bar{U}^{\mathrm{t}}\bar{A}^{\mathrm{t}}U\bar{U}^{\mathrm{t}}AU \\ & = & \bar{U}^{\mathrm{t}}\bar{A}^{\mathrm{t}}AU \\ & = & \bar{U}^{\mathrm{t}}A\bar{A}^{\mathrm{t}}U \\ & = & \bar{U}^{\mathrm{t}}AU\bar{U}^{\mathrm{t}}\bar{A}^{\mathrm{t}}U \\ & = & \left(\bar{U}^{\mathrm{t}}AU\right)\left(\overline{\bar{U}^{\mathrm{t}}AU}\right)^{\mathrm{t}} . \end{array}$$

Zu (ii). Ist $\bar{A}^{\mathrm{t}} = A$, so auch $A^{\mathrm{t}} = \bar{A}$, woraus wir $\bar{A}$ und A^{t} hermitesch ersehen. Ferner ist

$$\begin{array}{rcl} \left(\overline{\bar{U}^{\mathrm{t}}AU}\right)^{\mathrm{t}} & = & \bar{U}^{\mathrm{t}}\bar{A}^{\mathrm{t}}U \\ & = & \bar{U}^{\mathrm{t}}AU . \end{array}$$

Zu (iii). Ist $\bar{A}^{\mathrm{t}}A = E$, so auch $A^{\mathrm{t}}\bar{A} = E$, woraus wir $\bar{A}$ und A^{t} unitär ersehen. Damit genügt es zu zeigen, daß mit A und U auch das Produkt AU unitär ist. In der Tat wird

$$\begin{array}{rcl} \left(\overline{AU}\right)^{\mathrm{t}}(AU) & = & \bar{U}^{\mathrm{t}}\bar{A}^{\mathrm{t}}AU \\ & = & \bar{U}^{\mathrm{t}}U \\ & = & E . \end{array}$$

□

4.5.2.1 ∗ Beweis des Fundamentalsatzes der Algebra nach Derksen

Dieser Abschnitt ist nicht prüfungs- oder klausurrelevant. Wir folgen [**2**].

Fundamentalsatz der Algebra. *Der Körper $\mathbf{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

In anderen Worten, für jedes nichtkonstante normierte Polynom

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

ist ein $z \in \mathbf{C}$ mit $f(z) = 0$ als existent nachzuweisen.

Da die Matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \in \mathbf{C}^{n\times n}$$

das charakteristische Polynom $f(X)$ besitzt, genügt es zu zeigen, daß jede Matrix $A \in \mathbf{C}^{n\times n}$ einen Eigenvektor besitzt.

Aus der Analysis verwenden wir folgende zwei Lemmata, die beide mit dem Zwischenwertsatz folgen.

Lemma 1. *Für jedes Polynom $g(X) \in \mathbf{R}[X]$ mit $\deg g \equiv_2 1$ gibt es ein $x \in \mathbf{R}$ mit $g(x) = 0$.*

Lemma 2. *Für jedes $x \in \mathbf{R}_{\geqslant 0}$ gibt es ein eindeutiges $y \in \mathbf{R}_{\geqslant 0}$ mit $y^2 = x$, geschrieben $y = \sqrt{x}$.*

Nun können wir komplexe Wurzeln ziehen.

Lemma 3. *Es gibt für jedes $z \in \mathbf{C}$ ein $w \in \mathbf{C}$ mit $w^2 = z$.*

Beweis. Seien $u,\ v \in \mathbf{R}$, sei $v \geqslant 0$. Es ist

$$\begin{aligned} u + iv &= \left(\sqrt{\tfrac{u+\sqrt{u^2+v^2}}{2}} + i\sqrt{\tfrac{-u+\sqrt{u^2+v^2}}{2}}\right)^2 \\ u - iv &= \left(\sqrt{\tfrac{u+\sqrt{u^2+v^2}}{2}} - i\sqrt{\tfrac{-u+\sqrt{u^2+v^2}}{2}}\right)^2 . \end{aligned}$$

□

Sei K ein Körper, und seien $d \geqslant 1$, $r \geqslant 1$. Betrachte folgende, von K, d und r abhängende Aussage, über deren Wahrheitsgehalt zunächst nichts gesagt sei.

EV(K, d, r) Für alle ganzen Zahlen $n \geqslant 1$, die kein Vielfaches von d sind, und für alle Tupel $(A_1, \ldots, A_r)$ von Matrizen in $K^{n\times n}$ mit der Eigenschaft, daß $A_iA_j = A_jA_i$ für alle $i,\ j \in [1, n]$, gibt es einen Vektor $x \in K^n \smallsetminus \{0\}$, welcher Eigenvektor von A_i ist für alle $i \in [1, n]$.

Ein solches Tupel von Matrizen heiße auch ein *kommutierendes Tupel.* (Die Bezeichnung als A_j bedeute hier *nicht* die Matrix im linken oberen Eck von A der Größe $j \times j$.)

Lemma 4. *Die Aussage* EV$(K, d, 1)$ *impliziert die Aussage* EV(K, d, r) *für alle $r \geqslant 1$.*

Beweis. Wir führen eine Induktion nach r, nehmen für ein $r > 1$ die Aussage EV$(K, d, r-1)$ als zutreffend an, und haben EV(K, d, r) zu zeigen.

Wir führen hierzu eine weitere Induktion über das n, für welches das fragliche kommutierende Tupel aus Matrizen in $K^{n\times n}$ bestehe. D.h. wir nehmen die zu zeigende Aussage für alle Tupel von Matrizen der Größe $l \times l$ als gegeben an, solange $l \in [1, n-1]$ kein Vielfaches von d ist.

Sei $(A_1, \ldots, A_r)$ ein kommutierendes Tupel von Matrizen in $K^{n\times n}$, wobei n kein Vielfaches von d sei. Wegen EV$(K, d, 1)$ hat A_r einen Eigenwert $\lambda \in K$. Da $n = \dim \mathrm{Kern}(A_r - \lambda E) + \dim \mathrm{Im}(A_r - \lambda E)$, teilt d eine dieser beiden Dimensionen nicht.

Nun ist $A_i \,\mathrm{Kern}(A_r - \lambda E) \subseteq \mathrm{Kern}(A_r - \lambda E)$ und $A_i \,\mathrm{Im}(A_r - \lambda E) \subseteq \mathrm{Im}(A_r - \lambda E)$ für $i \in [1, r]$. Wählt man Basen dieses Kerns und dieses Bildes, so bekommt man ein kommutierendes Tupel beschreibender Matrizen $(A'_1, \ldots, A'_r)$ der auf den Kern und ein kommutierendes Tupel beschreibender Matrizen $(A''_1, \ldots, A''_r)$ der auf das Bild eingeschränkten linearen Abbildungen. Mit Induktion über n hat eines der beiden Tupel einen gemeinsamen Eigenvektor. Also hat das Tupel $(A_1, \ldots, A_r)$ selbst ebenfalls einen gemeinsamen Eigenvektor, und zwar in $\mathrm{Kern}(A_r - \lambda E)$ oder in $\mathrm{Im}(A_r - \lambda E)$. □

Lemma 5. *Es gilt* EV$(\mathbf{R}, 2, r)$ *für alle $r \geqslant 1$.*

Beweis. Mit Lemma 4 genügt es zu zeigen, daß EV$(\mathbf{R}, 2, 1)$ gilt. Sei also (A_1) ein Tupel der Länge 1, mit $A_1 \in \mathbf{R}^{n\times n}$, wobei n kein Vielfaches von 2 sei. Mit Lemma 1 hat aber $\chi_{A_1}(X)$ eine Nullstelle, und damit

A_1 einen Eigenvektor. ▫

Lemma 6. *Es gilt* $\mathrm{EV}(\mathbf{C}, 2, r)$ *für alle* $r \geqslant 1$.

Beweis. Mit Lemma 4 genügt es zu zeigen, daß $\mathrm{EV}(\mathbf{C}, 2, 1)$ gilt. Sei also (A_1) ein Tupel der Länge 1, mit $A_1 \in \mathbf{R}^{n\times n}$, wobei n kein Vielfaches von 2 sei. Wir kürzen $A := A_1$ ab und haben die Existenz eines $\mathbf{C}$-linearen Eigenvektors von A in $\mathbf{C}^n$ nachzuweisen.

Sei

$$\mathrm{Hermite}_n \;:=\; \{B \in \mathbf{C}^{n\times n} \mid B = \bar{B}^{\mathrm{t}}\} \;\subseteq\; \mathbf{C}^{n\times n}$$

die Teilmenge der hermiteschen Matrizen. Dies ist ein $\mathbf{R}$-linearer Unterraum der $\mathbf{R}$-linearen Dimension $n + 2\cdot n(n-1)/2 = n^2$, da auf der Diagonale von B beliebige Einträge in $\mathbf{R}$ und oberhalb der Diagonalen beliebige Einträge in $\mathbf{C}$ stehen dürfen, und aber damit die hermitesche Matrix B dann festliegt.

Betrachte die $\mathbf{R}$-linearen Abbildungen

$$\begin{array}{rcl} \mathrm{Hermite}_n & \xrightarrow{f} & \mathrm{Hermite}_n \\ B & \longmapsto & \frac{1}{2}(AB + B\bar{A}^{\mathrm{t}}) \end{array}$$

$$\begin{array}{rcl} \mathrm{Hermite}_n & \xrightarrow{g} & \mathrm{Hermite}_n \\ B & \longmapsto & \frac{1}{2i}(AB - B\bar{A}^{\mathrm{t}})\ . \end{array}$$

Zunächst ist zu bemerken, daß f und g in der Tat von den hermiteschen Matrizen in die hermiteschen Matrizen abbilden.

Nun sehen wir, daß $f \circ g = g \circ f$. Wählt man eine $\mathbf{R}$-lineare Basis von $\mathrm{Hermite}_n$, und schreibt man $F \in \mathbf{R}^{n^2\times n^2}$ für die diesbezüglich beschreibende Matrix von f, und $G \in \mathbf{R}^{n^2\times n^2}$ für die von g, so gilt entsprechend $FG = GF$. Da n^2 kein Vielfaches von 2 ist, gibt es einen gemeinsamen Eigenvektor von F und G, da mit Lemma 5 ja $\mathrm{EV}(\mathbf{R}, 2, 2)$ gilt. In anderen Worten, es gibt ein $B \in \mathrm{Hermite}_n \smallsetminus \{0\}$ und λ, $\mu \in \mathbf{R}$ so, daß

$$\begin{array}{rcccl} f(B) & = & \frac{1}{2}(AB + B\bar{A}^{\mathrm{t}}) & = & \lambda B \\ g(B) & = & \frac{1}{2i}(AB - B\bar{A}^{\mathrm{t}}) & = & \mu B \end{array}$$

Zusammen ist $AB = (\lambda + i\mu)B$. Jede nichtverschwindende Spalte von $B \neq 0$ ist also ein Eigenvektor von A. ▫

Lemma 7. *Es gilt* $\mathrm{EV}(\mathbf{C}, 2^k, r)$ *für alle* $r \geqslant 1$ *und für alle* $k \geqslant 1$.

Beweis. Mit Lemma 4 genügt es, $\mathrm{EV}(\mathbf{C}, 2^k, 1)$ nachzuweisen. Wir führen eine Induktion nach k, wobei Lemma 6 den Induktionsanfang $k = 1$ übernommen hat. Sei also $k > 1$ und sei $\mathrm{EV}(\mathbf{C}, 2^{k-1}, 1)$ als zutreffend angenommen. Wir wollen zeigen, daß $\mathrm{EV}(\mathbf{C}, 2^k, 1)$ gilt. Sei (A_1) ein Tupel der Länge 1 mit $A_1 \in \mathbf{C}^{n\times n}$, wobei n kein Vielfaches von 2^k sei. Wir kürzen $A := A_1$ ab und müssen zeigen, daß A einen $\mathbf{C}$-linearen Eigenvektor in $\mathbf{C}^n$ besitzt.

Ist n auch kein Vielfaches von 2^{k-1}, so folgt dies aus $\mathrm{EV}(\mathbf{C}, 2^{k-1}, 1)$, was als zutreffend angenommen wurde. Bleibt der Fall zu betrachten, daß n ein Vielfaches von 2^{k-1}, aber kein Vielfaches von 2^k ist. Insbesondere ist n nun also ein Vielfaches von 2.

Sei

$$\mathrm{Schiefsymmetrisch}_n \;:=\; \{B \in \mathbf{C}^{n\times n} \mid B = -B^{\mathrm{t}}\} \;\subseteq\; \mathbf{C}^{n\times n}\ .$$

Dies ist ein $\mathbf{C}$-linearer Unterraum der $\mathbf{C}$-linearen Dimension $n(n-1)/2$, da auf der Hauptdiagonalen einer solchen schiefsymmetrischen Matrix Nullen stehen, und die Einträge oberhalb der Hauptdiagonalen diejenigen unterhalb festlegen.

Betrachte die $\mathbf{C}$-linearen Abbildungen

$$\begin{array}{rcl} \text{Schiefsymmetrisch}_n & \xrightarrow{f} & \text{Schiefsymmetrisch}_n \\ B & \longmapsto & AB + BA^{\mathrm{t}} \end{array}$$

$$\begin{array}{rcl} \text{Schiefsymmetrisch}_n & \xrightarrow{g} & \text{Schiefsymmetrisch}_n \\ B & \longmapsto & ABA^{\mathrm{t}}\ . \end{array}$$

Zunächst ist zu bemerken, daß f und g in der Tat von den schiefsymmetrischen Matrizen in die schiefsymmetrischen Matrizen abbilden.

Nun sehen wir, daß $f \circ g = g \circ f$. Wählt man eine $\mathbf{C}$-lineare Basis von $\text{Schiefsymmetrisch}_n$, und schreibt man $F \in \mathbf{C}^{n(n-1)/2 \times n(n-1)/2}$ für die diesbezüglich beschreibende Matrix von f, und $G \in \mathbf{C}^{n(n-1)/2 \times n(n-1)/2}$ für die von g, so gilt entsprechend $FG = GF$. Da n ein Vielfaches von 2, aber kein Vielfaches von 2^k ist, ist $n(n-1)/2$ kein Vielfaches von 2^{k-1}. Es gilt $\mathrm{EV}(\mathbf{C}, 2^{k-1}, 1)$ nach Induktionsvoraussetzung, und somit $\mathrm{EV}(\mathbf{C}, 2^{k-1}, 2)$ nach Lemma 4. Daher gibt es einen gemeinsamen Eigenvektor von F und G. In anderen Worten, es gibt ein $B \in \text{Schiefsymmetrisch}_n \smallsetminus \{0\}$ und $\lambda,\ \mu \in \mathbf{C}$ so, daß

$$\begin{array}{rcccl} f(B) & = & AB + BA^{\mathrm{t}} & = & \lambda B \\ g(B) & = & ABA^{\mathrm{t}} & = & \mu B \end{array}$$

Zusammen ist $\mu B = ABA^{\mathrm{t}} = A(\lambda B - AB)$, d.h. mit $f(X) = X^2 - \lambda X + \mu$ ist $f(A)B = 0$. Mit Lemma 3 faktorisieren wir $f(X) = (X - z)(X - w)$ mit gewissen $w,\ z \in \mathbf{C}$, so daß $(A - zE)(A - wE)B = 0$.

Sei $x \in \mathbf{C}^n \smallsetminus \{0\}$ eine nichtverschwindende Spalte von B. Dann ist entweder $(A - wE)x = 0$, und x somit ein Eigenvektor von A. Oder aber, es ist $(A - wE)x \neq 0$. Dann ist aber $(A - zE)((A - wE)x) = 0$, und somit $(A - wE)x$ ein Eigenvektor von A. In beiden Fällen hat A einen Eigenvektor. □

Beweis zum Fundamentalsatz der Algebra. Für $n \geqslant 1$ und eine gegebene Matrix $A \in \mathbf{C}^{n \times n}$ suchen wir ein $k \geqslant 1$ so groß, daß 2^k das n nicht teilt. Mit Lemma 7 hat A einen Eigenvektor, und das blieb uns zu zeigen.

Bemerkung. Ebenso sieht man mit Lemma 7 und einem geeignet großen $k \geqslant 1$, daß jedes kommutierende Tupel $(A_1, \ldots, A_r)$ von Matrizen aus $\mathbf{C}^n$ einen gemeinsamen Eigenvektor hat.

4.5.3 Unitäres Diagonalisieren normaler Matrizen

Lemma von Schur (unitäre Version). *Für jede Matrix $A \in \mathbf{C}^{n \times n}$ gibt es eine unitäre Matrix $U \in \mathrm{U}_n(\mathbf{C})$ so, daß $\bar{U}^{\mathrm{t}} AU$ eine obere Dreiecksmatrix bildet. D.h. schreiben wir $\bar{U}^{\mathrm{t}} AU = (c_{j,k})_{j,k}$, so ist $c_{j,k} = 0$ für $j, k \in [1, n]$ mit $j > k$.*

Beweis. Es genügt es zu zeigen, daß wir eine unitäre Matrix $U \in \mathrm{U}_n(\mathbf{C})$ so finden können, daß mit $\bar{U}^{\mathrm{t}} AU = (c_{j,k})_{j,k}$ zumindest $c_{j,1} = 0$ ist für $j \in [2, n]$, d.h. so, daß die erste Spalte bis auf den Diagonaleintrag verschwindet. Denn dann können wir mit Induktion eine unitäre Matrix $V \in \mathrm{U}_{n-1}(\mathbf{C})$ finden, die die Matrix $(c_{j,k})_{j,k \in [2,n]}$ in obere Dreiecksform bringt. Schreiben wir $W \in \mathbf{C}^{n \times n}$ für die Blockdiagonalmatrix mit den Blöcken $E_1 = (1)$ und V, so ist auch UW unitär, und $(\overline{UW})^{\mathrm{t}} A(UW) = \bar{W}^{\mathrm{t}}(\bar{U}^{\mathrm{t}} AU)W$ ist in oberer Dreiecksform.

Wir schreiben $U = (u_{j,k})_{j,k}$ und setzen als erste Spalte $u_{*,1}$ einen normierten Eigenvektor von A ein. Sei λ sein Eigenwert. Wir ergänzen diese Spalte mit Gram-Schmidt zu einer unitären Matrix U. Nun ist die erste Spalte von $\bar{U}^{\mathrm{t}}AU$ gegeben durch

$$\bar{U}^{\mathrm{t}}Au_{*,1} \;=\; U^{-1}(\lambda u_{*,1}) \;=\; \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix} .$$

□

Definition. Eine Matrix $A \in \mathbf{C}^{n\times n}$ heißt *unitär diagonalisierbar,* wenn es eine unitäre Matrix $U \in \mathbf{C}^{n\times n}$ so gibt, daß $\bar{U}^{\mathrm{t}}AU \;\; (= U^{-1}AU)$ eine Diagonalmatrix ist.

Vorsicht. Wir werden unten sehen, daß unitäre Matrizen unitär diagonalisierbar sind. Umgekehrt gibt es aber unitär diagonalisierbare Matrizen, die nicht unitär sind, wie etwa $(2) \in \mathbf{C}^{1\times 1}$. Das Adverb 'unitär' in 'unitär diagonalisierbare Matrix' bezieht sich auf die besondere Form der Diagonalisierbarkeit, nicht auf die Matrix.

Satz 15 *Sei $A \in \mathbf{C}^{n\times n}$.*

(i) *Die Matrix A ist normal genau dann, wenn sie unitär diagonalisierbar ist.*

(ii) *Die Matrix A ist hermitesch genau dann, wenn sie so unitär diagonalisierbar ist, daß die resultierende Diagonalmatrix reelle Diagonaleinträge besitzt. Insbesondere sind die Eigenwerte von A dann reell.*

(iii) *Die Matrix A ist unitär genau dann, wenn sie so unitär diagonalisierbar ist, daß die resultierende Diagonalmatrix Diagonaleinträge von Betrag 1 besitzt. Insbesondere sind die Eigenwerte von A dann von Betrag 1.*

Beweis. Zu (i). Finden wir U unitär so, daß $\bar{U}^{\mathrm{t}}AU =: D$ eine Diagonalmatrix ist, so ist D normal, und damit auch $A = UD\bar{U}^{\mathrm{t}}$.

Sei umgekehrt A normal. Mit dem Lemma von Schur in unitärer Version finden wir eine unitäre Matrix U so, daß $\bar{U}^{\mathrm{t}}AU$ eine obere Dreiecksmatrix ist. Da mit A auch $\bar{U}^{\mathrm{t}}AU$ normal ist, genügt es zu zeigen, daß eine normale obere Dreiecksmatrix $C = (c_{j,k})_{j,k}$ bereits eine Diagonalmatrix ist. Die Normalität $\bar{C}^{\mathrm{t}}C = C\bar{C}^{\mathrm{t}}$ liefert nun an Position $(1,1)$

$$|c_{1,1}|^2 \;=\; \sum_{k\in[1,n]} |c_{1,k}|^2 \,,$$

und somit $c_{1,k} = 0$ für $k \in [2,n]$.

An Position $(2,2)$ erhalten wir nun

$$|c_{2,2}|^2 \;=\; \sum_{k\in[2,n]} |c_{2,k}|^2 \,,$$

und somit $c_{2,k} = 0$ für $k \in [3,n]$.

So bis Position $(n-1,n-1)$ fortfahrend, erhalten wir $c_{j,k} = 0$ für $j,k \in [1,n]$ mit $j < k$. □

Zu (ii). Finden wir U unitär so, daß $\bar{U}^{\mathrm{t}} A U =: D$ eine Diagonalmatrix mit reellen Einträgen ist, so ist D hermitesch, und damit auch $A = U D \bar{U}^{\mathrm{t}}$.

Sei umgekehrt A hermitesch. Mit (i) finden wir eine unitäre Matrix U mit $\bar{U}^{\mathrm{t}} A U =: D$ Diagonalmatrix. Mit A hermitesch ist auch D hermitesch und hat folglich reelle Diagonaleinträge.

Zu (iii). Finden wir U unitär so, daß $\bar{U}^{\mathrm{t}} A U =: D$ eine Diagonalmatrix mit Einträgen von Betrag 1 ist, so ist D unitär, und damit auch $A = U D \bar{U}^{\mathrm{t}}$.

Sei umgekehrt A unitär. Mit (i) finden wir eine unitäre Matrix U mit $\bar{U}^{\mathrm{t}} A U =: D$ Diagonalmatrix. Mit A unitär ist auch D unitär und hat folglich Diagonaleinträge von Betrag 1.

Bemerkung. Wir haben also folgende Implikationen für eine Matrix $A \in \mathbf{C}^{n\times n}$.

$$
\begin{tikzcd}
\text{unitär} \arrow[dr, Rightarrow] & & & \\
& \text{normal} \arrow[r, Leftrightarrow] & \text{unitär diagonalisierbar} \arrow[r, Rightarrow] & \text{diagonalisierbar} \\
\text{hermitesch} \arrow[ur, Rightarrow] & & &
\end{tikzcd}
$$

Es gelten keine weiteren Implikationen. Zum Beispiel ist $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ wegen der Eigenwerte 0 und 1 mit jeweils algebraischer und daher auch geometrischer Vielfachheit 1 diagonalisierbar, aber als nichtdiagonale obere Dreiecksmatrix mit obigem Argument nicht normal, also auch nicht unitär diagonalisierbar.

Frage. Mit Schurs Lemma, unitäre Version, wissen wir, daß es Repräsentanten unitärer Konjugationsklassen in oberer Dreiecksgestalt gibt. Kann man ein Repräsentantensystem auflisten? Für die Teilmenge der normalen Matrizen wird dies durch Satz 15 geleistet.

Bemerkung. Sei $A \in \mathbf{C}^{n\times n}$ normal, sei x ein Eigenvektor von A zum Eigenwert λ, und sei y ein Eigenvektor von A zum Eigenwert μ, und sei $\lambda \neq \mu$. Mit Satz 15 finden wir unter geeigneter Anordnung ihrer Spalten eine unitäre Matrix U so, daß

$$\bar{U}^{\mathrm{t}} A U = \operatorname{diag}(\underbrace{\lambda, \ldots, \lambda}_{s \text{ Einträge}}, \underbrace{\mu, \ldots, \mu}_{t \text{ Einträge}}, \ldots) \;=:\; D$$

ist, wobei s die algebraische Vielfachheit von λ, und t die algebraische Vielfachheit von μ bezeichne. Dann ist

$$\begin{array}{rcl} E_A(\lambda) & = & \langle u_{*,1}, \ldots, u_{*,s} \rangle \\ E_A(\mu) & = & \langle u_{*,s+1}, \ldots, u_{*,s+t} \rangle \,, \end{array}$$

da diese Vektoren je ein linear unabhängiges Tupel von Eigenvektoren zum jeweiligen Eigenwert bilden, wie man U regulär und $AU = UD$ entnimmt. Wegen $x \in E_A(\lambda)$ und $y \in E_A(\mu)$ können wir nun also

$$\begin{array}{rcl} x & = & \sum_{j\in[1,s]} \xi_j u_{*,j} \\ y & = & \sum_{k\in[1,t]} \eta_k u_{*,s+k} \end{array}$$

schreiben für gewisse $\xi_j \in \mathbf{C}$ und gewisse $\eta_k \in \mathbf{C}$. Mithin wird

$$\begin{array}{rcl} \bar{x}^{\mathrm{t}} y & = & \overline{\left(\sum_{j\in[1,s]} \xi_j u_{*,j}\right)}^{\mathrm{t}} \left(\sum_{k\in[1,t]} \eta_k u_{*,s+k}\right) \\ & = & \sum_{j\in[1,s]} \sum_{k\in[1,t]} \bar{\xi}_j \eta_k \bar{u}^{\mathrm{t}}_{*,j} u_{*,s+k} \\ & = & 0\,, \end{array}$$

letzteres, da verschiedene Spalten von U orthogonal zueinander sind. Kurz, Eigenvektoren von A zu verschiedenen Eigenwerten sind orthogonal zueinander.

Wegen $\mathbf{C}^n = \bigoplus_{i\in[1,k]} E_A(\lambda_i)$, wobei λ_i die Eigenwerte von A durchläuft, ist die Aneinandersetzung von Basistupeln der Eigenräume eine Basis von $\mathbf{C}^n$. Wählen wir nun als Basistupel der Eigenräume unter Zuhilfenahme von Gram-Schmidt orthonormale Tupel, so setzen diese sich mit der eben gezeigten Orthogonalität zu einer Orthonormalbasis von $\mathbf{C}^n$ zusammen. Die aus diesen Spaltenvektoren bestehende unitäre Matrix U diagonalisiert die Matrix A. Auf diese Weise kann für die unitäre Diagonalisierung normaler Matrizen die Anwendung des für das Schursche Lemma in unitärer Version angeführten Verfahrens umgangen werden.

Verfahren. Eine gegebene normale Matrix $A \in \mathbf{C}^{n\times n}$ kann in den folgenden Schritten unitär diagonalisiert werden.

(1) Berechne und zerlege das charakteristische Polynom $\chi_A(X) = \det(XE - A) = \prod_{i\in[1,k]}(X - \lambda_i)^{m_i}$, wobei $\lambda_i \neq \lambda_j$ für $i \neq j$.

$\forall\, i$ {

(2) Berechne eine Basis von $E_A(\lambda_i) = \mathrm{Kern}(A - \lambda_i E)$.

(3) Verwende das Verfahren von Gram-Schmidt, um aus der in (2) konstruierten Basis eine Orthonormalbasis von $E_A(\lambda_i)$ zu erhalten.

}

(4) Setze die in (3) gefundenen Basistupel für $i \in [1,k]$ nebeneinander zu einer Orthonormalbasis von $\mathbf{C}^n$ und beschreibe $x \longmapsto Ax$ in dieser Basis.

Bemerkung. Eine reellwertige hermitesche Matrix $A \in \mathbf{R}^{n\times n} \subseteq \mathbf{C}^{n\times n}$ heißt auch *symmetrisch.* Das in der vorigen Bemerkung beschriebene Verfahren kann für A dann mit Vektoren in $\mathbf{R}^n$ durchgeführt werden. Wir erhalten eine reellwertige unitäre Matrix $U \in \mathbf{R}^{n\times n} \cap \mathrm{U}_n(\mathbf{C})$, eine sogenannte *orthogonale* Matrix, die A diagonalisiert.

4.5.4 Definitheit

Sei $A \in \mathbf{C}^{n\times n}$ eine hermitesche Matrix.

4.5.4.1 Begriff

Definition. Sei die zu A gehörige *quadratische Form* gegeben durch

$$\begin{array}{rcl} \mathbf{C}^n & \xrightarrow{q_A} & \mathbf{R} \\ x & \longmapsto & q_A(x) \; := \; \bar{x}^{\mathrm{t}} A x \; . \end{array}$$

Es ist wegen $\overline{\bar{x}^{\mathrm{t}} A x} = x^{\mathrm{t}} \bar{A} \bar{x} \overset{\text{transponiere in } \mathbf{C}^{1\times 1}}{=} \bar{x}^{\mathrm{t}} \bar{A}^{\mathrm{t}} x = \bar{x}^{\mathrm{t}} A x$ in der Tat $\bar{x}^{\mathrm{t}} A x \in \mathbf{R}$.

Es ist $q_A(0) = 0$. Die Matrix A heißt nun

- *positiv definit,* falls $q_A(x) > 0$ für alle $x \in \mathbf{C}^n \smallsetminus \{0\}$,
- *positiv semidefinit,* falls $q_A(x) \geqslant 0$ für alle $x \in \mathbf{C}^n \smallsetminus \{0\}$,
- *negativ definit,* falls $q_A(x) < 0$ für alle $x \in \mathbf{C}^n \smallsetminus \{0\}$,
- *negativ semidefinit,* falls $q_A(x) \leqslant 0$ für alle $x \in \mathbf{C}^n \smallsetminus \{0\}$.
- *indefinit,* falls es $x, y \in \mathbf{C}^n \smallsetminus \{0\}$ gibt mit $q_A(x) > 0$ und $q_A(y) < 0$.

Wegen $q_{(-A)}(x) = -q_A(x)$ ist A negativ (semi)definit genau dann, wenn $-A$ positiv (semi)definit ist.

Beispiel. Die Matrix $A = \left(\begin{smallmatrix} 2 & 5 \\ 5 & -1 \end{smallmatrix}\right)$ ist wegen $q_A(e_1) = 2 > 0$ und $q_A(e_2) = -1 < 0$ indefinit.

Bemerkung. Eine Diagonalmatrix $D = \operatorname{diag}(d_1, \ldots, d_n)$ mit reellen Diagonaleinträgen d_j bekommt die quadratische Form

$$q_D((\xi_j)_j) \;=\; d_1|\xi_1|^2 + \cdots + d_n|\xi_n|^2$$

zugeordnet. Also ist D positiv definit genau dann, wenn stets $d_j > 0$; positiv semidefinit genau dann, wenn stets $d_j \geqslant 0$; negativ definit genau dann, wenn stets $d_j < 0$; negativ semidefinit genau dann, wenn stets $d_j \leqslant 0$. Sie ist indefinit, wenn es ein j mit $d_j > 0$ und ein k mit $d_k < 0$ gibt.

Damit ist z.B. $\left(\begin{smallmatrix} 0 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ negativ semidefinit, aber nicht negativ definit.

4.5.4.2 Eigenwertkriterium

Lemma. *Die hermitesche Matrix* $A \in \mathbf{C}^{n\times n}$ *ist*

- *positiv definit genau dann, wenn alle ihre Eigenwerte* > 0 *sind,*
- *positiv semidefinit genau dann, wenn alle ihre Eigenwerte* $\geqslant 0$ *sind,*
- *negativ definit genau dann, wenn alle ihre Eigenwerte* < 0 *sind,*

- *negativ semidefinit genau dann, wenn alle ihre Eigenwerte* $\leqslant 0$ *sind,*
- *indefinit genau dann, wenn sie wenigstens einen positiven und wenigsten einen negativen Eigenwert hat.*

Beweis. Es genügt, die Aussagen über die positive Definitheit (bzw. Semidefinitheit) zu zeigen. Ist $U \in \mathrm{U}_n(\mathbf{C})$ eine unitäre Matrix, so behaupten wir, daß A genau dann positiv definit (bzw. semidefinit) ist, wenn dies für $\bar{U}^{\mathrm{t}}AU$ zutrifft. Da mit U auch $U^{-1} = \bar{U}^{\mathrm{t}}$ unitär ist, genügt es, die direkte Implikation zu zeigen.

Sei A positiv definit (bzw. semidefinit). Sei $x \in \mathbf{C}^n \smallsetminus \{0\}$. Da auch $Ux \neq 0$, ist $\bar{x}^{\mathrm{t}}\bar{U}^{\mathrm{t}}AUx = (\overline{Ux})^{\mathrm{t}}A(Ux) > 0$ (bzw. $\geqslant 0$). Dies zeigt die Behauptung.

Damit dürfen wir mit unitärer Diagonalisierung annehmen, daß A eine Diagonalmatrix mit reellen Diagonaleinträgen, namentlich ihren Eigenwerten, ist. Eine solche Diagonalmatrix ist positiv definit (bzw. semidefinit) genau dann, wenn alle ihre Diagonaleinträge > 0 (bzw. $\geqslant 0$) sind. ▫

Folgerung. *Schreibe* $\chi_A(X) = X^n + h_{n-1}X^{n-1} + h_{n-2}X^{n-2} + \cdots + h_0X^0 \in \mathbf{R}[X]$. *Es ist* A

- *positiv definit genau dann, wenn* $(-1)^{n-j}h_j > 0$ *für alle* $j \in [0, n-1]$.

  D.h. A *ist positiv definit genau dann, wenn die Vorzeichen der Koeffizienten alternieren, angefangen mit einem negativen Vorzeichen von* h_{n-1}.
- *positiv semidefinit genau dann, wenn* $(-1)^{n-j}h_j \geqslant 0$ *für alle* $j \in [0, n-1]$
- *negativ definit genau dann, wenn* $h_j > 0$ *für alle* $j \in [0, n-1]$.
- *negativ semidefinit genau dann, wenn* $h_j \geqslant 0$ *für alle* $j \in [0, n-1]$.
- *indefinit, falls sie nicht positiv semidefinit und nicht negativ semidefinit ist.*

Beweis. Beachte zunächst, daß das charakteristische Polynom einer hermiteschen Matrix in der Tat in $\mathbf{R}[X]$ liegt, da es nur reelle Nullstellen hat und sich daher in ein Produkt von Linearfaktoren in $\mathbf{R}[X]$ zerlegen läßt.

Sei $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0X^0 \in \mathbf{R}[X]$ ein normiertes Polynom.

Sind alle Nullstellen von f kleiner (oder gleich) 0, so zeigt die Darstellung von f als Produkt von Linearfaktoren, daß $a_j > 0$ ($\geqslant 0$) für $j \in [0, n-1]$.

Ist umgekehrt $a_j > 0$ ($\geqslant 0$) für $j \in [0, n-1]$, so ist $f(\lambda) > 0$ für alle $\lambda \geqslant 0$ (> 0), so daß die Nullstellen von f alle kleiner (oder gleich) Null sind.

Mit vorstehendem Lemma zeigt dies die Aussagen über die negative (Semi-)Definitheit.

Verwendet man, daß A positiv (semi)definit ist genau dann, wenn $(-A)$ negativ (semi-)definit ist, sowie, daß $\chi_{-A}(X) = \det(XE + A) = (-1)^n \det((-X)E - A) = (-1)^n \chi_A(-X)$, so folgen die Aussagen über die positive (Semi-)Definitheit. ▫

Folgerung. Ist A positiv definit, so ist $\det A$ reell und positiv als Produkt der Eigenwerte (genommen mit algebraischen Vielfachheiten).

4.5.4.3 Hauptminorenkriterium

Schreibe $A = (a_{j,k})_{j,k\in[1,n]}$. Bezeichne für $l \in [1,n]$ mit $A_l := (a_{j,k})_{j,k\in[1,l]}$ die quadratische $l \times l$-Teilmatrix im linken oberen Eck von A. Die Determinanten $\det A_l$ heißen *Hauptminoren* von A. Aus A hermitesch folgt A_l hermitesch für alle $l \in [1,n]$.

Lemma. *Die hermitesche Matrix* $A \in \mathbf{C}^{n\times n}$ *ist positiv definit genau dann, wenn* A_l *positiv definit ist für alle* $l \in [1,n]$.

Beweis. Sind alle A_l positiv definit, so insbesondere auch $A_n = A$.

Umgekehrt, sei $l \in [1,n]$ und sei $x = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_l \end{pmatrix} \in \mathbf{C}^l \smallsetminus \{0\}$. Wir schreiben $x' := \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_l \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbf{C}^n \smallsetminus \{0\}$ für den mit Nulleinträgen ergänzten Vektor. Dann ist $q_{A_l}(x) = q_A(x') > 0$. Dies zeigt, daß A_l positiv definit ist. □

Satz 16 (Hauptminorenkriterium) *Eine hermitesche Matrix* $A \in \mathbf{C}^{n\times n}$ *ist*

- *positiv definit genau dann, wenn alle Hauptminoren* $\det A_l$ *positiv sind,* $l \in [1,n]$*;*
- *negativ definit genau dann, wenn* $(-1)^l \det A_l$ *positiv ist für alle* $l \in [1,n]$*; d.h. wenn die Hauptminoren alternieren, angefangen mit* $\det A_1 < 0$.

Beweis. Da A negativ definit genau dann ist, wenn $-A$ positiv definit ist, genügt es, die Aussage für die positive Definitheit zu zeigen.

Ist A positiv definit, so trifft dies mit vorigem Lemma auch für jedes A_l mit $l \in [1,n]$ zu. Es folgt, daß die Hauptminoren alle positiv sind.

Seien nun umgekehrt die Hauptminoren von A alle positiv. Wir wollen per Induktion zeigen, daß A_l positiv definit ist für alle $l \in [1,n]$.

Für den Induktionsanfang bemerken wir, daß der Eintrag von A_1 positiv ist, und daß somit A_1 positiv definit ist.

Sei nun für $l \in [1,n-1]$ die Matrix A_l als positiv definit bekannt. Wir wollen A_{l+1} als positiv definit nachweisen. Dazu diagonalisieren wir die hermitesche Matrix A_{l+1} unitär zu einer Diagonalmatrix

$$D \;=\; \operatorname{diag}(d_1,\ldots,d_{l+1}) \;:=\; \bar{U}^{\mathrm{t}} A_{l+1} U \in \mathbf{C}^{(l+1)\times(l+1)}\;,$$

wobei $U \in \mathrm{U}_{l+1}(\mathbf{C})$. Sei

$$V_{>0} \;:=\; \{\bar{U}^{\mathrm{t}}x \mid x = (\xi_i)_i \in \mathbf{C}^{l+1} \text{ mit } \xi_{l+1} = 0\} \;.$$

Es ist $\dim V_{>0} = l$, und es ist $q_D(y) = \bar{y}^{\mathrm{t}}\bar{U}^{\mathrm{t}}A_{l+1}Uy = (\overline{Uy})^{\mathrm{t}}A_{l+1}(Uy) > 0$ für $y \in V_{>0} \smallsetminus \{0\}$.

Hätte D nun wenigstens zwei Diagonaleinträge $\leqslant 0$, sagen wir, $d_j \leqslant 0$ und $d_k \leqslant 0$ mit $j \neq k$, so gäbe es auch den zweidimensionalen Teilraum $V_{\leqslant 0} := \langle e_j, e_k \rangle$, für den $q_D(y) \leqslant 0$ wäre für $y \in V_{\leqslant 0} \smallsetminus \{0\}$. Die Dimensionsformel aus Satz 4 lieferte dann $V_{>0} \cap V_{\leqslant 0} \neq 0$, was nicht möglich ist. Also hat D höchstens einen Diagonaleintrag $\leqslant 0$.

Da nun aber das Produkt der Diagonaleinträge $\det A_{l+1} = \det D$ positiv ist, sind vollends alle Diagonaleinträge von D positiv. Deswegen ist D positiv definit, und damit auch A_{l+1}. □

Vorsicht. Für positive Semidefinitheit gibt es kein Hauptminorenkriterium. So z.B. sind die Hauptminoren von $\left(\begin{smallmatrix} 0 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ beide $\geqslant 0$, wohingegen die Matrix nicht positiv semidefinit ist.

Bemerkung. Eine hermitesche Matrix, die positiv semidefinit, aber nicht positiv definit ist, hat nach dem Eigenwertkriterium einen Eigenwert 0, ist also singulär. Genauso hat eine hermitesche Matrix, die negativ semidefinit, aber nicht negativ definit ist, einen Eigenwert 0. Somit ist eine Matrix, die weder das Hauptminorenkriterium für positive Definitheit noch das Hauptminorenkriterium für negative Definitheit erfüllt, die aber *Determinante ungleich* 0 *hat,* auch nicht positiv oder negativ semidefinit, d.h. sie ist indefinit.

Aber Vorsicht, eine indefinite hermitesche Matrix kann durchaus Determinante 0 haben, wie z.B. $\left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right)$.

4.5.4.4 Sylvesterscher Trägheitssatz

Für eine hermitesche Matrix $A \in \mathbf{C}^{n\times n}$ sei

$$\begin{array}{rcl} \operatorname{pos}(A) & := & \sum_{\lambda \text{ Eigenwert von } A,\ \lambda > 0} \dim E_A(\lambda) \\ \operatorname{neg}(A) & := & \sum_{\lambda \text{ Eigenwert von } A,\ \lambda < 0} \dim E_A(\lambda) \end{array}$$

In anderen Worten, $\operatorname{pos}(A)$ ist die Anzahl der positiven Eigenwerte von A, und $\operatorname{neg}(A)$ die Anzahl der negativen Eigenwerte, gezählt mit jeweiliger algebraischer Vielfachhheit.

Das Tupel $(\operatorname{pos}(A), \operatorname{neg}(A))$ wird auch als *Signatur* von A bezeichnet.

Es ist A positiv definit genau dann, wenn $\operatorname{pos}(A) = n$; positiv semidefinit genau dann, wenn $\operatorname{neg}(A) = 0$; negativ definit genau dann, wenn $\operatorname{neg}(A) = n$; negativ semidefinit genau dann, wenn $\operatorname{pos}(A) = 0$; indefinit genau dann, wenn $\operatorname{neg}(A) \neq 0$ und $\operatorname{pos}(A) \neq 0$. Dies zeigt, daß zur Entscheidung der Definitheit einer Matrix auch die Signatur herangezogen werden kann.

Satz 17 (Sylvesterscher Trägheitssatz) *Ist $S \in \mathrm{GL}_n(\mathbf{C})$, so ist*

$$(\operatorname{pos}(A), \operatorname{neg}(A)) \;=\; (\operatorname{pos}(\bar{S}^{\mathrm{t}}AS), \operatorname{neg}(\bar{S}^{\mathrm{t}}AS)) \;.$$

Beweis. Setze

$$\begin{aligned} \mathrm{Pos}(A) &:= \textstyle\bigoplus_{\lambda \text{ Eigenwert von } A,\ \lambda > 0} E_A(\lambda) \\ \mathrm{Neg}(A) &:= \textstyle\bigoplus_{\lambda \text{ Eigenwert von } A,\ \lambda > 0} E_A(\lambda)\ . \end{aligned}$$

Dann ist $\mathrm{pos}(A) = \dim \mathrm{Pos}(A)$ und $\mathrm{neg}(A) = \dim \mathrm{Neg}(A)$. Beachte, daß

$$\mathbf{C}^n \;=\; \mathrm{Pos}(A) \oplus \mathrm{Kern}(A) \oplus \mathrm{Neg}(A)\ .$$

Es ist ferner $q_A(x) > 0$ für $x \in \mathrm{Pos}(A) \smallsetminus \{0\}$ wegen der Orthogonalität der Eigenräume, deren direkte Summe $\mathrm{Pos}(A)$ ergibt.

Wir schreiben $B := \bar{S}^{\mathrm{t}} A S$. Zu zeigen genügt $\mathrm{pos}(A) = \mathrm{pos}(B)$. Da umgekehrt auch $A = \overline{(S^{-1})}^{\mathrm{t}} B (S^{-1})$ ist, genügt es hierfür zu zeigen, daß $\mathrm{pos}(A) \leqslant \mathrm{pos}(B)$.

Wir behaupten, daß

$$S^{-1}\mathrm{Pos}(A) \cap \big(\mathrm{Kern}(B) \oplus \mathrm{Neg}(B)\big) \;=\; 0\ .$$

Sei ein $x \neq 0$ in diesem Schnitt als existent angenommen. Dann ist $q_A(Sx) > 0$ und zugleich $q_A(Sx) = q_{\bar{S}^{\mathrm{t}} A S}(x) = q_B(x) \leqslant 0$. Widerspruch.

Damit ist auch

$$S^{-1}\mathrm{Pos}(A) \oplus \mathrm{Kern}(B) \oplus \mathrm{Neg}(B)$$

eine direkte Summe. Für die Dimensionen gilt also

$$\begin{aligned} \dim S^{-1}\mathrm{Pos}(A) + \dim \mathrm{Kern}(B) + \dim \mathrm{Neg}(B) &\leqslant n \\ \dim \mathrm{Pos}(B) + \dim \mathrm{Kern}(B) + \dim \mathrm{Neg}(B) &= n\ , \end{aligned}$$

und folglich

$$\mathrm{pos}(A) \;=\; \dim \mathrm{Pos}(A) \;=\; \dim S^{-1}\mathrm{Pos}(A) \;\leqslant\; \dim \mathrm{Pos}(B) \;=\; \mathrm{pos}(B)\ .$$

> **Frage.** Kann man in der Situation von Satz 17 einen Isomorphismus $\mathrm{Pos}(A) \xrightarrow{\sim} \mathrm{Pos}(\bar{S}^{\mathrm{t}} A S)$ angeben?

Beidseitiges Gaußverfahren. Zur Berechnung der Signatur von A genügt es also, eine invertierbare Matrix S derart zu finden, daß $\bar{S}^{\mathrm{t}} A S$ Diagonalgestalt hat; notwendigerweise, da wiederum hermitesch, mit reellen Diagonaleinträgen. Die Anzahl der positiven Diagonaleinträge ist dann $\mathrm{pos}(\bar{S}^{\mathrm{t}} A S) = \mathrm{pos}(A)$, die Anzahl der negativen Diagonaleinträge gleich $\mathrm{neg}(\bar{S}^{\mathrm{t}} A S) = \mathrm{neg}(A)$. Vorsicht, die Diagonaleinträge von $\bar{S}^{\mathrm{t}} A S$ sind in aller Regel *nicht* die Eigenwerte von A.

Wir können also wie folgt vorgehen, um die Signatur einer hermiteschen Matrix $A \in \mathbf{C}^{n\times n}$ zu bestimmen. Zunächst formen wir A folgendermaßen um zu einer Matrix der Gestalt $\left(\begin{smallmatrix} b & 0 \\ 0 & B \end{smallmatrix}\right)$, mit $b \in \mathbf{C}$ und $B \in \mathbf{C}^{(n-1)\times(n-1)}$.

(1) Ist der Eintrag an Position $(j, 1)$ gleich Null für $j \in [2, n]$, so sind wir fertig.

(2) Ist der Eintrag an Position $(1, 1)$ ungleich Null, so gehe zu (4).

(3) Bestimme ein $j \in [2, n]$ mit einem Eintrag an Position $(j, 1)$ ungleich Null. Bestimme ein $\lambda \in \mathbf{R} \setminus \{0\}$ so, daß das Doppelte dieses Eintrags ungleich dem $(-\lambda)$-fachen des Eintrags an Position (j, j) ist. Addiere nun das λ-fache der j-ten Zeile zur ersten Zeile, und das λ-fache der j-ten Spalte zur ersten Spalte.

(4) Addiere für $j \in [2, n]$ ein Vielfaches der ersten Zeile auf die j-te Zeile so, daß der Eintrag an Position $(j, 1)$ annulliert wird.

(5) Ersetze den Eintrag an der Position $(1, j)$ durch 0 für $j \in [2, n]$.

Da diese Prozedur einer Multiplikation mit einer invertierbaren Matrix S von links, gefolgt mit der Multiplikation mit $\bar{S}^{\mathrm{t}}$ von rechts gleichkommt, ist das Resultat eine hermitesche Matrix. Insbesondere ist auch der Block B eine hermitesche Matrix. Somit kann man die Prozedur erneut für B durchführen, usf. Die schließlich resultierende Diagonalmatrix hat nach Satz 17 dieselbe Signatur wie A.

4.5.4.5 Beispiel.

Wir betrachten alle Kriterien an einem Beispiel. In der Praxis genügt es hingegen, sich ein geeignetes Kriterium zu wählen.

Sei $A = \begin{pmatrix} 2 & 2 & 2 & 0 \\ 2 & 3 & 2 & i \\ 2 & 2 & 3 & 0 \\ 0 & -i & 0 & 1 \end{pmatrix} \in \mathbf{C}^{4\times 4}$. Mit Betrachtung der Hauptdiagonaleinträge kann man von vorneherein ausschließen, daß A negativ semidefinit ist.

Die Hauptminoren ergeben sich zu $\det \left(2 \right) = 2 > 0$, $\det \begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix} = 2 > 0$, $\det \begin{pmatrix} 2 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix} = 2 > 0$ und $\det A = 0$. Somit wissen wir, daß A nicht positiv definit ist. Über die positive Semidefinitheit wissen wir an dieser Stelle noch nichts.

Das charakterisische Polynom ergibt sich zu $\chi_A(X) = X^4 - 9X^3 + 16X^2 - 6X$. Den Koeffizienten entnehmen wir, daß A positiv semidefinit ist. Da der Eigenwert 0 die algebraische Vielfachheit 1 hat, können wir darauf schließen, daß A die Signatur $(3, 0)$ hat. Dieser Schluß wäre für eine indefinite Matrix an dieser Stelle noch nicht möglich. Die Berechnung der Eigenwerte von A wäre schwierig.

Das beidseitige Gaußverfahren liefert

$$\begin{pmatrix} 2 & 2 & 2 & 0 \\ 2 & 3 & 2 & i \\ 2 & 2 & 3 & 0 \\ 0 & -i & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & 0 \\ 0 & -i & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Wiederum erhalten wir die Signatur $(3, 0)$.

Literaturverzeichnis

[1] Baur, G., *Lineare Algebra (für Informatiker),* Vorlesungsmanuskript, Ulm, 2002.

[2] Derksen, H., *The Fundamental Theorem of Algebra and Linear Algebra,* Am. Math. Monthly 110, 2003.

[3] Ebbinghaus, H.-D. et al., *Zahlen,* Grundwissen Mathematik, Springer, 1983.

[4] Fischer, G., *Lineare Algebra,* 10. Aufl., Vieweg, 1995.

[5] Koecher, M., *Lineare Algebra und Analytische Geometrie,* 2. Aufl., Grundwissen Mathematik, Springer, 1985.

[6] Kowalsky, H. J.; Michler, G. O., *Lineare Algebra,* 11. Aufl., de Gruyter, 1998.

[7] Kostrikin, A. I.; Manin, Yu. I., *Linear Algebra and Geometry,* Gordon and Breach, 1989.

[8] Lang, S., *Linear Algebra,* 3. Aufl., Addison-Wesley, 1972.

[9] Lorenz, F., *Einführung in die Algebra, Teil I,* BI Wissenschaftsverlag, 1992.

[10] Lorenz, F., *Lineare Algebra II,* BI Wissenschaftsverlag, 1992.

[11] Lütkebohmert, W., *Lineare Algebra,* Vorlesungsmanuskript, Ulm, 2002.

[12] Mansfield, L., *Linear Algebra,* Dekker, 1976.

[13] Meyberg, K; Vachenauer, P, *Höhere Mathematik 2,* 3. Auflage, Springer, 1999.