Ralf Gerkmann

Mathematisches Institut der
Ludwig-Maximilians-Universität München

Wintersemester 2024-25 / Sommersemester 2025 / Wintersemester 2025-26

Lineare Algebra

Inhaltsverzeichnis

§ 1. *Aussagenlogik*

Inhaltsübersicht

Unter einer ***Aussage*** verstehen wir einen (sprachlich oder in mathematischer Notation formulierten) Satz, von dem auf sinnvolle und objektive Weise gesagt werden kann, dass er ***wahr*** oder ***falsch*** ist. Mit Hilfe von logischen Symbolen $\neg, \wedge, \Rightarrow$ usw. lassen sich einfache Aussagen zu komplexeren Aussagen zusammensetzen. Die ***Tautologien*** bilden eine besonders wichtige Klasse zusammengesetzter Aussagen, weil sie für logische Schlüsse verwendet werden können. Aus solchen Schlüssen wiederum werden mathematische ***Beweise*** aufgebaut.

Wichtige Begriffe und Sätze

- Aussagen und ihre Wahrheitswerte (wahr oder falsch)
- Aussagenschema, Parameter
- Verknüpfung von Aussagen (Konjunktion, Disjunktion, Negation, Implikation, Äquivalenz)
- Tautologien und logische Schlüsse

(1.1) Definition Unter einer ***Aussage*** verstehen wir einen (sprachlich oder in mathematischer Notation formulierten) Satz, von dem auf sinnvolle und objektive Weise gesagt werden kann, dass er ***wahr*** oder ***falsch*** ist.

Die folgenden Sätze sind zweifellos Aussagen.

(i) Heute ist Dienstag. (*wahr*, jedenfalls am 15.10.2024)

(ii) $1 + 1 = 2$ *(wahr)*

(iii) Es gibt eine natürliche Zahl, die größer ist als alle anderen natürlichen Zahlen.
(*Falsch*. Nehmen wir an, n wäre eine solche Zahl. Dann müsste $n > n + 1$ gelten.
Wir wissen aber, dass $n < n + 1$ gilt.)

(iv) Die Summe der Innenwinkel eines beliebigen Dreiecks beträgt 180°.
(*wahr*, zumindest in der „normalen“ euklidischen Geometrie)

(v) Jede differenzierbare Funktion ist stetig. *(wahr)*

(vi) Jede gerade Zahl größer als zwei kann als Summe von zwei Primzahlen dargestellt werden.
(Dies ist die sog. *Goldbachsche Vermutung*. Zur Zeit ist noch unbekannt, ob sie wahr oder falsch ist.)

Dagegen sind die folgenden Sätze mit Sicherheit nicht als Aussagen zu bezeichnen.

(i) Hallo!

(ii) Mach endlich Deine Hausaufgaben!

(iii) 10^{100} ist eine große Zahl

(iv) Die Kreiszahl π ist ungefähr gleich 3.14.

(v) $x^3 - 3x^2 - 3x + 1$

(vi) $a^2 + b^2 = c^2$

Offenbar ist es sinnlos, einer Begrüßung oder einer Aufforderung einen Wahrheitswert zuzuordnen. Die Sätze (iii) und (iv) sind für eine Aussage nicht hinreichend objektiv. Der Ausdruck (v) ist ein ***Term*** (genauer gesagt, ein Polynom), für den die Feststellung *wahr* oder *falsch* ebenfalls keinen Sinn macht.

Satz (vi) ist für sich genommen keine Aussage, solange den Symbolen a, b und c keine Bedeutung zugeordnet wird. Legt man fest, dass $a = 3$, $b = 4$ und $c = 5$ sein soll, erhält man eine wahre Aussage, denn es gilt $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. Für viele andere Belegungen von a, b, c (zum Beispiel $a = 1$, $b = 2$, $c = 3$) erhält man dagegen eine falsche Aussage. Legt man fest, dass a, b, c Seitenlängen eines rechtwinkligen Dreiecks sein sollen, wobei c der längsten Seite zugeordnet ist, dann erhält man wiederum eine wahre Aussage. Einer der häufigsten Fehler bei der Formulierung mathematischer Aussagen besteht darin, dass Bezeichnungen (wie hier a, b, c) verwendet werden, die zuvor nicht definiert wurden!

Die Gleichung $a^2 + b^2 = c^2$ ist also keine Aussage; statt dessen fällt sie eine allgemeinere Kategoriev von Sätzen, die man unter dem Begriff „***Aussagenschema***“ zusammenfasst. Bei einem Aussagenschema handelt es sich um einen Satz, in dem eine Reihe von ***Parametern*** $x, y, \ldots$ vorkommen, und der zu einer Aussage wird, wenn man die Parameter durch geeignete mathematische Objekte ersetzt. Beispielsweise wird $a^2 + b^2 = c^2$ zu einer Aussage, wenn man für a, b, c die Längen der Katheten und der Hypothenuse eines rechtwinkligen Dreiecks einsetzt. Auch der (sprachlich formulierte) Satz

„Die Zahl x ist eine Primzahl.“

ist ein Aussagenschema mit x als Parameter. Setzt man für x die Werte 4 oder 6 ein, so erhält man eine falsche Aussage. Setzt man dagegen 2 oder 13 ein, dann erhält man eine wahre Aussage.

Zu beachten ist, dass im Allgemeinen natürlich nicht jede Einsetzung eine ***sinnvolle*** Aussage liefert. Zum Beispiel würde es keinen Sinn machen, in der Gleichung $a^2 + b^2 = c^2$ für a die leere Menge $\varnothing$ einzusetzen, da nicht ohne Weiteres klar ist, was der Ausdruck $\varnothing^2 + b^2 = c^2$ bedeuten soll.

Einfache Aussagen können umgangssprachlich, zum Beispiel durch Bindewörter wie „und“, „oder“, oder auch durch bestimmte Symbole ($\vee$, $\wedge$) zu komplexeren Aussagen ***verknüpft*** werden. Der Wahrheitswert der neuen Aussage ist dann durch die Wahrheitswerte der verknüpften Aussagen festgelegt. Wie diese Festlegung im einzelnen aussieht, kann am einfachsten durch sog. ***Wahrheitstabellen*** beschrieben werden. Seien φ und ψ zwei Aussagen. Die folgenden Verknüpfungen von Aussagen sind in der Mathematik allgemein gebräuchlich.

(i) ***Konjunktion*** $\varphi \wedge \psi$ „Es gilt φ und ψ.“

φ	ψ	$\varphi \wedge \psi$
w	w	w
w	f	f
f	w	f
f	f	f

Die erste Zeile der Tabelle bedeutet ausformuliert: „Sind die Aussagen φ und ψ beide wahr, dann ist auch die zusammengesetzte Aussage $\varphi \wedge \psi$ eine wahre Aussage.“ Beispielsweise ist der Satz

„Heute ist Mittwoch, und es gilt $1+1=2$.“

eine wahre Aussage - über den Erkenntniswert kann man geteilter Meinung sein. Wichtig hierbei ist, dass auch die zusammengesetzten Aussage entweder *wahr* oder *falsch* ist; in der mathematischen Logik ist kein Platz für „Halbwahrheiten“. So ist der Satz

„Heute ist Mittwoch, und es gilt $1+1=3$.“

auch am Mittwoch, dem 16. Oktober 2024 auf Grund des Eintrags in der zweiten Tabellenzeile eindeutig als *falsch* zu bezeichnen. (Am 18. Oktober 2024 entnimmt man der *vierten* Tabellenzeile, dass die Aussage *falsch* ist, denn in diesem Fall sind beide Teilaussagen falsch.)

(ii) ***Disjunktion*** $\varphi \vee \psi$ „Es gilt φ oder ψ.“

φ	ψ	$\varphi \vee \psi$
w	w	w
w	f	w
f	w	w
f	f	f

Zum Beispiel ist die Aussage „Es gilt $1+2=3$ oder $3+5=7$.“ wahr (zweite Tabellenzeile). Ebenso stimmt für jede reelle Zahl a die Aussage „Es gilt $a \geq 0$ oder $a \leq 0$.“, und zwar unabhängig davon, welche konkrete Zahl a man dort einsetzt. Hier kommt zum Beispiel für $a=0$ die erste, für $a=-2$ die dritte Zeile zur Anwendung.

Zu beachten ist, dass sich beim mathematischen „oder“ die beiden Aussagen φ und ψ nicht gegenseitig ausschließen, wie dies beim umgangssprachlichen „entweder - oder“ der Fall ist: Die Aussage $\varphi \vee \psi$ ist auch dann wahr, wenn die Aussagen φ und ψ beide zutreffen!

(iii) ***Negation*** $\neg\varphi$ „φ gilt nicht.“ / „φ ist falsch.“

φ	$\neg\varphi$
w	f
f	w

Beispielsweise ist der Satz „Die Gleichung $1+1=3$ gilt nicht.“ eine wahre Aussage (laut zweiter Tabellenzeile), und der Satz „Die Gleichung $1+1=2$ gilt nicht.“ ist falsch (laut erster Zeile).

(iv) ***Implikation*** $\varphi \Rightarrow \psi$ „Aus φ folgt ψ.“ / „Wenn φ gilt, dann gilt auch ψ.“ / „φ ist eine ***hinreichende*** Bedingung für ψ.“ / „ψ ist eine ***notwendige*** Bedingung für φ.“

φ	ψ	$\varphi \Rightarrow \psi$
w	w	w
w	f	f
f	w	w
f	f	w

Man bezeichnet φ als die ***Prämisse***, ψ als die ***Konklusion*** der Implikation $\varphi \Rightarrow \psi$. Bemerkenswert ist die Festlegung in der vierten Zeile: Wenn die Prämisse falsch ist, dann gilt die Implikation $\varphi \Rightarrow \psi$ auf jeden Fall als wahr, unabhängig vom Wahrheitswert der Aussage Konklusion. So gesehen ist

„Wenn $1+1=3$ ist, dann gilt auch $2+7=11$.“

eine wahre (wenn auch nicht besonders nützliche) Aussage. Logiker verwenden dafür den Ausspruch *„Ex falso quodlibet“*, d.h. aus etwas Falschem folgt alles Mögliche.

Bei der Implikation ist zu beachten, dass es zwischen den Aussagen A und B kein *kausaler* Zusammenhang bestehen muss, damit die Implikation $A \Rightarrow B$ zu einer wahren Aussage wird. Es kommt nur auf die Wahrheitswerte von φ und ψ an. Beispielsweise ist die Implikation

„Wenn $1+1=2$ ist, dann beträgt die Summe der Innenwinkel aller Dreiecke $180°$.“

wahr, obwohl die Gleichung $1+1=2$ wenig bis nichts mit den geometrischen Eigenschaften irgendwelcher Dreiecke zu tun hat. Ausschlaggebend für den Wahrheitsgehalt der Implikation ist hier nur, dass die beiden Teilaussagen wahr sind.

Implikationen spielen in der Mathematik eine sehr wichtige Rolle; so gut wie jeder mathematische Satz wird als Implikation formuliert. Im Mathematikunterricht werden Implikationen bereits bei ganz elementaren Vorgängen wie etwa der ***Umformung*** von Gleichungen verwendet. So verwendet man beispielsweise die Tatsache, dass die Implikation „$x+3=5 \Rightarrow x=2$“ für alle reellen Zahlen x gültig ist, um die Gleichung $x+3=5$ nach x hin „aufzulösen“.

(v) **Äquivalenz** $\varphi \Leftrightarrow \psi$ „Es gilt φ genau dann, wenn ψ gilt.“ / „φ ist hinreichende und zugleich notwendige Bedingung für ψ.“

φ	ψ	$\varphi \Leftrightarrow \psi$
w	w	w
w	f	f
f	w	f
f	f	w

Beim Arbeiten mit Implikationen ist es sehr wichtig, die zusammengesetzten Aussagen „$\varphi \Rightarrow \psi$“, „$\psi \Rightarrow \varphi$“ und „$\varphi \Leftrightarrow \psi$“ sorgfältig auseinander zu halten. Geschieht dies nicht, dann kann das bereits beim Auflösen von quadratischen Gleichungen zu Fehlern führen. Beispielsweise ist die Implikation $x = 3 \Rightarrow x^2 = 9$ für alle reellen Zahlen x gültig, während $x^2 = 9 \Rightarrow x = 3$ für alle reellen Zahlen $x \neq -3$ richtig, für $x = -3$ aber falsch ist: In diesem Fall ist Prämisse $x^2 = 9$ wahr, die Konklusion $x = 3$ aber falsch, damit ist die gesamte Implikation falsch. Wendet man nun diese fehlerhafte Implikation bei der Auflösung der Gleichung $x^2 - 8x + 7 = 0$ an, so erhält man

$$x^2 - 8x + 7 = 0 \quad \Rightarrow \quad x^2 - 8x = -7 \quad \Rightarrow \quad x^2 - 8x + 16 = 9 \quad \Rightarrow \quad (x-4)^2 = 9$$

$$\text{„}\Rightarrow\text{“} \quad x - 4 = 3 \quad \Rightarrow \quad x = 7$$

und „verliert“ somit die Lösung $x = 1$ der Gleichung. Der Fehler tritt an der Stelle auf, wo das Implikationszeichen $\Rightarrow$ in Anführungsstriche gesetzt wurde. Man könnte auch sagen, dass der Fehler in der Rechnung oben dadurch zu Stande kam, dass an einer Stelle eine notwendige Bedingung mit einer hinreichenden Bedingung verwechselt wurde: Die Gleichung $(x-4)^2 = 9$ ist zwar eine notwendige Bedingung dafür, dass $x - 4 = 3$ ist, aber eben keine hinreichende. Dieser Unterschied spielt, wie wir noch sehen werden, bei vielen mathematischen Sätzen eine wichtige Rolle, zum Beispiel bei der Bestimmung von lokalen Extremstellen einer Funktion.

Häufig werden durch ***mehrfache*** Anwendung der Verknüpfungssymbole nicht nur zwei, sondern mehrere Aussagen miteinander verbunden. In welcher Reihenfolge dies geschieht, wird durch Klammern festgelegt. Beispielsweise bedeutet $(\varphi \wedge \psi) \vee \rho$, dass zuerst φ und ψ miteinander „und“-verknüpft und diese Aussage dann anschließend mit der Aussage ρ noch „oder“-verknüpft wird.

Um Schreibarbeit (also Klammern) einzusparen, legt man fest, dass bestimmte Symbole stärker binden als andere, vergleichbar mit der Konvention „Punktrechnung vor Strichrechnung“ aus der Arithmetik. Per Festlegung bindet das Negationszeichen $\neg$ am stärksten, danach in absteigender Reihenfolge die Zeichen $\wedge$, $\vee$, $\Rightarrow$ und $\Leftrightarrow$. Beispielsweise ist der Ausdruck

$$\neg\varphi \wedge \neg\psi \Rightarrow \varphi \Leftrightarrow \psi \qquad \text{gleichbedeutend mit} \qquad (((\neg\varphi) \wedge (\neg\psi)) \Rightarrow \varphi) \Leftrightarrow \psi.$$

Gelegentlich kann der Wahrheitsgehalt einer zusammengesetzte Aussage bestimmt werden, ohne dass man die Teilaussagen, aus denen die Aussage besteht, überhaupt kennt. Solche Aussagen wirken auf den ersten Blick eher nutzlos, bilden aber die Grundlage für das ***logische Schließen*** innerhalb einer mathematischen Beweisführung.

(1.2) Definition Eine zusammengesetzte Aussage, die unabhängig vom Wahrheitsgehalt ihrer Teilaussagen immer wahr ist, wird ***Tautologie*** genannt.

Ein Beispiel für eine Tautologie ist die bekannte Bauernregel

„Wenn der Hahn kräht auf dem Mist, dann ändert sich das Wetter, oder es bleibt, wie es ist."

Isolieren wir hier die Teilaussagen

$$\begin{aligned} \varphi &= \text{„Der Hahn kräht auf dem Mist."} \\ \psi &= \text{„Das Wetter ändert sich."} \end{aligned}$$

und interpretieren den Satz „Das Wetter bleibt, wie es ist." als Negation $\neg\psi$ von ψ, dann ist unsere Bauernregel ϕ in Kurzschreibweise durch $\varphi \Rightarrow (\psi \vee \neg\psi)$ gegeben. Wir wissen bereits, dass der Wahrheitsgehalt von ϕ nur von den Wahrheitswerten der Aussagen φ und ψ abhängt. Um zu kontrollieren, ob es sich bei ϕ um eine Tautologie handelt, genügt es also, alle möglichen Kombinationen von Wahrheitswerten für φ und ψ in den Ausdruck ϕ einzusetzen. Wir erledigen dies durch Ausfüllen einer Tabelle.

φ	ψ	$\neg\psi$	$\psi \vee \neg\psi$	ϕ
w	w	f	w	w
w	f	w	w	w
f	w	f	w	w
f	f	w	w	w

Die zusammengesetzte Aussage ϕ ist unabhängig von φ und ψ immer wahr, also eine Tautologie.

(1.3) Definition Wir sagen, die Aussage ψ folgt aus den Aussagen $\varphi_1, ..., \varphi_n$ durch einen ***logischen Schluss***, wenn die Implikation

$$\varphi_1 \wedge ... \wedge \varphi_n \Rightarrow \psi \qquad \text{eine Tautologie ist.}$$

Wir sehen uns nun eine Reihe von logischen Schlüssen an, die in der Mathematik häufig verwendet werden. Im folgenden bezeichnen φ, ϕ und ψ jeweils beliebige Aussagen. Mit Hilfe von Wahrheitstabellen wird überprüft, dass die logischen Schlüsse zulässig sind.

(i) ***Modus Ponens*** $\varphi \wedge (\varphi \Rightarrow \psi) \Rightarrow \psi$

„Wenn φ gilt und aus φ die Aussage ψ folgt, dann gilt ψ."

φ	ψ	$\varphi \Rightarrow \psi$	$\varphi \wedge (\varphi \Rightarrow \psi)$	$\varphi \wedge (\varphi \Rightarrow \psi) \Rightarrow \psi$
w	w	w	w	w
f	w	w	f	w
w	f	f	f	w
f	f	w	f	w

(ii) ***Beweis durch Kontraposition*** $(\varphi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\varphi)$

„Aus φ folgt ψ genau dann, wenn aus $\neg\psi$ die Aussage $\neg\varphi$ folgt.

φ	ψ	$\neg\varphi$	$\neg\psi$	$\varphi \Rightarrow \psi$	$\neg\psi \Rightarrow \neg\varphi$	$(\varphi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\varphi)$
w	w	f	f	w	w	w
w	f	f	w	f	f	w
f	w	w	f	w	w	w
f	f	w	w	w	w	w

(iii) ***Beweis durch Widerspruch*** $(\neg\varphi \Rightarrow \phi \wedge \neg\phi) \Rightarrow \varphi$

"Wenn aus $\neg\varphi$ ein Widerspruch folgt (nämlich eine Aussage ϕ und zugleich auch ihr Gegenteil $\neg\phi$), dann ist φ wahr."

φ	ϕ	$\neg\varphi$	$\neg\phi$	$\phi \wedge \neg\phi$	$\neg\varphi \Rightarrow \phi \wedge \neg\phi$	$(\neg\varphi \Rightarrow \phi \wedge \neg\phi) \Rightarrow \varphi$
w	w	f	f	f	w	w
w	f	f	w	f	w	w
f	w	w	f	f	f	w
f	f	w	w	f	f	w

(iv) ***Satz vom Ringschluss*** $(\varphi \Rightarrow \phi) \wedge (\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi) \Rightarrow (\varphi \Leftrightarrow \phi) \wedge (\phi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \varphi)$

„Wenn aus φ die Aussage ϕ und aus ϕ die Aussage ψ und aus ψ wieder die Aussage φ folgt, dann sind die drei Aussagen φ, ϕ und ψ äquivalent."

Hier ist die Verifikation etwas aufwändiger als bei den vorherigen Regeln. Zur Abkürzung definieren wir die Teilaussagen $A = \varphi \Rightarrow \phi$, $B = \phi \Rightarrow \psi$, $C = \psi \Rightarrow \varphi$, $D = \varphi \Leftrightarrow \phi$, $E = \phi \Leftrightarrow \psi$ und $F = \psi \Leftrightarrow \varphi$.
Damit erhalten wir

φ	ϕ	ψ	A	B	C	D	E	F	$A \wedge B \wedge C$	$D \wedge E \wedge F$	$A \wedge B \wedge C \Rightarrow D \wedge E \wedge F$
w	w	w	w	w	w	w	w	w	w	w	w
w	w	f	w	f	w	w	f	f	f	f	w
w	f	w	f	w	w	f	f	w	f	f	w
w	f	f	f	w	w	f	w	f	f	f	w
f	w	w	w	w	f	f	w	f	f	f	w
f	w	f	w	f	w	f	f	w	f	f	w
f	f	w	w	w	f	w	f	f	f	f	w
f	f	f	w	w	w	w	w	w	w	w	w

§ 2. Mengenlehre und Prädikatenlogik

Inhaltsübersicht

Fast die gesamte moderne Mathematik ist auf dem Begriff der ***Menge*** aufgebaut. Eine Menge kann durch Aufzählung ihrer Elemente oder durch eine definierende Bedingung, ein sog. ***Aussagenschema***, beschrieben werden. Mit Hilfe von Aussagenschemata definieren wir auch einige wichtige ***Mengenoperationen***. Außerdem werden mit ihnen ***quantifizierte*** Aussagen gebildet, wie sie bei der Formulierung mathematischer Sätze fast immer vorkommen. Zum Abschluss führen wir die natürlichen Zahlen ein und besprechen das Prinzip der ***vollständigen Induktion***.

Wichtige Begriffe und Sätze

- Mengendefinition nach Cantor
- Bedeutung der Relationen $\in$, $\subseteq$, $\supseteq$, $\subsetneq$, $\supsetneq$
- Definition von Mengen durch definierende Bedingungen (Aussagenschemata)
- Mengenoperationen (Durchschnitt, Vereinigung, Differenz, kartesisches Produkt, Potenzmengenbildung)
- Nachweis der Mengengleichheit
- quantifizierte Aussagen, All- und Existenzquantor ($\forall, \exists$)
- Prinzip der vollständigen Induktion

Fast die gesamte moderne Mathematik basiert auf dem Konzept der Menge. Dies bedeutet, dass fast jedes mathematische Objekt, egal ob es sich dabei um eine Zahl, eine Funktion oder ein geometrisches Gebilde handelt, letztendlich durch eine Menge beschrieben werden kann. Desweiteren kann fast jede mathematische Aussage auf die Mengenlehre zurückgeführt und mit den Mitteln der Mengenlehre bewiesen werden, eine ganz erstaunliche Feststellung, wenn man sich die Vielfalt und Verschiedenartigkeit der mathematischen Strukturen vor Augen hält.

(2.1) Definition *(naive Mengendefinition von Cantor)*

„Eine ***Menge*** ist eine beliebige Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens – welche die ***Elemente*** dieser Menge genannt werden – zu einem Ganzen."

Hierbei handelt es sich nicht um eine Definition im streng mathematischen Sinn; Begriffe wie „Zusammenfassung", „Objekt", „Anschauung" usw. werden ihrerseits nicht definiert, sondern rein intuitiv verwendet. Auf Grund unserer Alltagserfahrung ist die Bedeutung der Cantorschen Definition dennoch unmittelbar klar. Jeder kann sich vorstellen, was es heißt, „Objekte unserer Anschauung" zu einem „Ganzen" zusammenzufassen (z.B. die Bürger einer Gemeinde, die Möbelstücke in einer Wohnung, die Moleküle eines Wassertropfens usw.), dasselbe gilt für die „Objekte unseres Denkens" wie etwa die natürlichen Zahlen oder geometrische Figuren.

Wir weisen auf zwei wichtige Punkte der Cantorschen Definition hin: Erstens sind sämtliche Objekte einer Menge ***verschieden***, es ist also nicht möglich, dass ein und dasselbe Objekt mehrfach in einer Menge vorkommt. Zweitens ist jede Menge als „Zusammenfassung“ durch ihre Elemente ***eindeutig bestimmt***. Dies bedeutet, dass zwei Mengen genau dann gleich sind, wenn sie dieselben Elemente enthalten.

Folgende Kurzschreibweisen sind in der Mengenlehre üblich.

$x \in M$	Das Objekt x ist Element der Menge M.
$x \notin M$	Das Objekt x ist *kein* Element der Menge M, in Kurzform also $\neg(x \in M)$.
$M \subseteq N$	Jedes Element x von M ist auch ein Element von N, d.h. die Implikation $x \in M \Rightarrow x \in N$ ist für alle Objekte x erfüllt. Man bezeichnet M dann als ***Teilmenge*** von N.
$M = N$	Es gilt $x \in M \Leftrightarrow x \in N$ für alle Objekte x (äquivalent: $M \subseteq N \wedge N \subseteq M$).
$M \supseteq N$	gleichbedeutend mit $N \subseteq M$
$M \subsetneq N$	$M \subseteq N \wedge \neg(M = N)$
$M \supsetneq N$	gleichbedeutend mit $N \subsetneq M$
$\varnothing$	die leere Menge Dies ist die eindeutig bestimmte Menge die $x \notin \varnothing$ für alle Objekte x erfüllt, also die Menge, die kein einziges Objekt als Element besitzt.

Es gibt mehrere Möglichkeiten, eine Menge konkret anzugeben. Zunächst kann dies ***umgangssprachlich*** geschehen.

„Sei P die Menge aller Primzahlen.“

Eine andere Möglichkeit besteht darin, die Elemente einer Menge explizit ***aufzuzählen***.

$$M = \{1, 2, 3, 4, 5, 6, 7\} \qquad \text{oder kürzer} \qquad M = \{1, 2, ..., 7\}$$

Bei der Verwendung von „ ... “ ist darauf zu achten, dass für den Leser klar ersichtlich ist, welche Elemente bei der Aufzählung weggelassen wurden. Schreibt man etwa $P = \{2, 3, 5, 7, 11, 13, 17, ...\}$, dann ist noch einigermaßen ersichtlich, dass die Menge der Primzahlen gemeint ist. Schwieriger wird das schon bei der Angabe

$$M = \{1, 4, ..., 64\}.$$

Hier ist nicht ohne weiteres klar, ob die Menge $\{1, 4, 16, 64\} = \{4^0, 4^1, 4^2, 4^3\}$ der ersten drei Viererpotenzen oder vielleicht $\{1, 4, 9, 16, 25, 36, 49, 64\} = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2\}$, die Menge der ersten acht Quadratzahlen, gemeint ist. Ein Vorteil der „ ... “-Schreibweise besteht aber darin, dass mit ihr auch unendliche Mengen direkt angeben werden können, zum Beispiel die Menge $\mathbb{N} = \{1, 2, 3, ...\}$ der natürlichen Zahlen.

Auch mit Hilfe der im letzten Kapitel eingeführten Aussagenschemata lassen sich Mengen definieren. Sei φ ein Aussagenschema mit einem Parameter x und M eine Menge. Für jedes $c \in M$ bezeichnen wir mit $\varphi(c)$ den Satz, den man erhält, wenn der Parameter x durch c ersetzt wird. Wir setzen voraus, dass $\varphi(c)$ für *jedes* $c \in M$ eine sinnvolle Aussage ist. Nach Definition besteht dann die Menge

$$N \quad = \quad \{c \in M \mid \varphi(c)\}$$

aus genau denjenigen Elementen c von M, für die $\varphi(c)$ eine wahre Aussage ist. Man nennt φ dann auch die ***definierende Bedingung*** für die Teilmenge N von M.

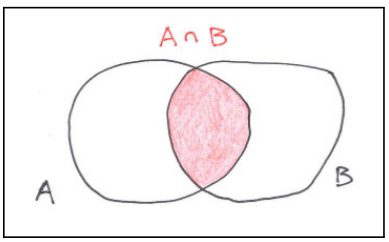
Beispielsweise beschreibt $\{c \in \mathbb{R} \mid c^2 < 1\}$ die Menge derjenigen reellen Zahlen, deren Quadrat kleiner als 1 ist. In dieser Situation ist also $M = \mathbb{R}$ die Grundmenge und $\varphi(x) = x^2 < 1$ das Aussagenschema, dass die Teilmenge beschreibt. Offenbar ist $c^2 < 1$ für jedes $c \in \mathbb{R}$ eine sinnvolle, aber nur für $-1 < c < 1$ auch eine wahre Aussage.

Gelegentlich verwendet man auch die Notation $N = \{\, c \mid \varphi(c)\}$, ohne die Angabe einer Grundmenge für die Objekte c. In diesem Fall besteht N aus *allen* mathematischen Objekten c, für die die Aussage $\varphi(c)$ wahr ist. Strenggenommen ist eine solche Definition für beliebige Aussagenschemta φ nicht zulässig, weil dies zu Widersprüchen führen kann (Stichwort „Russelsche Antinomie“). Wir werden die Notation aber nur in Situationen einsetzen, wo solche Probleme ausgeschlossen sind.

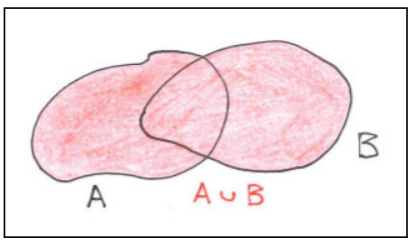
Aus gegebenen Mengen können durch weitere Operationen neue Mengen definiert werden. Seien A und B beliebig vorgegebene Mengen. Folgende Mengenoperationen sind in der Mathematik allgemein gebräuchlich.

Durchschnitt	$A \cap B$	$=$	$\{\, a \mid a \in A \wedge a \in B \,\}$
Vereinigung	$A \cup B$	$=$	$\{\, a \mid a \in A \vee a \in B \,\}$
Differenz	$A \setminus B$	$=$	$\{\, a \mid a \in A \wedge a \notin B \,\}$
kartesisches Produkt	$A \times B$	$=$	$\{\, (a,b) \mid a \in A \wedge b \in B \,\}$
Potenzmenge	$\mathscr{P}(A)$	$=$	$\{\, B \mid B \subseteq A \,\}$

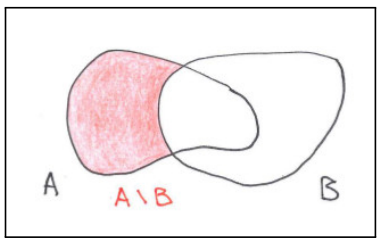
Einige dieser Operationen lassen sich durch sog. ***Venn-Diagramme*** veranschaulichen.



Durchschnitt



Vereinigung



Differenz

Das kartesische Produkt $A \times B$ besteht aus allen Paaren (a, b), die mit Elementen $a \in A$ und $b \in B$ gebildet werden können. Ist bespielsweise $A = \{1, 2, 3\}$ und $B = \{1, 2, 4, 5\}$, dann erhalten wir

$$A \times B \quad = \quad \{1,2,3\} \times \{1,2,4,5\} \quad = \quad \left\{ \begin{array}{llll} (1,1), & (1,2), & (1,4), & (1,5), \\ (2,1), & (2,2), & (2,4), & (2,5), \\ (3,1), & (3,2), & (3,4), & (3,5) \end{array} \right\}$$

(Die Elemente wurden nur zur besseren Übersicht in einem rechteckigen Schema angeordnet. Man hätte auch alle 12 Elemente direkt hintereinander schreiben können.)

Bei der Definition des kartesischen Produkts ist zu beachten, dass zwei ***Paare*** (a, b) und (c, d) von Objekten a, b, c, d nur dann gleich sind, wenn $a = c$ und $b = d$ erfüllt ist. Zum Beispiel sind die Paare $(3, 5)$ und $(5, 3)$ verschieden. Im Gegensatz dazu stimmen die zweielementigen Mengen $\{3, 5\}$ und $\{5, 3\}$ überein, da es keine Rolle spielt, in welcher Reihenfolge die Elemente einer Menge aufgezählt werden.

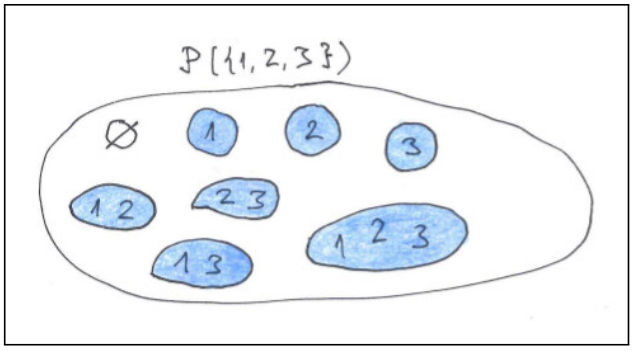
Das kartesische Produkt kann auch mit mehr als zwei Mengen gebildet werden. Die Elemente bezeichnet man dann nicht mehr als Paare, sondern als ***Tupel***. Sind beispielsweise A, B, C drei beliebige Mengen, dann setzt man

$$A \times B \times C \quad = \quad \{\, (a,b,c) \mid \, a \in A \,,\; b \in B \,,\; c \in C \}$$

wobei wieder $(a, b, c) = (a', b', c')$ nur dann erfüllt ist, wenn $a = a'$, $b = b'$ und $c = c'$ gilt. Es ist also beispielsweise $(1, 2, 3) \neq (1, 3, 2)$ und $(2, 2, 4) \neq (2, 4, 2)$. Häufig werden mehrfache kartesische Produkte auch mit ein- und derselben Menge gebildet. Man definiert $A^2 = A \times A$, $A^3 = A \times A \times A$, $A^4 = A \times A \times A \times A$ usw. Beispielsweise ist $(3, 4, \frac{1}{2}, \sqrt{2}, -9)$ ein Element der Menge $\mathbb{R}^5$.

Bei den Potenzmengen ist zu beachten, dass deren Elemente selbst wieder Mengen sind! Nach Definition ist für jede beliebige Mengen A, B die Aussage $B \in \mathscr{P}(A)$ äquivalent zu $B \subseteq A$. Intuitiv klar ist, dass bei einer endlichen Menge A die Potenzmenge $\mathscr{P}(A)$ ebenfalls nur endlich viele Elemente enthält. Ist beispielsweise $A = \{1, 2, 3\}$, dann enthält jede Teilmenge von A entweder kein, genau ein, genau zwei oder genau drei Elemente. Dies kann für eine systematische Aufzählung der Elemente von $\mathscr{P}(A)$ verwendet werden: Es gilt

$$\mathscr{P}(A) \quad = \quad \{\, \varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \,\}.$$



die achtelementige Potenzmenge von $\{1, 2, 3\}$

Eine häufige Fehlerquelle beim Umgang mit Mengen besteht darin, dass man zwischen einer Menge und ihren Elementen nicht klar unterscheidet. Beispielsweise wäre es falsch zu sagen, dass die 1 ein Element von $\mathscr{P}(A)$ ist. Lediglich die Menge $\{1\}$ ist ein Element von $\mathscr{P}(A)$, und 1 ist ein Element der Menge $\{1\}$. Momentan klingt das noch recht haarspalterisch; bei komplizierteren mengentheoretischen Konstruktionen (zum Beispiel Faktorstrukturen) kommt man aber in große Schwierigkeiten, wenn man sich an diese Unterscheidung nicht gewöhnt hat.

Eine wichtige Grundtechnik beim Führen von Beweisen ist der Nachweis der ***Gleichheit zweier Mengen***. Häufig bietet es sich an, die Aussage $M = N$ in die folgenden beiden Teilaussagen zu zerlegen und diese einzeln zu beweisen.

(i) Ist x ein Element der Menge M, dann ist x auch ein Element von N.
(ii) Ist x ein Element der Menge N, dann ist x auch ein Element von M.

Aus der ersten Aussage folgt $M \subseteq N$, aus der zweiten $N \subseteq M$, insgesamt also $M = N$.

Wie die Beweise der Teilaussagen (i) und (ii) aussehen können, schauen wir uns an einem konkreten Beispiel an. Unser Ziel ist der Beweis der Gleichung

$$\{\, (x,y,z) \in \mathbb{R}^3 \mid (xy+1)z = 0 \,\} \quad = \quad \{\, (x,y,0) \mid x,y \in \mathbb{R} \,\} \cup \{\, (x,-\tfrac{1}{x},z) \mid x \in \mathbb{R} \setminus \{0\}\ ,\ z \in \mathbb{R} \,\}.$$

Wir bezeichnen die Menge auf der linken Seite der Gleichung mit M und die Menge auf der rechten Seite der Gleichung mit N. Die Menge N enthält also alle Tupel der Form $(x,y,0)$ mit $x,y \in \mathbb{R}$ und alle Tupel der Form $(x,-\frac{1}{x},z)$ mit $x,z \in \mathbb{R}$ und $x \neq 0$.

Beweis der Teilaussage (i)
Sei $p \in M$. Nach Definition von M gilt $p = (x,y,z) \in \mathbb{R}^3$ mit $x,y,z \in \mathbb{R}$ und $(xy+1)z = 0$. Aus dieser Gleichung folgt $xy+1 = 0$ oder $z = 0$, denn das Produkt zweier reeller Zahlen ist nur dann gleich Null, wenn einer der beiden Faktoren gleich Null ist. Ist $z = 0$, dann hat p die Form $(x,y,0)$ mit $x,y \in \mathbb{R}$, also liegt p in N. Ist dagegen $xy+1 = 0$, dann muss $x \neq 0$ gelten, denn ansonsten wäre $xy+1 = 0 \cdot y + 1 = 1$. Aus $xy+1 = 0$ folgt $xy = -1$, wegen $x \neq 0$ dann auch $y = -\frac{1}{x}$ und somit ebenfalls $p = (x,y,z) = (x,-\frac{1}{x},z) \in N$.

Beweis der Teilaussage (ii)
Sei $p \in N$. Dann gilt $p = (x,y,0)$ mit geeigneten $x,y \in \mathbb{R}$ oder $p = (x,-\frac{1}{x},z)$ für geeignete $x \in \mathbb{R} \setminus \{0\}$ und ein $z \in \mathbb{R}$. Betrachten wir zunächst den Fall $p = (x,y,0)$ mit $x,y \in \mathbb{R}$. Setzen wir $z = 0$, dann gilt $p = (x,y,z) \in \mathbb{R}^3$ und $(xy+1)z = (xy+1) \cdot 0 = 0$. Daraus folgt $p \in M$. Betrachten wir nun den Fall, dass $p = (x,-\frac{1}{x},z)$ für ein $x \in \mathbb{R} \setminus \{0\}$ und ein $z \in \mathbb{R}$ gilt. Setzen wir $y = -\frac{1}{x}$, dann liegt $p = (x,y,z)$ in $\mathbb{R}^3$. Außerdem gilt $(xy+1)z = (x \cdot (-\frac{1}{x}) + 1)z = ((-1)+1)z = 0 \cdot z = 0$. Also liegt p auch in diesem Fall in M. □

In einfacheren Situationen lässt sich die Gleichheit zweier Mengen auch durch eine Kette von Äquivalenzumformungen beweisen. Als Beispiel betrachten wir die Mengengleichung

$$\{\, x \in \mathbb{R} \mid x^2 + x - 6 = 0 \,\} \quad = \quad \{\, -3, 2 \,\}.$$

Wieder sei M die Menge auf der linken und N die Menge auf der rechten Seite der Gleichung. Es gilt $M = N$, wenn wir für jedes Objekt x die Äquivalenz $x \in M \iff x \in N$ beweisen können. Da M und N beides Teilmengen von $\mathbb{R}$ sind, genügt es, die Äquivalenz für alle $x \in \mathbb{R}$ zu beweisen, denn ansonsten sind die Aussagen $x \in M$ und $x \in N$ beide falsch und die Äquivalenz damit auf jeden Fall wahr.

Sei also $x \in \mathbb{R}$ vorgegeben. Dann gilt

$$x \in M \iff x^2 + x - 6 = 0 \iff x^2 + x = 6 \iff x^2 + x + \tfrac{1}{4} = \tfrac{25}{4} \iff (x + \tfrac{1}{2})^2 = \left(\tfrac{5}{2}\right)^2$$
$$\iff (x + \tfrac{1}{2})^2 - \left(\tfrac{5}{2}\right)^2 = 0 \iff ((x + \tfrac{1}{2}) + \tfrac{5}{2})((x + \tfrac{1}{2}) - \tfrac{5}{2}) = 0 \iff (x+3)(x-2) = 0$$
$$\iff x + 3 = 0 \vee x - 2 = 0 \iff x = -3 \vee x = 2 \iff x \in \{-3, 2\} \iff x \in N.$$

Hier wurde nichts anderes getan, als die Gleichung durch Bildung der qudratischen Ergänzung zu lösen. Wichtig ist bei solchen Beweisen, dass jeder einzelne Schritt genau begründet werden kann, und dass jeweils *beide* Implikationsrichtungen gültig sind. Beispielsweise wäre $x = 3 \iff x^2 = 9$ keine zulässige Äquivalenzumformung, weil die Implikationsrichtung „$\Leftarrow$“ nicht für jede reelle Zahl x gültig ist. (Wie wir bereits oben festgestellt haben, ist sie ist für $x = -3$ falsch.)

In vielen Situationen möchte man Aussagen formulieren, die die Gesamtheit der Elemente einer Menge betreffen. Dazu verwendet man den sog. ***Allquantor*** $\forall$ und den ***Existenzquantor*** $\exists$. Sei φ ein Aussagenschema mit x als Parameter, und wiederum sei M eine Menge mit der Eigenschaft, dass man für jedes $c \in M$ durch Ersetzung von x durch c eine sinnvolle Aussage $\varphi(c)$ erhält. Dann kann man mit Hilfe von All- und Existenzquantor zwei neue Aussagen $\forall x \in M : \varphi$ und $\exists x \in M : \varphi$ bilden, die man als ***quantifizierte*** Aussagen bezeichnet. Den Umgang mit quantifizierten Aussagen bezeichnet man als ***Prädikatenlogik***, im Unterschied zur Aussagenlogik, wo man nur Aussagen ohne Quantoren betrachtet.

(2.2) Definition

(i) Die Aussage $\forall x \in M : \varphi$ bedeutet, dass $\varphi(c)$ für ***alle*** $c \in M$ wahr ist.
Es gilt also $\{c \in M \mid \varphi(c)\} = M$.

(ii) Die Aussage $\exists x \in M : \varphi$ bedeutet, dass $\varphi(c)$ für ***mindestens ein*** $c \in M$ wahr ist.
Es gilt also $\{c \in M \mid \varphi(c)\} \neq \varnothing$.

Betrachten wir beispielsweise das Aussagenschema $x \leq 5$ mit dem Parameter x über der Menge $M = \mathbb{R}$ der reellen Zahlen und bezeichnen es mit φ.

(i) Die Aussage $\forall x \in \mathbb{R} : x \leq 5$ ist ***falsch***, denn $\varphi(c)$ ist nicht für alle $c \in \mathbb{R}$ erfüllt. Beispielsweise ist $\varphi(7)$ falsch.

(ii) Die Aussage $\exists x \in \mathbb{R} : x \leq 5$ ist ***wahr***, denn es gibt Elemente $c \in \mathbb{R}$, für die $\varphi(c)$ wahr ist. Zum Beispiel ist $\varphi(4)$ eine wahre Aussage.

Die meisten Aussagen, die wir im Laufe der Zeit beweisen werden, sind quantifizierte Aussagen, enthalten also die Formulierungen „für alle“ oder „es gibt ein x, so dass...“. Dabei treten besonders zu Anfang häufig methodische Fehler auf. Um eine Aussage der Form $\forall x \in M : \varphi(x)$ zu beweisen, muss die Aussage $\varphi(c)$ für ***jedes*** $c \in M$ bewiesen werden. Dazu gibt man sich mit der Floskel „Sei $c \in M$.“ ein beliebiges Element c aus M vor und beweist anschließend die Aussage $\varphi(c)$. Während des Beweises darf dann nur verwendet werden, dass c ein Element der Menge M ist. Jede Einschränkung oder Spezialisierung von c macht den Beweis ***ungültig***.

Um andererseits eine Aussage der Form $\exists x \in M : \varphi(x)$ zu beweisen, genügt es, ein ***spezielles*** Element $c \in M$ anzugeben und die Aussage $\varphi(c)$ nur für dieses c zu beweisen. Natürlich kann es schwierig sein, ein solches c erst einmal zu finden. Um beispielsweise die Aussage $\exists x \in \mathbb{R} : x^2 + x - 6 = 0$ auf diesem Weg zu beweisen, muss eine Lösung der quadratischen Gleichung $x^2 + x - 6 = 0$ gefunden werden.

Gelegentlich hat man es auch mit der ***Negation*** einer quantifizierten Aussage zu tun.

(2.3) Satz Sei M eine Menge und $\varphi(x)$ ein Aussagenschema mit der Eigenschaft, dass $\varphi(c)$ für jedes $c \in M$ eine sinnvolle Aussage ist. Dann gelten die folgenden Äquivalenzen.

$$\text{(i)} \quad \neg\forall x \in M : \varphi(x) \iff \exists x \in M : \neg\varphi(x)$$
$$\text{(ii)} \quad \neg\exists x \in M : \varphi(x) \iff \forall x \in M : \neg\varphi(x)$$

Beweis: zu (i) „$\Leftarrow$“ (durch Widerspruch) Auf Grund der Voraussetzung gibt es ein $c \in M$, so dass $\neg\varphi(c)$ erfüllt ist. Nehmen wir nun an, auch die Aussage $\forall x \in M : \varphi(x)$ ist wahr. Dann muss insbesondere auch $\varphi(c)$ gelten. Die Aussagen $\varphi(c)$ und $\neg\varphi(c)$ wären also gleichzeitig erfüllt, was unmöglich ist. Der Widerspruch zeigt, dass $\neg\forall x \in M : \varphi(x)$ gelten muss.

„$\Rightarrow$“ (durch Kontraposition und Widerspruch) Wir setzen $\neg\exists x \in M : \neg\varphi(x)$ voraus und zeigen $\forall x \in M : \varphi(x)$. Sei dazu $c \in M$ vorgegeben. Angenommen, es gilt $\neg\varphi(c)$. Dann existiert also ein $c \in M$ mit $\neg\varphi(c)$, und das bedeutet, dass $\exists x \in M : \neg\varphi(x)$ gilt, im Widerspruch zu unserer Voraussetzung. Da also $\neg\varphi(c)$ zu einem Widerspruch führt, muss $\varphi(c)$ gelten. Weil $c \in M$ beliebig vorgegeben war, haben wir somit $\forall x \in M : \varphi(x)$ bewiesen.

zu (ii) „$\Leftarrow$“ (durch Kontraposition und Widerspruch) Wir setzen $\exists x \in M : \varphi(x)$ voraus und leiten daraus $\neg\forall x \in M : \neg\varphi(x)$ ab. Auf Grund unserer Voraussetzung existiert ein $c \in M$, so dass $\varphi(c)$ erfüllt ist. Nehmen wir nun an, es gilt $\forall x \in M : \neg\varphi(x)$. Dann müsste auch $\neg\varphi(c)$ gelten, im Widerspruch zu $\varphi(c)$. Also gilt statt dessen $\neg\forall x \in M : \neg\varphi(x)$.

„$\Rightarrow$“ (durch Widerspruch) Unsere Voraussetzung lautet $\neg\exists x \in M : \varphi(x)$. Zum Beweis von $\forall x \in M : \neg\varphi(x)$ sei $c \in M$ vorgegeben. Nehmen wir an, es gilt $\varphi(c)$. Dann wäre die Aussage $\exists x \in M : \varphi(x)$ erfüllt, im Widerspruch zu unserer Voraussetzung. Also gilt $\neg\varphi(c)$. Weil $c \in M$ beliebig vorgegeben war, ist damit $\forall x \in M : \neg\varphi(x)$ bewiesen. □

Schließlich ist es noch möglich, mehrere Quantoren zu ***verschachteln***. In diesem Fall benötigt man Aussagenschemata mit ***mehreren*** Parametern. Sei φ ein Aussagenschema mit den beiden Parametern x, y und M, N Mengen mit der Eigenschaft, dass man für alle $c \in M$ und $d \in N$ eine sinnvolle Aussage $\varphi(c,d)$ erhält, wenn man x durch c und y durch d ersetzt. Dann ist $\forall y \in N : \varphi$ ein Aussagenschema, das nur noch vom Parameter x abhängt, und

$$\exists x \in M : \forall y \in N : \varphi$$

ist eine Aussage, mit zwei ineinander verschachtelten Quantoren. Umgangssprachlich bedeutet diese Aussage: „Es gibt ein $c \in M$, so dass für alle $d \in N$ jeweils $\varphi(c,d)$ gilt."

Dabei sind die Quantoren $\exists$ und $\forall$ in beliebiger Kombination zugelassen. Es ergeben sich dadurch Aussagen mit unterschiedlicher Bedeutung.

- Der Ausdruck $\forall x \in M : \exists y \in N : \varphi$ bedeutet:
  „Für jedes $c \in M$ gibt es ein $d \in N$, so dass $\varphi(c,d)$ gilt."
- Der Ausdruck $\exists x \in M : \exists y \in N : \varphi$ bedeutet:
  „Es gibt Elemente $c \in M$ und $d \in N$, so dass $\varphi(c,d)$ gilt."
- Der Ausdruck $\forall x \in M : \forall y \in N : \varphi$ bedeutet:
  „Für alle $c \in M$ und alle $d \in N$ gilt $\varphi(c,d)$."

Man beachte, dass auch die Aussagen $\forall x \in M : \exists y \in N : \varphi$ und $\exists y \in N : \forall x \in M : \varphi$ nicht etwa gleichbedeutetend sind, es kommt also auch auf die ***Reihenfolge*** der Quantoren an. Wir machen uns dies am Beispiel des Aussagenschemas $x < y$ mit den Parametern x, y klar, das wir wieder mit φ bezeichnen. Offenbar erhält man jedes Mal eine sinnvolle Aussage, wenn man für x und y Elemente aus $\mathbb{R}$, der Menge der reellen Zahlen, einsetzt.

Die Aussage $\exists x \in \mathbb{R} : \forall y \in \mathbb{R} : x < y$ bedeutet nun: „Es gibt ein $c \in \mathbb{R}$, so dass für alle $d \in \mathbb{R}$ jeweils $c < d$ gilt." Diese Aussage ist offenbar falsch. Denn nehmen wir an, es gibt ein solches c. Dann ist $d = c - 1$ offenbar kleiner als c, und nicht größer. Somit ist $c < d$ nicht für alle $d \in \mathbb{R}$ erfüllt.

Die Aussage $\forall y \in \mathbb{R} : \exists x \in \mathbb{R} : x < y$ bedeutet andererseits, dass für jedes $d \in \mathbb{R}$ jeweils ein $c \in \mathbb{R}$ mit $c < d$ existiert. Diese Aussage ist wahr. Geben wir nämlich ein beliebiges $d \in \mathbb{R}$ vor, dann können wir $c = d - 1$ setzen, und die Aussage $c < d$ ist offenbar erfüllt.

Kommen wir nun zum letzten Thema dieses Kapitels, der ***vollständigen Induktion***. Wir werden die Menge $\mathbb{N} = \{1, 2, 3, ...\}$ der natürlichen Zahlen in einem späteren Kapitel als Teilmenge der reellen Zahlen definieren. Trotzdem soll an dieser Stelle bereits mit $\mathbb{N}$ gearbeitet werden. Wir setzen folgende Aussagen über die Menge $\mathbb{N}$ als bekannt voraus. Sie sind in der Literatur unter dem Namen ***Peano-Axiome*** bekannt, benannt nach dem italienischen Mathematiker *Guiseppe Peano (1858-1932)* und lauten

(P1) Es gibt ein ausgezeichnetes Element in $\mathbb{N}$, das wir mit 1 bezeichnen.
(P2) Jedes $n \in \mathbb{N}$ besitzt einen eindeutig bestimmten ***Nachfolger***, der mit $n + 1$ bezeichnet wird.
(P3) Kein Element aus $\mathbb{N}$ besitzt die 1 als Nachfolger.
(P4) Sind $m, n \in \mathbb{N}$ mit $m + 1 = n + 1$, dann folgt $m = n$.

Hinzu kommt noch das wichtige

(P5) *Induktionsprinzip:*
Sei φ ein Aussagenschema mit folgenden Eigenschaften: Für jedes $n \in \mathbb{N}$ ist $\varphi(n)$ eine sinnvolle Aussage, darüber hinaus seien $\varphi(1)$ und $\forall x \in \mathbb{N} : \varphi(x) \Rightarrow \varphi(x+1)$ *wahre* Aussagen. Dann ist auch $\forall x \in \mathbb{N} : \varphi(x)$ wahr.

Die Anwendung des Induktionsprinzips bezeichnet man als ***vollständige Induktion***, es ist eines der wichtigsten Beweisprinzipien der Mathematik. Wir werden sehen, dass in vielen Situationen die Beweise der Aussagen $\varphi(1)$ und $\forall x \in \mathbb{N} : \varphi(x) \Rightarrow \varphi(x+1)$ erheblich einfacher sind als ein direkter Beweis von $\forall x \in \mathbb{N} : \varphi(x)$.

Wie wir im nächsten Abschnitt sehen werden, kann das Induktionsprinzip zum Beispiel dafür benutzt werden, um auf den natürlichen Zahlen die Addition und die Multiplikation zu definieren, und um die aus der Schule bekannten Rechengesetze herzuleiten, zum Beispiel Assoziativ-, Kommutativ- und Distributivgesetz. Wir nehmen aber hier an, dass wir die aus der Schule bekannten Zahlbereiche schon zur Verfügung haben und betrachten als Beispiel den folgenden „Klassiker“ unter den Induktionsbeweisen.

(2.4) Satz Sei $n \in \mathbb{N}$. Dann ist die Summe der ersten n natürlichen Zahlen gegeben durch

$$1 + 2 + \ldots + n \quad = \quad \tfrac{1}{2} n(n+1).$$

Beweis: Unser Ziel besteht darin, das Induktionsprinzip auf das Aussagenschema $1 + 2 + \ldots + x = \frac{1}{2}x(x+1)$ mit dem Parameter x anzuwenden. Bezeichnen wir dieses Aussagenschema mit φ, dann müssen wir also $\varphi(1)$ und $\forall x \in \mathbb{N} : \varphi(x) \Rightarrow \varphi(x+1)$ beweisen. Die Aussage $\varphi(1)$ lautet $1 = \frac{1}{2} \cdot 1 \cdot (1+1)$. Diese Aussage ist offensichtlich wahr, denn tatsächlich gilt $\frac{1}{2} \cdot 1 \cdot (1+1) = \frac{1}{2} \cdot 1 \cdot 2 = 1$.

Nun beweisen wir $\forall x \in \mathbb{N} : \varphi(x) \Rightarrow \varphi(x+1)$. Sei dazu $n \in \mathbb{N}$ vorgegeben. Dann ist $\varphi(n) \Rightarrow \varphi(n+1)$ zu zeigen. Setzen wir dazu voraus, dass $\varphi(n)$ wahr ist. Dann gilt $1 + 2 + \ldots + n = \frac{1}{2}n(n+1)$. Diese Gleichung bleibt erhalten, wenn wir auf beiden Seiten $n+1$ addieren, es gilt also $1 + 2 + \ldots + n + (n+1) = \frac{1}{2}n(n+1) + (n+1)$. Wegen

$$\begin{aligned} \tfrac{1}{2}n(n+1) + (n+1) = \tfrac{1}{2}n(n+1) + 1 \cdot (n+1) \quad &= \quad (\tfrac{1}{2}n + 1)(n+1) \\ = \quad \tfrac{1}{2}(n+2)(n+1) = \tfrac{1}{2}(n+1)((n+1)+1) & \end{aligned}$$

erhalten wir $1+2+\ldots+n+(n+1) = \frac{1}{2}(n+1)((n+1)+1)$. Also gilt auch $\varphi(n+1)$. Damit ist insgesamt die Implikation $\varphi(n) \Rightarrow \varphi(n+1)$ bewiesen. □

In einem Induktionsbeweis über ein Aussagenschema φ bezeichnet man den Beweis von $\varphi(1)$ als ***Induktionsanfang*** und den Beweis der Implikation $\varphi(n) \Rightarrow \varphi(n+1)$ für ein beliebig vorgegebenes $n \in \mathbb{N}$ als ***Induktionsschritt***. Die Teilaussage $\varphi(n)$ nennt man dabei die ***Induktionsvoraussetzung***. Jeder Induktionsbeweis sollte so aufgeschrieben sein, dass klar zu erkennen ist, an welcher Stelle die Induktionsvoraussetzung verwendet wird. (In einem späteren Kapitel werden wir sehen, wie sich der Ausdruck $1 + 2 + \ldots + n$ mit Hilfe des Summenzeichens kompakter darstellen lässt.)

§ 3. *Relationen*

Inhaltsübersicht

Eine *Relation* auf einer Menge X ist eine Teilmenge des kartesischen Produkts $X \times X$; intuitiv kann man sich darunter eine Beziehung zwischen den Elementen der Menge vorstellen. Wir betrachten in diesem Kapitel zwei wichtige Klassen von Relationen, die *Halbordnungen* und die *Äquivalenzrelationen*. Eine Halbordnung auf X verwendet man, um die Elemente der Menge X auf irgendeine Weise zu „vergleichen". Von diesem Konzept werden wir vor allem in der Analysis Gebrauch machen. Dagegen dient eine Äquivalenzrelation auf X dient dazu, die Menge X geeignet zu zerlegen. Dies führt in erster Linie zu Anwendungen in der Algebra, auch in der Linearen Algebra.

Wichtige Begriffe und Sätze

- Relation auf einer Menge X, zwischen zwei Mengen X und Y
- Halbordnungen, Verbände und Totalordnungen
  (Beispiel: die Potenzmenge einer Menge als Verband)
- minimales und maximales Element, Minimum und Maximum, Infimum und Supremum
  (Beispiel: die Grenzen eines endlichen Intervalls als Infimum und Supremum)
- Äquivalenzrelation auf einer Menge, Äquivalenzklasse
  (Beispiel: die Kongruenzrelationen auf $\mathbb{Z}$)
- Korrespondenz zwischen Äquivalenzrelationen und Zerlegungen
  (Beispiel: die Zerlegung von $\mathbb{Z}$ in Kongruenzklassen)

(3.1) Definition Seien X und Y Mengen.

(i) Eine ***Relation*** auf X ist eine Teilmenge $R \subseteq X \times X$.
(ii) Eine Relation zwischen X und Y ist eine Teilmenge $R \subseteq X \times Y$.

Intuitiv kann man sich eine Relation R als *Beziehung* zwischen den Elemente von X und Y vorstellen. Für beliebige $x \in X$ und $y \in Y$ soll $(x, y) \in R$ genau dann gelten, wenn x und y miteinander in Beziehung stehen.

Betrachten wir als erstes Beispiel die Relation | auf der Menge $X = \{1, 2, 3, 4, 5, 6\}$ gegeben durch $|= \{ (a, b) \in X \times X \mid a \text{ ist Teiler von } b \}$. Man bezeichnet diese Relation als ***Teilerrelation***. In ausgeschriebener Form handelt es sich um die Menge

$$| \;=\; \{ (1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6) \} \;\subseteq\; X \times X.$$

Alternativ könnte man die Relation | auch in Tabellenform darstellen, wobei man für jedes Element von X eine Zeile und eine Spalte vorsieht und an der Position (x, y) genau dann ein Kreuz **X** setzt, wenn $(x, y) \in |$ gilt. Dies würde dann folgendermaßen ausehen.

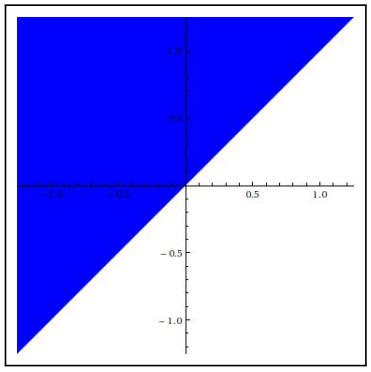
	1	2	3	4	5	6
1	X	X	X	X	X	X
2		X		X		X
3			X			X
4				X		
5					X	
6						X

Natürlich kann man die Teilerrelation auch auf der gesamten Menge $\mathbb{N}$ der natürlichen Zahlen betrachten. Da $\mathbb{N}$ aber unendlich ist, kann man die Elemente von $|$ natürlich nicht mehr einzeln angeben, weder als Aufzählung noch in Tabellenform.

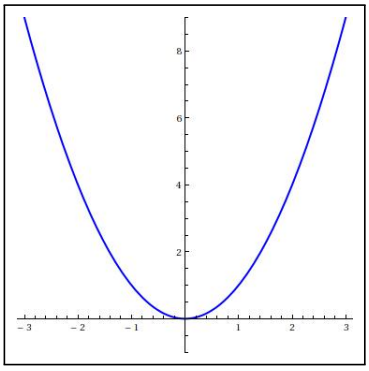
Viele Relationen auf $\mathbb{R}$ lassen sich wiederum graphisch darstellen, weil es sich dabei um nichts anderes als eine Teilmenge der Ebene $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ handelt. So könnte man etwa die Punkte, die zur Relation gehören, in der Ebene blau einzeichnen. Für die Relationen

$$R = \{(x,y) \in \mathbb{R}^2 \mid x \leq y\} \quad , \quad S = \{(x,y) \in \mathbb{R}^2 \mid y = x^2\} \quad \text{und} \quad T = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$$

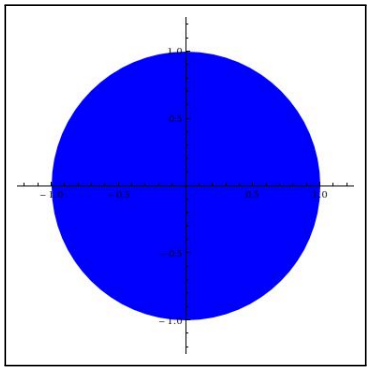
würde man zum Beispiel die folgenden Bilder erhalten.



Relation R



Relation S



Relation T

Beim Umgang mit Relationen verwendet man häufig die folgende ***Infix-Notation***: Ist R eine Relation zwischen zwei Mengen X und Y, dann schreibt man die Aussage „$(x,y) \in R$“ sehr oft in der Form „xRy“. Als Bezeichnung für Relationen werden häufig Symbole wie $\leq$, $<$, $\prec$, $\equiv$, $\cong$ usw. verwendet.

Es sei noch darauf hingewiesen, dass eine Relation $R \subseteq X \times Y$ keine bestimmte „Bedeutung“ zu haben braucht, sondern vollkommen willkürlich gewählt werden kann. So ist zum Beispiel auch $R = \{(3,7),(19,8),(2,44)\}$ eine Relation auf $\mathbb{N}$. Um allerdings zu mathematisch „interessanten“ Relationen zu kommen, beschränkt man sich auf Relationen mit bestimmten festgelegten Eigenschaften.

(3.2) Definition Sei X eine Menge. Eine Relation R auf X heißt

(i) ***reflexiv***, falls xRx für alle $x \in R$,
(ii) ***symmetrisch***, falls $xRy \Rightarrow yRx$ für alle $x, y \in R$,
(iii) ***anti-symmetrisch***, falls $xRy \wedge yRx \Rightarrow x = y$ für alle $x, y \in R$, und
(iv) ***transitiv***, falls $xRy \wedge yRz \Rightarrow xRz$ für alle $x, y, z \in R$ gilt.

Wir kommen nun zur Definition der ersten wichtigen großen Klasse von Relationen.

(3.3) Definition Sei X eine Menge.

(i) Eine ***Halbordnung*** auf X ist eine reflexive, anti-symmetrische und transitive Relation.

(ii) Bezeichnet $\leq$ eine Halbordnung auf X, so nennt man zwei Elemente $x, y \in X$ ***vergleichbar*** bezüglich $\leq$, wenn die Bedingung $(x \leq y) \vee (y \leq x)$ erfüllt ist.

(iii) Eine Halbordnung auf X wird ***Totalordnung*** genannt, wenn je zwei Elemente aus X miteinander vergleichbar sind.

Wir betrachten eine Reihe konkreter Beispiele.

(i) Die gewöhnliche $\leq$-Relation auf $\mathbb{N}$ ist eine Totalordnung, ebenso die entsprechende Relation auf jeder der Mengen $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Alle Eigenschaften einer Totalordnung (Reflexivität, Anti-Symmetrie, Transitivität, Vergleichbarkeit) lassen sich unmittelbar überprüfen.

(ii) Die oben beschriebene Teilerrelation $|$ auf der Menge $\mathbb{N}$ ist eine Halbordnung, aber keine Totalordnung.

Zuerst überprüfen wir die Halbordnungs-Eigenschaften. Für jede Zahl $n \in \mathbb{N}$ gilt $n = 1 \cdot n$, also gilt $n \mid n$. Dies zeigt, dass die Relation reflexiv ist. Zur Überprüfung der Anti-Symmetrie seien $m, n \in N$ mit $m \mid n$ und $n \mid m$ vorgegeben. Nach Definition der Teilbarkeit gibt es $k, \ell \in \mathbb{N}$ mit $n = k \cdot m$ und $m = \ell \cdot n$. Durch Einsetzen erhalten wir $n = k \cdot (\ell \cdot n) = (k \cdot \ell) \cdot n$, also $k \cdot \ell = 1$ und $m = n$. Damit ist die Anti-Symmetrie nachgewiesen. Um die Transitivität zu überprüfen, seien $m, n, p \in \mathbb{N}$ mit $m \mid n$ und $n \mid p$ vorgegeben. Es gibt $k, \ell \in \mathbb{N}$ mit $n = k \cdot m$ und $p = \ell \cdot n$. Wegen $p = \ell \cdot (k \cdot m) = (k \cdot \ell) \cdot m$ folgt $m \mid p$.

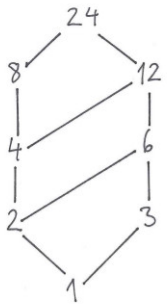
Um zu zeigen, dass $|$ keine Totalordnung ist, genügt es, zwei nicht vergleichbare Elemente $m, n \in \mathbb{N}$ anzugeben. Dies ist beispielsweise für $m = 2$ und $n = 3$ der Fall, denn weder ist 2 ein Teiler von 3, noch umgekehrt 3 ein Teiler von 2. □

(iii) Sei X eine Menge und $\mathscr{P}(X)$ die zugehörige Potenzmenge. Dann ist die „$\subseteq$“-Relation auf $\mathscr{P}(X)$ eine Halbordnung. Eine Totalordnung liegt genau dann vor, wenn X aus höchstens einem Element besteht. (Man bezeichnet diese Relation auch als ***Inklusionsrelation***.)

Wieder überprüfen wir zunächst die Halbordnungs-Eigenschaften. Für alle $A \in \mathscr{P}(X)$ gilt offenbar $A \subseteq A$, also ist die Relation $\subseteq$ reflexiv. Sind $A, B \in \mathscr{P}(X)$ mit $A \subseteq B$ und $B \subseteq A$ vorgegeben, dann folgt $A = B$. Also ist die Relation anti-symmetrisch. Für $A, B, C \in \mathscr{P}(X)$ folgt aus $A \subseteq B$ und $B \subseteq C$ offenbar $A \subseteq C$, also ist die Relation auch transitiv.

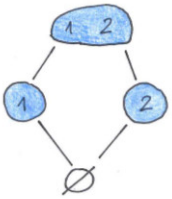
Enthält X zwei verschiedene Elemente x und y, dann ist die Relation keine Totalordnung, denn es gilt weder $\{x\} \subseteq \{y\}$ noch $\{y\} \subseteq \{x\}$. Ist $X = \emptyset$, dann gilt $\mathscr{P}(X) = \{\emptyset\}$. Es gibt also in $\mathscr{P}(X)$ gar keine zwei verschiedenen Elemente, und damit ist die Totalordnungs-Bedingung nach Definition erfüllt. Ist X einelementig, $X = \{x\}$, dann gilt $\mathscr{P}(X) = \{\emptyset, \{x\}\}$, und es gilt $\emptyset \subseteq \{x\}$. Es gibt also nur eine Möglichkeit, zwei verschiedene Elemente in $\mathscr{P}(X)$ zu wählen, und diese sind miteinander vergleichbar. Also liegt auch in diesem Fall auf $\mathscr{P}(X)$ eine Totalordnung vor. □

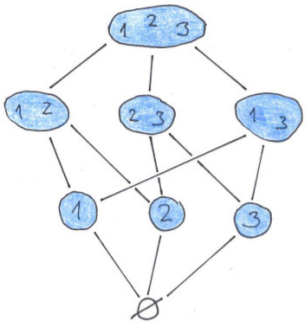
Beschränkt man sich auf eine endliche Teilmenge von $\mathbb{N}$, zum Beispiel auf die Menge der Teiler einer festen Zahl $n \in \mathbb{N}$, dann lässt sich die Teilbarkeitsrelation graphisch darstellen. Ein von unten nach oben verlaufender Weg von einem Element x zu einem Element y soll dabei bedeuten, dass $x \mid y$ erfüllt ist. Für die Fälle $n = 24$ und $n = 27$ erhält man zum Beispiel die folgenden Bilder.



Die lineare Struktur des Graphen rechts zeigt an, dass es sich bei der Relation | auf der Menge $\{1, 3, 9, 27\}$ um eine Totalordnung handelt. Die Teiler von 24 bilden aber nur eine Halbordnung.

Auch die Inklusionsrelation auf $\mathscr{P}(X)$ lässt sich für kleine Mengen X veranschaulichen. Für die Potenzmengen $\{1\}$, $\{1, 2\}$ und $\{1, 2, 3\}$ ergeben sich beispielsweise die folgenden Bilder.





Ist $\leq$ eine allgemeine Halbordnung auf einer beliebigen Menge X, dann ist es allgemein üblich, die folgenden abkürzenden Schreibweisen zu verwenden.

$x \geq y$	für die Aussage	$y \leq x$
$x < y$	für die Aussage	$x \leq y \wedge x \neq y$
$x > y$	für die Aussage	$y \leq x \wedge y \neq x$

Wir bemerken, dass sich die Bedingungen $x \leq y$ und $x > y$ (und ebenso die Bedingungen $x \geq y$ und $x < y$) gegenseitig ausschließen. Aus $x \leq y$ und $x > y$ würde nämlich insbesondere $x \leq y$ und $x \geq y$ und auf Grund der Anti-Symmetrie damit $x = y$ folgen, was zur Voraussetzung $x > y$ im Widerspruch steht.

(3.4) Definition Sei $(X, \leq)$ eine Halbordnung und $A \subseteq X$.

(i) Man nennt $a \in A$ ein ***größtes*** (bzw. ***kleinstes***) Element der Menge A, wenn $a \geq b$ (bzw. $a \leq b$) für alle $b \in A$ gilt.

(ii) Ein Element $a \in A$ wird ***maximales*** (bzw. ***minimales***) Element der Menge A genannt, wenn kein $b \in A$ mit $b > a$ (bzw. $b < a$) existiert.

Neben „größtes Element“ und „kleinstes Element“ sind auch die Bezeichnungen „Maximum“ und „Minimum“ gebräuchlich. Das Maximum einer Teilmenge $A \subseteq X$, sofern es existiert, wird mit $\max(A)$ bezeichnet, und ebenso das Minimum im Falle der Existenz mit $\min(A)$. Die soeben eingeführten Begriffe stehen in folgender Beziehung zueinander.

(3.5) Proposition Sei $(X, \leq)$ eine Halbordnung und $A \subseteq X$.

(i) Es gibt höchstens ein größtes und höchstens ein kleinstes Element in A.

(ii) Das größte (bzw. kleinste) Element von A, sofern es existiert, ist zugleich das einzige maximale (bzw. minimale) Element von A.

(iii) Ist $(X, \leq)$ eine Totalordnung, dann sind die Begriffe „größtes Element“ und „maximales Element“ (bzw. „kleinstes Element“ und „minimales Element“) gleichbedeutend.

Beweis: zu (i) Nehmen wir an, dass a und a' beides größte Elemente von A sind. Weil a größtes Element von A und $a' \in A$ ist, gilt $a \geq a'$. Weil a' größtes Element von A und $a \in A$ ist, gilt $a' \geq a$. Aus $a \geq a'$, $a' \geq a$ und der Anti-Symmetrie der Relation $\leq$ folgt $a = a'$. Genauso zeigt man, dass es höchstens ein kleinstes Element in A geben kann.

zu (ii) Wir beschränken uns auf den Beweis der Aussage für das größte Element. Sei also a das größte Element von A. Dann muss a zugleich ein maximales Element sein, denn die Existenz eines $b \in A$ mit $b > a$ würde der Definition des größten Elements widersprechen. Nehmen wir nun an, dass b ein von a verschiedenes maximales Element der Menge A ist. Dann gilt $a \geq b$ (weil a größtes Element von A ist), zugleich aber $a \neq b$ und damit insgesamt $a > b$. Aber dies widerspricht der Maximalität des Elements b.

zu (iii) Wieder beschränken wir uns auf den Beweis der Aussage für größte und maximale Elemente. Wegen Teil (ii) genügt es zu zeigen, dass im Falle einer Totalordnung jedes maximale Element zugleich größtes Element ist. Sei also a ein maximales Element, und sei $b \in A$ beliebig. Weil $\leq$ eine Totalordnung ist, muss $a \leq b$ oder $a \geq b$ und somit auch $a < b$ oder $a \geq b$ gelten. Der Fall $a < b$ würde der Maximalität von a widersprechen. Es gilt also $a \geq b$ für alle $b \in A$, und damit ist a das größte Element von A. □

Aus Teil (iii) der Proposition folgt insbesondere, dass es in Teilmengen der herkömmlichen Totalordnung $(\mathbb{R}, \leq)$ keinen Unterschied zwischen größten und maximalen bzw. kleinsten und minimalen Elementen gibt. In Halbordnungen kann es durchaus vorkommen, dass eine Teilmenge mehrere maximale oder minimale Elemente besitzt. Betrachten wir zum Beispiel in $\mathbb{N}$ mit der Teilerrelation die Teilmenge $A = \{1, 2, ..., 10\}$, so besitzt diese sogar fünf maximale Elemente, nämlich 6, 7, 8, 9 und 10. In dieser Situation kann es dann aber wegen Teil (ii) der Proposition kein größtes Element geben.

Offenbar besitzt in einer Totalordnung $(X, \leq)$ jede zweielementige Teilmenge $\{a, b\}$ ein Maximum und ein Minimum. Denn in diesem Fall gilt $a \leq b$ oder $a \geq b$. Im ersten Fall ist a das Minimum und b das Maximum, im zweite Fall ist es umgekehrt. Durch vollständige Induktion lässt sich leicht zeigen, dass jede nichtleere, endliche Teilmenge von A ein Minimum und ein Maximum besitzt.

(3.6) Definition Sei $(X, \leq)$ eine Halbordnung und $A \subseteq X$.

(i) Sei Element $s \in X$ wird ***obere Schranke*** (bzw. ***untere Schranke***) von A genannt, wenn $s \geq a$ (bzw. $s \leq a$) für alle $a \in A$ gilt.

(ii) Wir bezeichnen mit $\mathscr{S}^+(A)$ bzw. $\mathscr{S}^-(A)$ die Menge aller oberen bzw. unteren Schranken von A.

(iii) Das kleinste Element von $\mathscr{S}^+(A)$, sofern es existiert, wird das ***Supremum*** von A genannt und mit $\sup(A)$ bezeichet. Ebenso nennt man das größte Element von $\mathscr{S}^-(A)$ im Falle der Existenz das ***Infimum*** von A, und bezeichnet es mit $\inf(A)$.

Ist die Menge A nichtleer, gilt aber $\mathscr{S}^+(A) = \emptyset$, dann setzt man $\sup(A) = +\infty$. Ebenso wird $\inf(A)$ im Fall $A \neq \emptyset$ und $\mathscr{S}^-(A) = \emptyset$ auf den Wert $-\infty$ gesetzt.

Auch diese Begriffe illustrieren wir anhand eines konkreten Beispiels.

(3.7) Proposition Seien $a, b \in \mathbb{R}$ mit $a < b$ und $I = \{x \in \mathbb{R} \mid a < x < b\}$. (Eine solche Teilmenge nennt man ein endliches offenes Intervall.)

(i) Die Menge besitzt weder maximale noch minimale Elemente, also erst recht weder ein größtes noch ein kleinstes Element.

(ii) Es gilt $\mathscr{S}^+(I) = \{x \in \mathbb{R} \mid x \geq b\}$ und $\mathscr{S}^-(I) = \{x \in \mathbb{R} \mid x \leq a\}$.

(iii) Es gilt $\sup(I) = b$ und $\inf(I) = a$.

Beweis: Der Beweis beruht auf der folgenden allgemeinen Tatsache, deren Beweis wir nachliefern, sobald wir in der Vorlesung die angeordneten Körper definiert haben: Sind $c, d \in \mathbb{R}$ mit $c < d$, dann gelten für den Durchschnitt $e = \frac{1}{2}(c + d)$ der beiden Zahlen die Ungleichungen $c < e < d$.

zu (i) Nehmen wir an, dass $c \in I$ ein maximales Element von I ist. Dann gilt $a < c < b$. Setzen wir $c' = \frac{1}{2}(c+b)$, dann gilt $a < c < c' < b$ und somit $c' \in I$. Damit steht $c' > c$ aber im Widerspruch zur Maximalität von I. Genauso widerlegt man die Existenz minimaler Elemente. Dass es damit auch kein größtes oder kleinstes Element in I geben kann, folgt aus Teil (ii) von Proposition (3.5).

zu (ii) Wir beschränken uns auf den Beweis der Gleichung für $\mathscr{S}^+(I)$. Ist $x \geq b$, dann gilt insbesondere $x \geq b > c$ für alle $c \in I$. Somit ist x eine obere Schranke von I, also in $\mathscr{S}^+(I)$ enthalten. Setzen wir umgekehrt $x \in \mathscr{S}^+(I)$ voraus, und nehmen wir an, dass $x \geq b$ nicht erfüllt ist. Dann muss $x < b$ gelten. Setzen wir $a' = \max\{a, x\}$ und $c = \frac{1}{2}(a'+b)$, dann gilt $a \leq a' < c < b$ und somit $c \in I$. Aber damit steht $c > a' \geq x$ im Widerspruch zur Voraussetzung, dass x eine obere Schranke von I ist.

zu (iii) Nach Teil (ii) gilt $b \in \mathscr{S}^+(I)$ und $x \geq b$ für alle $x \in \mathscr{S}^+(I)$. Also ist b das kleinste Element von $\mathscr{S}^+(I)$, und es folgt $b = \sup(I)$. Der Beweis der Gleichung $a = \inf(I)$ läuft analog. □

Allgemein gilt zwischen Maximum und Supremum bzw. Minimum und Infimum die folgende Beziehung.

(3.8) Satz Sei $(X, \leq)$ eine Halbordnung und $A \subseteq X$.

(i) Das Maximum (bzw. Minimum) von A, sofern es existiert, ist zugleich das Supremum (bzw. Infimum) von A.

(ii) Existiert das Supremum (bzw. Infimum) von A, und ist es in A enthalten, so ist es zugleich das Maximum (bzw. Minimum) von A.

Beweis: zu (i) Es genügt, die Aussage für das Maximum zu beweisen, denn für das Minimum läuft der Beweis analog. Sei also $a = \max(A)$. Aus der Definition des größten Elements folgt unmittelbar, dass $a \in A$ und $a \in \mathscr{S}^+(A)$ gilt. Ein $s \in \mathscr{S}^+(A)$ mit $s < a$ kann es nicht geben, denn wegen $a \in A$ könnte ein solches s keine oberen Schranke von A sein. Also ist a zugleich das Supremum von A.

zu (ii) Auch hier beschränken wir uns wieder auf den Fall des Supremums. Gilt $s = \sup(A)$, dann gilt insbesondere $s \in \mathscr{S}^+(A)$ und somit $s \geq a$ für alle $a \in A$. Ist a zugleich in A enthalten, dann handelt es sich nach Definition um das größte Element der Menge A. □

Betrachten wir zum Beispiel in der Totalordnung $(\mathbb{R}, \leq)$ eine Teilmenge der Form $I = [a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ mit $a, b \in \mathbb{R}, a < b$ (ein sog. endliches abgeschlossenes Intervall), dann gilt $\max(I) = \sup(I) = b$ und $\min(I) = \inf(I) = a$.

(3.9) Definition Eine Halbordnung $(X, \leq)$, in der jede zweielementige Teilmenge $\{a, b\} \subseteq X$ ein Infimum und ein Supremum besitzt, bezeichnet man als ***Verband***. Man verwendet die Bezeichnungen $a \vee b = \sup\{a, b\}$ und $a \wedge b = \inf\{a, b\}$.

Auch hier betrachten wir eine Reihe von Beispielen.

(i) Jede Totalordnung $(X, \leq)$ ist ein Verband, mit $a \vee b = \max\{a, b\}$ und $a \wedge b = \min\{a, b\}$ für alle $a, b \in X$.

(ii) Die natürliche Zahlen mit der Teilerrelation bilden einen Verband. Für alle $m, n \in \mathbb{N}$ gilt jeweils $m \vee n = \text{kgV}(m, n)$ und $m \wedge n = \text{ggT}(m, n)$.

(iii) Ist X eine beliebige Menge, dann ist $(\mathscr{P}(X), \subseteq)$ ein Verband. Für alle $A, B \in \mathscr{P}(X)$ gilt jeweils $A \vee B = A \cup B$ und $A \wedge B = A \cap B$.

(iv) Schränkt man die Teilerrelation auf $\mathbb{N}$ auf die Teilmenge $X = \{1, 2, ..., 10\}$ ein, so erhält man eine Halbordnung, die kein Verband mehr ist. Beispielsweise besitzt die Teilmenge $\{7, 8\}$ keine obere Schranke in X, somit erst recht keine kleinste obere Schranke, also kein Supremum.

(v) Ebenso geht die Verbandsstruktur verloren, wenn man die Teilerrelation auf die Menge $\mathbb{N} \setminus \{56\}$ einschränkt. Es existieren dann zwar mehrere minimale obere Schranken von $\{7, 8\}$, zum Beispiel 112 oder 168, aber keine kleinste obere Schranke.

Wir kommen nun zu einer weiteren wichtigen Klasse von Relationen, den Äquivalenzrelationen.

(3.10) Definition Eine Relation $\sim$ auf einer Menge X wird ***Äquivalenzrelation*** genannt, wenn sie reflexiv, symmetrisch und transitiv ist.

Wir betrachten ein erstes Beispiel für eine Äquivalenzrelation. Sei X eine endliche Menge und $\mathscr{P}(X)$ die Potenzmenge von X. Dann ist durch $A \sim B \Leftrightarrow |A| = |B|$ eine Äquivalenzrelation auf $\mathscr{P}(X)$ definiert, wobei $|A|$ jeweils die Anzahl der Elemente von A bezeichnet. Diese Relation ist reflexiv, denn für alle $A \in \mathscr{P}(X)$ gilt $|A| = |A|$ und somit $A \sim A$. Sie ist symmetrisch, denn für alle $A, B \in \mathscr{P}(X)$ mit $A \sim B$ gilt $|A| = |B|$, damit auch $|B| = |A|$, und folglich $B \sim A$. Die Relation ist auch transitiv. Sind nämlich $A, B, C \in \mathscr{P}(X)$ mit $A \sim B$ und $B \sim C$ vorgegeben, dann gilt $|A| = |B|$ und $|B| = |C|$, damit auch $|A| = |C|$ und somit $A \sim C$.

Für jede natürliche Zahl n erhält man auf folgende Weise eine Relation auf der Menge $\mathbb{Z}$ der natürlichen Zahlen.

(3.11) Definition Für jedes $n \in \mathbb{N}$ sei die Relation $\equiv_n$ auf $\mathbb{Z}$ definiert durch die Festlegung

$$a \equiv_n b \quad \Leftrightarrow \quad n \mid (a - b) \quad \forall\, a, b \in \mathbb{Z}.$$

Hierbei steht $\mid$ für die Teilerrelation; die Schreibweise $n \mid (a - b)$ bedeutet also, dass n ein Teiler der ganzen Zahl $a - b$ ist. Die Relation $\equiv_n$ wird als ***Kongruenzrelation modulo*** n bezeichnet. Zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $a \equiv_n b$ werden auch ***kongruent*** modulo n genannt.

An Stelle von $a \equiv_n b$ sind auch die Schreibweisen $a \equiv b \mod n$ und $a \equiv b(n)$ gebräuchlich.

(3.12) Satz Für jedes $n \in \mathbb{N}$ ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis: Für alle $a \in \mathbb{Z}$ gilt offenbar $a \equiv_n a$, denn n ist stets ein Teiler von $a - a = 0$. Also ist die Relation $\equiv_n$ reflexiv. Sind $a, b \in \mathbb{Z}$ mit $a \equiv_n b$, dann gilt nach Definition $n \mid (a - b)$. Es gibt also ein $k \in \mathbb{Z}$ mit $a - b = kn$. Aber dann gilt auch $b - a = (-k)n$, also $n \mid (b - a)$, und damit auch $b \equiv_n a$. Dies zeigt, dass $\equiv_n$ eine symmetrische Relation ist.

Seien nun $a, b, c \in \mathbb{Z}$ mit $a \equiv_n b$ und $b \equiv_n c$ vorgegeben. Dann gilt $n \mid (a - b)$ und $n \mid (b - c)$, es gibt also $k, \ell \in \mathbb{Z}$ mit $a - b = kn$ und $b - c = \ell n$. Es folgt $a - c = (a - b) + (b - c) = (k + \ell)n$, also $n \mid (a - c)$ und somit $a \equiv_n c$. Dies zeigt, dass $\equiv_n$ auch transitiv ist. Insgesamt handelt es sich bei $\equiv_n$ also tatsächlich um eine Äquivalenzrelation. □

Die intuitive Bedeutung der Äquivalenzrelationen auf einer Menge wird durch den folgenden Begriff besser verständlich.

(3.13) Definition Als ***Zerlegung*** einer Menge X bezeichnen wir eine Teilmenge $\mathscr{Z} \subseteq \mathscr{P}(X)$ mit den Eigenschaften $A \neq \emptyset$ für alle $A \in \mathscr{Z}$, dass für jedes $x \in X$ ein $A \in \mathscr{Z}$ mit $x \in A$ existiert, und dass für alle $A, B \in \mathscr{Z}$ aus $A \cap B \neq \emptyset$ jeweils $A = B$ folgt.

Die zweite Bedingung besagt also, dass X die Vereinigung aller Elemente aus $\mathscr{Z}$ ist, und die dritte, dass je zwei verschiedene Mengen aus X disjunkt sind. Ist zum Beispiel $X = \{1, 2, 3, 4, 5\}$, dann ist sowohl $\{\{1, 2, 3\}, \{4, 5\}\}$ als auch $\{\{1\}, \{5\}, \{2, 3, 4\}\}$ eine Zerlegung von X. Dagegen ist $\{\{1, 2, 3\}, \{3, 4, 5\}\}$ oder $\{\{1, 3\}, \{2, 5\}\}$ oder auch $\{\emptyset, \{1, 2\}, \{3, 4\}, \{5\}\}$ keine Zerlegung von X.

(3.14) Definition Sei X eine Menge, $\sim$ eine Äquivalenzrelation auf X und $x \in X$. Dann nennt man die Teilmenge

$$[x]_\sim \quad = \quad \{y \in X \mid x \sim y$$

die ***Äquivalenzklasse*** des Elements x bezüglich $\sim$.

(3.15) Proposition Sei X eine Menge und $\sim$ eine Äquivalenzrelation auf X. Für alle $x, y \in X$ folgt aus $y \in [x]_\sim$ stets $[x]_\sim = [y]_\sim$. Die Äquivalenzklassen von $\sim$ bilden also eine Zerlegung der Menge X.

Beweis: Seien $x, y \in X$ mit $y \in [x]_\sim$ vorgegeben. Nach Definition $[x]_\sim$ gilt dann $x \sim y$. Zum Beweis von $[y]_\sim \subseteq [x]_\sim$ sei nun $z \in [y]_\sim$ vorgegeben. Dann gilt $y \sim z$. Aus $x \sim y$ und $y \sim z$ folgt $x \sim z$, auf Grund der Transitivität. Daraus wiederum folgt $z \in [x]_\sim$. Zum Beweis von $[x]_\sim \subseteq [y]_\sim$ sei nun $z \in [x]_\sim$. Dann gilt $x \sim z$. Aus $x \sim y$ und der Symmetrie von $\sim$ folgt $y \sim x$. Aus $y \sim x$ und $x \sim z$ folgt $y \sim z$. Damit ist $z \in [y]_\sim$ nachgewiesen. Insgesamt haben wir damit $[x]_\sim = [y]_\sim$ gezeigt.

Für jedes $x \in X$ enthält die Äquivalenzklasse $[x]_\sim$ auf jeden Fall das Element x, denn auf Grund der Reflexivität gilt $x \sim x$ und damit $x \in [x]_\sim$. Sämtliche Äquivalenzklassen sind also nicht leer, und jedes $x \in X$ ist in mindestens einer Äquivalenzklasse enthalten. Seien nun $x, y \in X$ mit $[x]_\sim \cap [y]_\sim \neq \emptyset$ vorgegeben. Dann existiert ein $z \in [x]_\sim \cap [y]_\sim$. Wie wir oben gezeigt haben, folgt daraus $[x]_\sim = [z]_\sim = [y]_\sim$. Damit haben wir für die Menge der Äquivalenzklassen die Eigenschaften einer Zerlegung nachgewiesen. □

Umgekehrt lässt sich jeder Zerlegung eine Äquivalenzrelation zuordnen.

(3.16) Proposition Sei X eine Menge und $\mathscr{Z}$ eine Zerlegung von X. Dann ist durch die Festlegung

$$x \sim_{\mathscr{Z}} y \quad \Leftrightarrow \quad \exists A \in \mathscr{Z} : (x \in A) \wedge (y \in A) \quad \forall\, x, y \in X$$

eine Äquivalenzrelation auf X definiert.

Beweis: Für jedes $x \in X$ existiert nach Definition der Zerlegungen ein $A \in \mathscr{Z}$ mit $x \in A$. Die Aussage $(x \in A) \wedge (x \in A)$ ist somit erfüllt, es gilt also $x \sim_{\mathscr{Z}} x$. Dies zeigt, dass $\sim_{\mathscr{Z}}$ reflexiv ist. Seien nun $x, y \in X$ mit $x \sim_{\mathscr{Z}} y$ vorgegeben. Dann existiert ein $A \in \mathscr{Z}$ mit $(x \in A) \wedge (y \in A)$. Es gilt dann auch $(y \in A) \wedge (x \in A)$; daraus folgt $y \sim_{\mathscr{Z}} x$. Die Relation $\sim_{\mathscr{Z}}$ ist also auch symmetrisch. Seien schließlich $x, y, z \in X$ mit $x \sim_{\mathscr{Z}} y$ und $y \sim_{\mathscr{Z}} z$. Dann gibt es Menge $A, B \in \mathscr{Z}$ mit $(x \in A) \wedge (y \in A)$ und $(y \in B) \wedge (z \in B)$. Aus $y \in A \cap B$ und den Eigenschaften einer Zerlegung folgt $A = B$. Damit ist dann auch $(x \in A) \wedge (z \in A)$ erfüllt, und wir erhalten $x \sim_{\mathscr{Z}} z$. Dies zeigt, dass $\sim_{\mathscr{Z}}$ auch transitiv ist. Insgesamt ist durch $\sim_{\mathscr{Z}}$ also eine Äquivalenzrelation gegeben. □

(3.17) Proposition Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist die Äquivalenzklasse $[a]_n$ von a bezüglich der Relation $\equiv_n$ gegeben durch die Menge $a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$. Man nennt $[a]_n$ auch die ***Kongruenz-*** oder ***Restklasse*** von a modulo n.

Beweis: Zum Beweis der Inklusion $[a]_n \subseteq a + n\mathbb{Z}$ sei $c \in [a]_n$ vorgegeben. Dann gilt $a \equiv_n c$, also $n \mid (a - c)$. Es existiert also ein $k \in \mathbb{Z}$ mit $a - c = nk$. Daraus wiederum folgt $c = a + n(-k) \in a + n\mathbb{Z}$. Zum Nachweis von $a + n\mathbb{Z} \subseteq [a]_n$ sei $c \in a + n\mathbb{Z}$. Dann gilt $c = a + nk$ für ein $k \in \mathbb{Z}$. Es folgt $n(-k) = a - c$, also $n \mid (a - c)$ und somit $a \equiv_n c$. Dies wiederum ist gleichbedeutend mit $c \in [a]_n$. □

Nach Proposition (3.15) bilden die Kongrenzklassen modulo einer Zahl $n \in \mathbb{N}$ also eine Zerlegung von $\mathbb{Z}$. Beispielsweise wird $\mathbb{Z}$ durch die Kongruenzklassen modulo 2 in die geraden und die ungeraden Zahlen zerlegt. Durch die Kongruenz modulo 3 erhalten wir eine Zerlegung $\mathbb{Z} = A \cup B \cup C$ von $\mathbb{Z}$ in drei Teilmengen, nämlich $A = 3\mathbb{Z} = \{..., -6, -3, 0, 3, 6, 9, ...\}$, $B = 1 + 3\mathbb{Z} = \{..., -5, -2, 1, 4, 7, 10, ...\}$ und $C = 2 + 3\mathbb{Z} = \{..., -4, -1, 2, 5, 8, 11, ...\}$.

Wenden wir Proposition (3.15) auf die Relation $\equiv_n$ an, so erhalten wir

(3.18) Folgerung Für alle $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ gilt die Äquivalenz

$$a \equiv_n b \quad \Leftrightarrow \quad b \in a + n\mathbb{Z} \quad \Leftrightarrow \quad a + n\mathbb{Z} = b + n\mathbb{Z}.$$

Beispielsweise gelten in $\mathbb{Z}/5\mathbb{Z}$ die Gleichungen $2+5\mathbb{Z} = 7+5\mathbb{Z} = 12+5\mathbb{Z} = -3+5\mathbb{Z}$.

Aus der Schulmathematik ist das Konzept der ***Division mit Rest*** bekannt: Ist $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ vorgegeben, so findet man stets Elemente $q, r \in \mathbb{Z}$, so dass $a = qn + r$ und $0 \leq r < n$ erfüllt ist.

> **(3.19) Proposition** Für jedes $n \in \mathbb{N}$ sei $\mathbb{Z}/n\mathbb{Z}$ die Menge der Kongruenzklassen modulo n. Dann besitzt $\mathbb{Z}/n\mathbb{Z}$ genau n verschiedene Elemente, nämlich $r + n\mathbb{Z}$ mit $0 \leq r < n$.

Beweis: Zunächst zeigen wir, dass jede Kongruenzklasse mit einem dieser n Elemente übereinstimmt. Sei $a + n\mathbb{Z}$ vorgegeben, mit $a \in \mathbb{Z}$. Division mit Rest liefert $q, r \in \mathbb{Z}$ mit $a = qn + r$ und $0 \leq r < n$. Wegen $a - r = qn$ gilt $n \mid (a-r)$ und somit $a \equiv_n r$. Wir erhalten $a + n\mathbb{Z} = [a]_n = [r]_n = r + n\mathbb{Z}$, nach Proposition (3.18). Um zu zeigen, dass die angegebenen Elemente alle verschieden sind, seien $r, s \in \mathbb{Z}$ mit $0 \leq r, s < n$ vorgegeben. Nehmen wir an, es gilt $r + n\mathbb{Z} = s + n\mathbb{Z}$; zu zeigen ist, dass dann $r = s$ folgt. Aus $[r]_n = [s]_n$ folgt $s \in [r]_n$ und somit $r \equiv_n s$, also $n \mid (r-s)$. Aber wegen $0 \leq r, s < n$ ist $|r-s| < n$; somit ist $n \mid (r-s)$ nur möglich, wenn $r = s$ ist. □

Statt mit $[a]_n$ oder $a + n\mathbb{Z}$ bezeichnet man die Restklasse von a auch mit $\bar{a}$, sofern n aus dem Kontext heraus bekannt ist. Nach Proposition (3.19) ist die Menge $\mathbb{Z}/7\mathbb{Z}$ beispielsweise gegeben durch

$$\mathbb{Z}/7\mathbb{Z} \quad = \quad \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}.$$

§ 4. *Abbildungen und Mächtigkeiten*

Inhaltsübersicht

Eine *Abbildung* $f : X \to Y$ zwischen zwei Mengen X und Y ist gegenüber einer beliebigen Relation dadurch ausgezeichnet, dass für jedes x aus X, dem *Definitionsbereich* von f, ein eindeutig bestimmtes y aus Y, dem *Wertebereich* von f, existiert, das dann mit $f(x)$ bezeichnet wird. Man umschreibt dies mit der Formulierung, dass die Abbildung f jedem $x \in X$ ein Element $y \in Y$ „zuordnet“.

Im Allgemeinen können mehrere $x \in X$ demselben $y \in Y$ zugeordnet werden; ist dies nicht der Fall, nennt man die Abbildung *injektiv*. Ist jedes $y \in Y$ das Ziel von mindestens einer Zuordnung, wird also der gesamte Definitionsbereich durch f „abgedeckt“, spricht man von einer surjektiven Abbildung. Abbildungen, die injektiv und surjektiv sind, werden bijektiv oder auch „1-zu-1“-Abbildungen genannt. Für sie existiert eine sog. *Umkehrabbildung* in Gegenrichtung $f^{-1} : Y \to X$, die dadurch gekennzeichnet ist, dass für alle $x \in X$ und $y \in Y$ die Äquivalenz

$$y = f(x) \quad \Leftrightarrow \quad x = f^{-1}(y)$$

erfüllt ist. Mit anderen Worten, die Gleichung $y = f(x)$ kann nach x „aufgelöst“ werden.

Mit Hilfe der bijektiven Abbildungen kann auch die *Mächtigkeit* einer Menge definiert werden. Ist die Menge *endlich*, so handelt es sich dabei einfach um die Anzahl der Elemente. Mit Hilfe der vollständigen Induktion aus § 2 leiten wir eine Reihe von Rechenregeln für die Mächtigkeit endlicher Mengen her. Außerdem behandeln wir einige Grundlagen zu *unendlichen* Mengen, indem wir beispielsweise durch das Konzept der Abzählbarkeit verschiedene Stufen der Unendlichkeit unterscheiden.

Wichtige Begriffe und Sätze

- Abbildung zwischen zwei Mengen
- Definitions- und Wertebereich einer Abbildung
- Einschränkung und Komposition von Abbildungen
- Bildmengen und Urbildmengen
- injektive, surjektive und bijektive Abbildungen, Umkehrabbildung
- endliche und unendliche Mengen, Mächtigkeit einer endlichen Menge
- Rechenregeln für die Mächtigkeit endlicher Mengen
  (für Vereinigung, Durchschnitt, kartesischem Produkt und Potenzmenge)
- Binomialkoeffizienten
- Gleichmächtigkeit; höchstens abzählbare, abzählbar unendliche und überabzählbare Mengen
- Familie von Elementen, Indexmenge, Folge
- Abzählbarkeitskriterien, Abzählbarkeit von $\mathbb{Q}$ als Folgerung

(4.1) Definition Seien X, Y Mengen. Eine Relation f zwischen X und Y wird ***Abbildung*** genannt, wenn für jedes $x \in X$ genau ein $y \in Y$ mit $(x, y) \in f$ existiert. In Formelschreibweise:

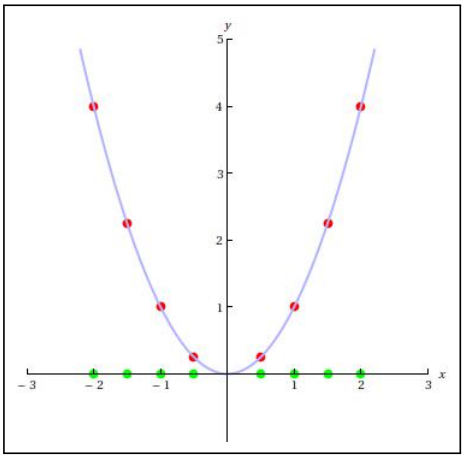
(i) $\forall x \in X : \exists y \in Y : (x, y) \in f$
(ii) $\forall x \in X : \forall y, y' \in Y : (x, y) \in f \wedge (x, y') \in f \Rightarrow y = y'$.

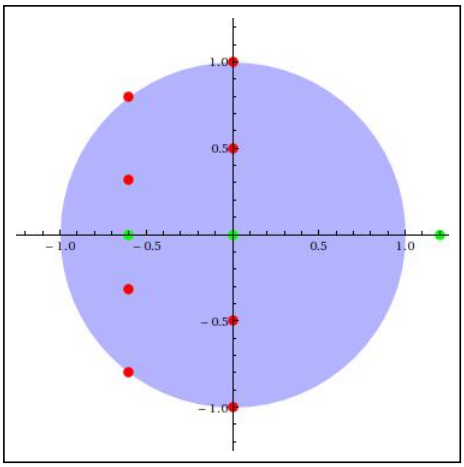
Dabei nennt man X den ***Definitions-*** und Y den ***Wertebereich*** der Abbildung.

Für gegebenes $x \in X$ bezeichnet man das eindeutig bestimmte $y \in Y$ mit der Eigenschaft $(x, y) \in R$ mit $f(x)$ und nennt es das ***Bild*** von x unter R.

Die Notation $f : X \to Y$ drückt aus, dass f eine Abbildung von X nach Y, also eine Abbildung mit Definitionsbereich X und Wertebereich Y ist. Die Schreibweise $x \mapsto y$ ist gleichbedeutend mit $y = f(x)$; man sagt auch, dass f dem Element x das Element y ***zuordnet***.

Ob eine Relation f auf der Menge $\mathbb{R}$ der reellen Zahlen eine Abbildung ist, ob also für jedes $x \in X$ genau ein $y \in Y$ mit $(x, y) \in f$ existiert, lässt sich gut an der graphischen Darstellung von f erkennen.





Zum Beispiel ist $S = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$ eine Abbildung, denn für jeden x-Wert (grün) gibt es genau einen zugehörigen Punkt $(x, y) \in S$ (rot), also genau ein $y \in \mathbb{R}$ mit $(x, y) \in S$. Dagegen ist $T = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ keine Abbildung, denn für einige x-Werte (zum Beispiel für $x = 1.2$) gibt es gar kein y mit $(x, y) \in T$. Für andere x-Werte (zum Beispiel $x = 0$) gibt es dagegen gleich mehrere, sogar unendlich viele, zugehörige y-Werte, was bei einer Abbildung ebenfalls nicht zulässig ist.

Als nächstes definieren wir zwei wichtige Operationen: die Einschränkung und die Komposition von Funktionen. Die erste Operation läuft darauf hinaus, dass man den Definitionsbereich einer Funktion f verkleinert.

(4.2) Proposition Sind X, Y Mengen, $f \subseteq X \times Y$ eine Abbildung und $U \subseteq X$. Dann ist durch $f|_U = \{(x, y) \in f \mid x \in U\} = f \cap (U \times Y)$ eine Abbildung von U nach Y definiert. Wir bezeichnen sie als die ***Einschränkung*** von f auf die Teilmenge U.

Beweis: Um zu zeigen, dass $g = f \cap (U \times Y)$ eine Abbildung $U \to Y$ ist, sei $x \in U$ vorgegeben. Weil f eine Abbildung ist, existiert jedenfalls ein $y \in Y$ mit $(x,y) \in f$. Wegen $(x,y) \in U \times Y$ ist (x,y) auch in g enthalten. Seien nun $x \in U$ und $y, y' \in Y$ mit $(x,y) \in g$ und $(x,y') \in g$. Dann gilt auch $(x,y) \in f$ und $(x,y') \in f$. Weil f eine Abbildung ist, folgt $y = y'$. Insgesamt haben wir damit für g beide in Definition (4.1) angegeben Bedingungen verifiziert. □

(4.3) Proposition Seien X, Y, Z Mengen und $f : X \to Y$, $g : Y \to Z$ zwei Abbildungen. Dann ist $g \circ f = \{ (x,z) \in X \times Z \mid \exists y \in Y : (x,y) \in f \wedge (y,z) \in g \}$ eine Abbildung von X nach Z, und es gilt $(g \circ f)(x) = g(f(x))$ für alle $x \in X$. Man nennt $g \circ f$ die ***Komposition*** der Abbildungen f und g.

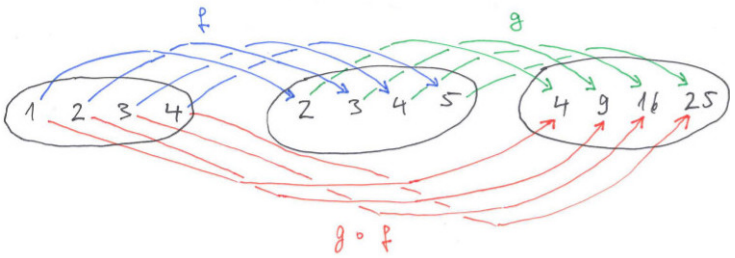
Beweis: Sei $x \in X$ vorgegeben. Setzen wir $y = f(x) \in Y$, dann gilt $(x,y) \in f$ und $(y, g(y)) \in g$ nach Definition der Bildelemente $f(x)$ und $g(y)$. Dies zeigt, dass das Paar (x,z) mit $z = g(y) = g(f(x))$ in $g \circ f$ enthalten ist.

Nehmen wir nun an, $z' \in Z$ ist ein weiteres Element mit $(x,z') \in g \circ f$ ist. Dann exitiert nach Definition ein $y' \in Y$ mit $(x,y') \in f$ und $(y',z') \in g$. Weil f eine Abbildung ist, gilt $y = f(x) = y'$, und aus der Abbildungs-Eigenschaft von g und der Voraussetzung $(y,z) \in g$ und $(y',z') = (y,z') \in g$ folgt $z = z'$. Insgesamt ist damit gezeigt, dass $g \circ f$ eine Abbildung ist, und dass $(g \circ f)(x) = g(f(x))$ gilt. □

Die Komposition $g \circ f$ entsteht also einfach dadurch, dass f in g „eingesetzt“ wird. Später werden wir häufig mit Abbildungen auf den reellen Zahlen arbeiten, zum Beispiel $f : \mathbb{R} \to \mathbb{R}, x \mapsto x+1$ oder $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. Die Komposition von f und g ergibt in diesem Fall also

$$(g \circ f)(x) \quad = \quad g(f(x)) \quad = \quad g(x+1) \quad = \quad (x+1)^2 \qquad \text{für alle } x \in \mathbb{R}.$$

Man kann sich das Zusammenspiel von f, g und $g \circ f$ durch folgendes Diagramm veranschaulichen.



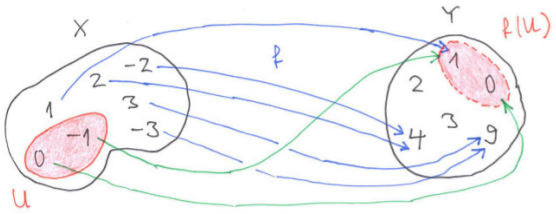
Eine Abbildung wirkt nicht nur auf einzelne Elemente, sondern auch auf Teilmengen ihres Definitions- und Wertebereichs. Die folgenden beiden Konzepte werden später bei der Formulierung der Ketten- und der Umkehrregel in der Analysis eine wichtige Rolle spielen.

(4.4) Definition Seien $f : X \to Y$ eine Abbildung und $U \subseteq X$, $V \subseteq Y$.

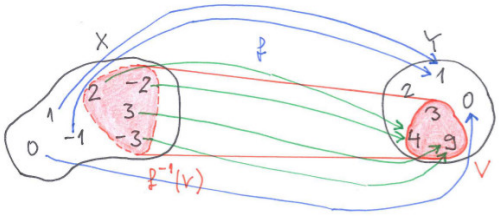
(i) Die Teilmenge $f(U) = \{ f(x) \mid x \in U \} \subseteq Y$ wird die ***Bildmenge*** von U unter der Abbildung f genannt. Es handelt sich um die Elemente von Y, die man dadurch erhält, dass man f auf ein Element aus U anwendet.

(ii) Die Teilmenge $f^{-1}(V) = \{ x \in X \mid f(x) \in V \} \subseteq X$ wird die ***Urbildmenge*** von V unter f genannt. Sie besteht aus genau den Elementen von X, die nach V abgebildet werden.

Wir betrachten als Beispiel die Abbildung $f : X \to Y$ zwischen den Mengen $X = \{-3,-2,-1,0,1,2,3\}$ und $Y = \{0,1,2,3,4,9\}$ gegeben durch $f(x) = x^2$ für alle $x \in X$. Seien $U \subseteq X$ und $V \subseteq Y$ gegeben durch $U = \{-1,0\}$ und $V = \{3,4,9\}$.



Bestimmung der Bildmenge $f(U)$



Bestimmung der Urbildmenge $f^{-1}(V)$

Nach Definition besteht $f(U)$ aus allen Elementen, die man durch Quadrierung von Elementen aus $U = \{-1,0\}$ erhält, also $(-1)^2 = 1$ und $0^2 = 0$. Die Urbildmenge $f^{-1}(V)$ enthält alle Elemente $x \in X$, deren Quadrat in $V = \{3,4,9\}$ liegt. Wegen $(-2)^2 = 2^2 = 4$ und $(-3)^2 = 3^2 = 9$ sind dies die Zahlen $-3,-2,2,3$.

(4.5) Proposition Sei $f : X \to Y$ eine Abbildung, $U \subseteq X$ und $V \subseteq Y$. Dann gilt

$$\text{(i) } f(f^{-1}(V)) \subseteq V \qquad \text{(ii) } U \subseteq f^{-1}(f(U))$$

Beweis: zu (i) Ist $y \in f(f^{-1}(V))$, dann gibt es nach Definition der Bildmenge ein $x \in f^{-1}(V)$ mit $y = f(x)$. Aus $x \in f^{-1}(V)$ folgt $f(x) \in V$, insgesamt also $y = f(x) \in V$.

zu (ii) Sei $x \in U$ vorgegeben. Dann gilt $f(x) \in f(U)$. Das Element x wird also auf ein Element aus $f(U)$ abgebildet. Nach Definition der Urbildmenge folgt daraus unmittelbar $x \in f^{-1}(f(U))$. □

Anhand passender Beispiele werden wir uns in den Übungen klarmachen, dass die beiden Inklusionen in der Proposition im Allgemeinen keine Gleichungen sind, es braucht also weder $f(f^{-1}(V)) = V$ noch $f^{-1}(f(U)) = U$ zu gelten. Die Operationen „Bildmenge“ und „Urbildmenge“ heben sich also nicht immer gegenseitig auf.

(4.6) Definition Sei $f : X \to Y$ eine Abbildung.

(i) Wenn für alle x_1, x_2 aus $f(x_1) = f(x_2)$ jeweils $x_1 = x_2$ folgt, dann nennt man die Abbildung ***injektiv***.

(ii) Wenn es für jedes $y \in Y$ ein $x \in X$ mit $f(x) = y$ gibt, dann wird f ***surjektiv*** genannt.

(iii) Eine Abbildung f, die sowohl injektiv als auch surjektiv ist, bezeichnet man als ***bijektiv***.

Die drei soeben definierten Eigenschaften von Abbildungen lassen sich auch mit Hilfe der Urbildmengen charakterisieren. Eine Abbildung ist genau dann injektiv, wenn $f^{-1}(\{y\})$ für jedes $y \in Y$ ***höchstens*** ein Element enthält. Zum

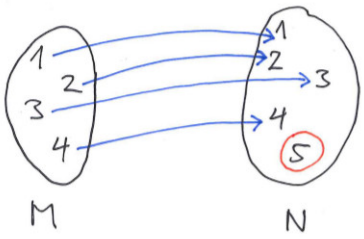
Beweis setzen wir die Injektivität voraus und geben uns ein beliebiges $y \in Y$ vor. Sind nun $x_1, x_2 \in f^{-1}(\{y\})$, dann gilt $f(x_1) = y = f(x_2)$, und aus der Injektivität folgt $x_1 = x_2$. Dies zeigt, dass $f^{-1}(\{y\})$ keine zwei verschiedenen Elemente enthält. Setzen wir umgekehrt voraus, dass $f^{-1}(\{y\})$ für jedes $y \in Y$ höchstens ein Element enthält, und seien $x_1, x_2 \in X$ mit $f(x_1) = f(x_2)$. Setzen wir $y = f(x_1)$, dann sind x_1, x_2 beides Elemente von $f^{-1}(\{y\})$. Weil aber $f^{-1}(\{y\})$ nach Voraussetzung höchstens einelementig ist, muss $x_1 = x_2$ gelten. Damit ist die Injektivität bewiesen.

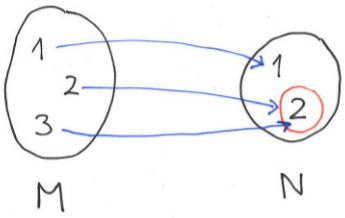
Auf ähnliche Weise zeigt man, dass die Surjektivität gleichbedeutend damit ist, dass $f^{-1}(\{y\})$ für jedes $y \in Y$ aus ***mindestens*** einem Element besteht. Ebenfalls zur Surjektivität äquivalent ist die Gleichung $f(X) = Y$, denn nach Definition besteht $f(X)$ genau aus den Elementen $y \in Y$, für die ein $x \in X$ mit $f(x) = y$ existiert.

Aus den Feststellungen zur Injektivität und Surjektivität ergibt sich unmittelbar, dass eine Abbildung $f : X \to Y$ genau dann bijektiv ist, wenn die Menge $f^{-1}(\{y\})$ für jedes $y \in Y$ jeweils ***genau*** ein Element enthält.

Wieder schauen wir uns die neuen Begriffe anhand einer Reihe von Beispielen an.

(i) Sei $M = \{1,2,3,4\}$ und $N = \{1,2,3,4,5\}$. Die Abbildung $f : M \to N$ mit $f(a) = a$ für $1 \leq a \leq 4$ ist injektiv. Dafür müssen wir zeigen, dass die Aussage $\forall x_1, x_2 \in M : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ gültig ist. Seien also $a_1, a_2 \in M$ mit $f(a_1) = f(a_2)$ vorgegeben. Dann gilt $a_1 = f(a_1) = f(a_2) = a_2$, also ist die Implikation $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ tatsächlich für alle $a_1, a_2 \in M$ erfüllt. Die Abbildung ist aber nicht surjektiv, denn es gibt kein $a \in M$ mit $f(a) = 5$.





(ii) Sei $M = \{1,2,3\}$ und $N = \{1,2\}$. Dann ist die Abbildung $f : M \to N$ gegeben durch $1 \mapsto 1$, $2 \mapsto 2$, $3 \mapsto 2$ zwar surjektiv, aber nicht injektiv. Zwar gibt es für jedes $b \in N = \{1,2\}$ ein $a \in M$ mit $f(a) = b$ ($f(1) = 1$, $f(2) = 2$), aber die Implikation $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ ist beispielsweise für $a_1 = 2$, $a_2 = 3$ nicht erfüllt.

(iii) Die Abbildung $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ ist weder injektiv noch surjektiv. Die Implikation $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ ist beispielsweise für $a_1 = -1$, $a_2 = 1$ nicht erfüllt, und es gibt kein $a \in \mathbb{R}$ mit $f(a) = -1$.

(iv) Die Abbildung $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$ ist bijektiv. Zunächst zeigen wir die Injektivität. Sind $a_1, a_2 \in \mathbb{R}$ beliebig vorgegeben, dann gelten die Implikationen

$$f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 + 1 = a_2 + 1 \quad \Rightarrow \quad a_1 = a_2 \quad ,$$

also ist $\forall x_1, x_2 \in \mathbb{R} : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ wahr. Ist $b \in \mathbb{R}$ beliebig vorgegeben, dann setzen wir $a = b - 1$ und erhalten $f(a) = f(b-1) = (b-1) + 1 = b$. Für jedes $b \in \mathbb{R}$ gibt es also ein $a \in \mathbb{R}$ mit $f(a) = b$, d.h. die Aussage $\forall y \in \mathbb{R} : \exists x \in \mathbb{R} : f(x) = y$ ist erfüllt.

(v) Für jede Menge X nennt man $\mathrm{id}_X : X \to X,\ x \mapsto x$ die ***identische Abbildung*** oder ***Identität*** auf der Menge X. Sie ist offenbar ebenfalls bijektiv.

(4.7) Satz Die Komposition zweier injektiver (bzw. surjektiver, bijektiver) Abbildungen ist injektiv (bzw. surjektiv, bijektiv).

Beweis: Seien X, Y, Z Mengen und $f : X \to Y$, $g : Y \to Z$ Abbildungen. Zunächst setzen wir voraus, dass f und g injektiv sind und beweisen die Injektivität von $g \circ f$. Seien dazu $x_1, x_2 \in X$ mit $(g \circ f)(x_1) = (g \circ f)(x_2)$ vorgegeben. Nach Definition der Komposition $\circ$ ist dies gleichbedeutend mit $g(f(x_1)) = g(f(x_2))$. Weil g injektiv ist, folgt daraus $f(x_1) = f(x_2)$. Weil auch f injektiv ist, erhalten wir $x_1 = x_2$. Damit ist die Injektivität von $g \circ f$ bewiesen.

Nun setzen wir voraus, das f und g surjektiv sind, und beweisen die Surjektivität von $g \circ f$. Sei $z \in Z$ vorgegeben. Zu zeigen ist, dass ein $x \in X$ mit $(g \circ f)(x) = z$ existiert. Weil g surjektiv ist, gibt es ein $y \in Y$ mit $g(y) = z$. Weil auch f surjektiv ist, existiert ein $x \in X$ mit $f(x) = y$. Insgesamt gilt also $(g \circ f)(x) = g(f(x)) = g(y) = z$. Damit ist die Surjektivität von $g \circ f$ bewiesen.

Setzen wir nun voraus, dass f und g bijektiv sind. Dann sind f und g insbesondere injektiv, und wie wir im ersten Absatz gezeigt haben, folgt daraus die Injektivität von $g \circ f$. Die Abbildung f und g sind auch beide surjektiv. Wie im zweiten Absatz gezeigt, folgt daraus die Surjektivität von $g \circ f$. Als injektive und surjektive Abbildung ist $g \circ f$ also insgesamt bijektiv. □

Oft werden wir auch die folgende Charakterisierung injektiver, surjektiver und bijektiver Abbildungen verwenden.

(4.8) Satz Seien X, Y nichtleere Mengen und $f : X \to Y$ eine Abbildung.

(i) Es ist f genau dann injektiv, wenn eine Abbildung $g : Y \to X$ mit $g \circ f = \mathrm{id}_X$ existiert.

(ii) Sie ist genau dann surjektiv, wenn es ein $g : Y \to X$ mit $f \circ g = \mathrm{id}_Y$ gibt.

(iii) Sie ist bijektiv genau dann, wenn ein $g : Y \to X$ mit den Eigenschaften $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ existiert. Die Abbildung g mit diesen beiden Eigenschaften ist dann eindeutig bestimmt. Man nennt sie die ***Umkehrabbildung*** von f und bezeichnet sie mit f^{-1}.

Beweis: zu (i) „⇒“ Sei $f : X \to Y$ eine injektive Abbildung und $x_0 \in X$ ein beliebig gewähltes Element. Gibt es für $y \in Y$ ein Urbild von $x \in X$, so ist dieses eindeutig bestimmt, und wir definieren $g(y) = x$. Besitzt y dagegen kein Urbild, dann setzen wir $g(y) = x_0$. Ist nun $x \in X$ und $y = f(x)$, dann ist x das eindeutig bestimmte Urbild von y, und nach Definition von g gilt $(g \circ f)(x) = g(f(x)) = g(y) = x = \mathrm{id}_X(x)$. Also besitzt g die gewünschte Eigenschaft $g \circ f = \mathrm{id}_X$.

„⇐“ Sei $f : X \to Y$ eine Abbildung und $g : Y \to X$ mit $g \circ f = \mathrm{id}_X$. Wir müssen zeigen, dass f injektiv ist. Seien dazu $x_1, x_2 \in X$ Elemente mit $f(x_1) = f(x_2)$. Dann gilt

$$x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2.$$

Also ist f tatsächlich injektiv.

zu (ii) „⇒“ Sei $f : X \to Y$ eine surjektive Abbildung. Für jedes $y \in Y$ wählen wir ein beliebiges Urbild $x_y \in f^{-1}(\{y\})$ und definieren $g(y) = x_y$. Für jedes $y \in Y$ gilt dann $(f \circ g)(y) = f(g(y)) = f(x_y) = y = \mathrm{id}_Y(y)$, also besitzt g die gewünschte Eigenschaft.

„⇐“ Sei $f : X \to Y$ eine Abbildung und $g : Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Um die Surjektivität von f nachzuweisen, müssen wir zeigen, dass es für jedes $y \in Y$ ein $x \in X$ mit $f(x) = y$ existiert. Ein solches Element x ist durch $x = g(y)$ gegeben, denn es gilt $f(g(y)) = (f \circ g)(y) = \mathrm{id}_Y(y) = y$.

zu (iii) „⇐“ Sei $f : X \to Y$ eine Abbildung und $g : Y \to X$ mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$. Dann ist f nach (i) injektiv, nach (ii) surjektiv, insgesamt also bijektiv.

„⇒“ Sei $f : X \to Y$ eine bijektive Abbildung. Dann gibt es nach (i) eine Abbildung $g_1 : Y \to X$ mit $g_1 \circ f = \mathrm{id}_X$ und nach (ii) eine Abbildung $g_2 : Y \to X$ mit $f \circ g_2 = \mathrm{id}_Y$. Wir zeigen, dass $g_1 = g_2$ gilt. Für gegebenes $y \in Y$ erhalten wir auf Grund unserer Voraussetzungen

$$g_1(y) = g_1(\mathrm{id}_Y(y)) = g_1((f \circ g_2)(y)) = g_1(f(g_2(y))) = (g_1 \circ f)(g_2(y)) = \mathrm{id}_X(g_2(y)) = g_2(y).$$

Also gilt tatsächlich $g_1 = g_2$, d.h. $g = g_1$ ist eine Abbildung mit den beiden gewünschten Eigenschaften. Sei nun $h : Y \to X$ eine weitere Abbildung mit $h \circ f = \mathrm{id}_X$ und $f \circ h = \mathrm{id}_Y$. Aus $g \circ f = \mathrm{id}_X$ und $f \circ h = \mathrm{id}_Y$ folgt dann, wie soeben gezeigt, die Identität $g = h$. Also ist g eindeutig bestimmt. □

Im Folgenden bezeichnet $M_n = \{1, 2, 3, ..., n\}$ für jedes $n \in \mathbb{N}$ die Menge der natürlichen Zahlen von 1 bis n. Außerdem setzen wir $M_0 = \varnothing$.

(4.9) Definition Sei $n \in \mathbb{N}_0$. Man sagt, eine Menge A besteht aus n Elementen oder hat die ***Mächtigkeit*** n, falls eine bijektive Abbildung $\varphi : M_n \to A$ existiert. Wir schreiben dann $|A| = n$.

Darauf aufbauend können wir definieren

(4.10) Definition Eine Menge A ist ***endlich***, falls ein $n \in \mathbb{N}_0$ mit $|A| = n$ existiert. Ansonsten bezeichnen wir die Menge A als ***unendlich***.

Wir müssen sicherstellen, dass unsere Definition der Mächtigkeit einer endlichen Menge eindeutig ist, dass also nicht $|A| = m$ und $|A| = n$ für zwei verschiedene Zahlen $m, n \in \mathbb{N}_0$ gilt. Dies erfordert ein wenig Aufwand.

(4.11) Lemma Sei A eine beliebige Menge, und seien $a, b \in A$ zwei verschiedene Elemente. Dann ist die Abbildung $\tau_{ab} : A \to A$ gegeben durch

$$\tau_{ab}(x) \quad = \quad \begin{cases} b & \text{falls } x = a \\ a & \text{falls } x = b \\ x & \text{sonst} \end{cases} \qquad \text{eine Bijektion.}$$

(Die Abbildung τ_{ab} vertauscht die beiden Elemente a und b miteinander, alle übrigen Elemente werden auf sich selbst abgebildet.)

Beweis: Zunächst beweisen wir die Surjektivität. Sei $y \in A$ vorgegeben. Ist $y = a$, dann gilt $\tau_{ab}(b) = y$. Im Fall $y = b$ ist $\tau_{ab}(a) = y$, und im verbleibenden Fall $y \notin \{a, b\}$ gilt $\tau_{ab}(y) = y$. Also liegt y auf jeden Fall in der Bildmenge der Abbildung τ_{ab}. Zum Nachweis der Injektivität seien $u, v \in A$ mit $\tau_{ab}(u) = \tau_{ab}(v)$ vorgegeben. Ist $\tau_{ab}(u) = \tau_{ab}(v) = a$, dann muss $u = v = b$ gelten. Im Fall $\tau_{ab}(u) = \tau_{ab}(v) = b$ gilt $u = v = a$. Ist schließlich $\tau_{ab}(u)$ nicht in $\{a, b\}$ enthalten, dann folgt $u = \tau_{ab}(u) = \tau_{ab}(v) = v$. □

Für den Beweis der nächsten Aussage bemerken wir vorweg, dass die vollständige Induktion aus § 2 statt über $\mathbb{N}$ auch über $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ geführt werden kann, wenn man den Induktionsanfang bei $n = 0$ ansetzt.

(4.12) Proposition Sei $n \in \mathbb{N}_0$. Dann ist jede injektive Abbildung $M_n \to M_n$ auch surjektiv.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über $n \in \mathbb{N}_0$. Die einzige Abbildung von M_0 nach M_0 ist wegen $M_0 = \varnothing$ die leere Menge, und diese ist nach Definition sowohl injektiv als auch surjektiv (also bijektiv). Damit ist die Aussage für $n = 0$ bewiesen.

Sei nun $n \in \mathbb{N}_0$ vorgegeben und $\psi : M_{n+1} \to M_{n+1}$ eine injektive Abbildung. Zu zeigen ist, dass ψ auch surjektiv ist. Zunächst betrachten wir den Fall, dass $\psi(n+1) = n+1$ ist. Dann gilt $\psi(M_n) \subseteq M_n$. Denn wäre dies nicht der Fall, dann gäbe es ein $k \in M_n$ mit $\psi(k) = n+1$, was aber wegen $\psi(k) = n+1 = \psi(n+1)$ im Widerspruch zur Injektivität von ψ stehen würde. Mit ψ ist auch die Einschränkung $\psi|_{M_n}$ injektiv. Es handelt sich also um eine injektive Abbildung $M_n \to M_n$; laut Induktions- voraussetzung ist diese auch surjektiv. Daraus folgt $\psi(M_n) = M_n$. Wegen $\psi(n+1) = n+1$ ist damit insgesamt gezeigt, dass jedes Element in M_{n+1} von ψ getroffen wird, die Abbildung ψ also surjektiv ist. Damit ist die Betrachtung dieses Falls abgeschlossen.

Betrachten wir nun den Fall, dass $\psi(n+1) = k$ mit $k \in M_n$ gilt. Weil $\tau_{k,n+1}$ nach Lemma (4.11) bijektiv ist, ist nach Satz (4.7) mit ψ auch die Abbildung $\tilde{\psi} = \tau_{k,n+1} \circ \psi$ injektiv; darüber hinaus gilt

$$\tilde{\psi}(n+1) \quad = \quad (\tau_{k,n+1} \circ \psi)(n+1) \quad = \quad \tau_{k,n+1}(\psi(n+1)) \quad = \quad \tau_{k,n+1}(k) \quad = \quad n+1.$$

Wie im vorherigen Absatz gezeigt, folgt daraus, dass $\tilde{\psi}$ surjektiv ist. Aber damit ist auch $\psi = \tau_{k,n+1}^{-1} \circ \tilde{\psi}$ surjektiv. Damit ist der Induktionsschritt abgeschlossen. □

Aus Proposition (4.12) folgt nun in der Tat die Eindeutigkeit von $|A|$ für eine endliche Menge A. Denn nehmen wir an, es gäbe $m, n \in \mathbb{N}_0$ mit $m < n$ und der Eigenschaft, dass sowohl $|A| = m$ als auch $|A| = n$ erfüllt ist. Dann gäbe es Bijektionen $\varphi : M_m \to A$ und $\psi : M_n \to A$. Nach Satz (4.7) wäre dann durch $\alpha = \varphi^{-1} \circ \psi$ eine bijektive Abbildung $M_n \to M_m$ gegeben. Wegen $M_m \subseteq M_n$ können wir α als injektive Abbildung $M_n \to M_n$ auffassen. Wegen $\alpha(M_n) = M_m \subsetneq M_n$ ist α als Abbildung $M_n \to M_n$ jedoch nicht surjektiv. Wir haben also eine injektive, nicht surjektive Abbildung $M_n \to M_n$ konstruiert. Aber die Existenz einer solchen Abbildung ist nach Proposition (4.12) ausgeschlossen. Also war unsere Annahme falsch, es kann nicht gleichzeitig $|A| = m$ und $|A| = n$ gelten.

(4.13) Proposition Zwei endliche Mengen A, B haben genau dann dieselbe Mächtigkeit, wenn eine Bijektion $A \to B$ existiert.

Beweis: „⇒“ Sei $n \in \mathbb{N}_0$ mit $|A| = n = |B|$. Die Gleichung $|A| = n$ bedeutet, dass eine bijektive Abbildung $\varphi : M_n \to A$ existiert. Aus $|B| = n$ folgt, dass es eine Bijektion $\psi : M_n \to B$ gibt. Nach Satz (4.7) ist durch $\psi \circ \varphi^{-1}$ eine Bijektion von A nach B gegeben.

„⇐“ Weil A endlich ist, gibt es ein $n \in \mathbb{N}_0$ und eine Bijektion $\varphi : M_n \to A$. Außerdem existiert nach Voraussetzung eine Bijektion $\psi : A \to B$. Somit ist $\psi \circ \varphi$ eine Bijektion $M_n \to B$, und daraus folgt $|B| = n = |A|$. □

(4.14) Proposition Eine Menge A ist genau dann unendlich, wenn eine injektive Abbildung $\mathbb{N} \to A$ existiert.

Beweis: „⇐“ Nehmen wir an, es gibt eine injektive Abbildung $\psi : \mathbb{N} \to A$, obwohl A endlich ist. Setzen wir $|A| = n$, dann existiert also eine bijektive Abbildung $\varphi : M_n \to A$. Durch Einschränkung von ψ auf M_{n+1} erhalten wir eine injektive Abbildung $M_{n+1} \to A$. Durch $\alpha = \varphi^{-1} \circ (\psi|_{M_{n+1}})$ ist dann eine injektive Abbildung $M_{n+1} \to M_n$ gegeben. Aufgefasst als Abbildung $M_{n+1} \to M_{n+1}$ ist diese injektiv, aber nicht surjektiv wegen $\alpha(M_{n+1}) = M_n \subsetneq M_{n+1}$. Da nach Proposition (4.12) eine solche Abbildung nicht existiert, war unsere Annahme falsch. Wenn eine injektive Abbildung $\psi : \mathbb{N} \to A$ existiert, muss A also unendlich sein.

„⇒“ Nun setzen wir voraus, dass A unendlich ist. Wir konstruieren eine Abbildung $\psi : \mathbb{N} \to A$, indem wir die Bilder $\psi(n)$ der Reihe nach definieren. Zunächst wählen wir ein beliebiges Element $a \in A$ und setzen $\psi(1) = a$. Diese Abbildung ist offenbar injektiv. Sei nun $n \in \mathbb{N}$, und nehmen wir an, dass ψ auf der Teilmenge $M_n \subseteq \mathbb{N}$ bereits definiert und dort injektiv ist. Wäre $\psi(M_n) = A$, dann hätten wir eine Bijektion zwischen M_n und A. Die Menge A wäre dann endlich, im Widerspruch zur Annahme.

So aber können wir ein neues Element $a \in A \setminus \psi(M_n)$ wählen und $\psi(n+1) = a$ setzen. Dann ist ψ auf M_{n+1} weiterhin injektiv, denn wegen der Injektivität von $\psi|_{M_n}$ ist $\psi(k) = \psi(\ell)$ für $k < \ell$ und $k, \ell \in M_n$ ausgeschlossen. Wegen $\psi(n+1) = a \notin \psi(M_n)$ ist $k \in M_n$ und $\ell = n+1$ ebenfalls unmöglich. Wir erhalten so eine Abbildung ψ, die auf ganz $\mathbb{N}$ definiert ist. Auch diese ist injektiv. Wäre nämlich $\psi(k) = \psi(\ell)$ für zwei $k, \ell \in \mathbb{N}$ mit $k < \ell$, dann würde sich ein Widerspruch zur Injektivität von $\psi|_{M_\ell}$ ergeben. □

(4.15) Satz *(Rechenregeln für Mächtigkeiten)*

(i) Sind A und B endliche ***disjunkte*** Mengen, ist also $A \cap B = \emptyset$, dann gilt $|A \cup B| = |A| + |B|$.

(ii) Ist B endlich und $A \subseteq B$, dann gilt $|A| \leq |B|$ und $|B \setminus A| = |B| - |A|$.

(iii) Sind A und B beliebige endliche Mengen, dann gilt $|A \cup B| = |A| + |B| - |A \cap B|$ und $|A \times B| = |A| \cdot |B|$.

(iv) Für jede endliche Menge A gilt $|\mathscr{P}(A)| = 2^{|A|}$.

Ist A eine endliche Menge, dann ist also $\mathscr{P}(A)$ und jede Teilmenge von A endlich.

Beweis: zu (i) Sei $m = |A|$ und $n = |B|$. Dann gibt es Bijektionen $\varphi : M_m \to A$ und $\psi : M_n \to B$. Wir definieren nun eine Abbildung $\alpha : M_{m+n} \to A \cup B$ durch $\alpha(k) = \varphi(k)$ für $1 \leq k \leq m$ und $\alpha(k) = \psi(k-m)$ für $m+1 \leq k \leq n$. Wenn wir zeigen können, dass α bijektiv ist, dann folgt daraus $|A \cup B| = m + n = |A| + |B|$.

Zum Nachweis der Injektivität seien $k, \ell \in M_{m+n}$ mit $\alpha(k) = \alpha(\ell)$ vorgegeben. Ist $k \in M_m$, dann muss auch $\ell \in M_m$ gelten, denn ansonsten wäre $\alpha(k) = \alpha(\ell)$ ein Element von $A \cap B$, was wegen $A \cap B = \emptyset$ ausgeschlossen ist. Nach Definition der Abbildung α folgt daraus $\varphi(k) = \alpha(k) = \alpha(\ell) = \varphi(\ell)$, und weil φ injektiv ist, erhalten wir $k = \ell$. Ist $k > m$, dann folgt wegen $A \cap B = \emptyset$ ebenso $\ell > m$. Wir erhalten $\alpha(k) = \psi(k-m) = \psi(\ell - m) = \alpha(\ell)$ und wiederum $k = \ell$, diesmal auf Grund der Injektivität von ψ.

Zum Nachweis der Surjektivität sei $x \in A \cup B$ vorgegeben. Dann gilt $x \in A$ oder $x \in B$. Ist $x \in A$, dann gibt es ein $k \in M_m$ mit $\varphi(k) = x$. Daraus folgt $\alpha(k) = x$. Gilt dagegen $x \in B$, so existiert ein $k \in M_n$ mit $\psi(k) = x$, und wir erhalten $\alpha(k+m) = x$. Damit ist die Surjektivität bewiesen, insgesamt ist α also bijektiv.

zu (ii) Sei $n = |B|$. Zum Beweis von $|A| \leq n$ nehmen wir an, dass A unendlich ist oder zumindest $|A| \geq n+1$ gilt. Im ersten Fall gibt es nach Proposition (4.14) eine injektive Abbildung $\mathbb{N} \to A$, im zweiten eine bijektive Abbildung $M_r \to A$ für ein $r \geq n+1$. In beiden Fällen können wir die Abbildung zu einer injektiven Abbildung $M_{n+1} \to A$ einschränken, die wir wegen $A \subseteq B$ auch als injektive Abbildung $\varphi : M_{n+1} \to B$ betrachten können. Wegen $|B| = n$ gibt es nun eine Bijektion $\psi : M_n \to B$. Durch $\psi^{-1} \circ \varphi$ ist dann eine injektive Abbildung $M_{n+1} \to M_n$ definiert. Fassen wir diese als Abbildung $\alpha : M_{n+1} \to M_{n+1}$ auf, so ist α zwar injektiv, wegen $\alpha(M_{n+1}) = M_n \subsetneq M_{n+1}$ aber nicht surjektiv. Die Existenz einer solchen Abbildung ist durch Proposition (4.12) ausgeschlossen. Also war unsere Annahme falsch, und $|A| \leq n$ ist bewiesen. Weil die Menge B disjunkt in A und $B \setminus A$ zerlegt werden kann, gilt nach Teil (i) $|B| = |A| + |B \setminus A|$, also $|B \setminus A| = |B| - |A|$.

zu (iii) Zum Beweis der ersten Gleichung zerlegen wir $|A \cup B|$ disjunkt in die Teilmengen $A \cap B$, $A \setminus (A \cap B)$ und $B \setminus (A \cap B)$. Durch Anwendung von (i) und (ii) erhalten wir

$$\begin{aligned} |A \cup B| &= |A \cap B| + |A \setminus (A \cap B)| + |B \setminus (A \cap B)| = |A \cap B| + (|A| - |A \cap B|) + (|B| - |A \cap B|) \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

Die Gleichung $|A \times B| = |A| \cdot |B|$ beweisen wir durch vollständige Induktion über $n = |B|$. Ist $n = 0$, dann gilt $B = \varnothing$ und $A \times B = \varnothing$, also $|A \times B| = 0 = |A| \cdot 0 = |A| \cdot |B|$. Ist $n = 1$, dann gilt $B = \{b\}$ für ein $b \in B$. Wir bemerken, dass durch $A \to A \times B$, $a \mapsto (a, b)$ eine Bijektion gegeben ist. Denn aus $(a_1, b) = (a_2, b)$ folgt $a_1 = a_2$, also ist die Abbildung injektiv. Andererseits hat jedes Element in $A \times B$ die Form (a, b) für ein $a \in A$, stimmt also mit dem Bild von a überein. Daraus folgt die Surjektivität. Insgesamt ist die Abbildung bijektiv. Mit Proposition (4.13) erhalten wir $|A \times B| = |A| = |A| \cdot |B|$.

Sei nun $n \in \mathbb{N}$ vorgegeben, und setzen wir die Aussage für dieses n voraus. Sei $|B| = n+1$, $b \in B$ ein beliebig gewähltes Element und $B' = B \setminus \{b\}$. Nach (i) gilt $|B'| = |B| - 1 = n$, und die Induktionsvoraussetzung liefert $|A \times B'| = |A| \cdot n$. Weil $A \times B$ sich disjunkt in die Teilmengen $A \times B'$ und $A \times \{b\}$ zerlegen lässt, gilt

$$|A \times B| \quad = \quad |A \times B'| + |A \times \{b\}| \quad = \quad |A| \cdot n + |A| \quad = \quad |A|(n+1) \quad = \quad |A| \cdot |B|.$$

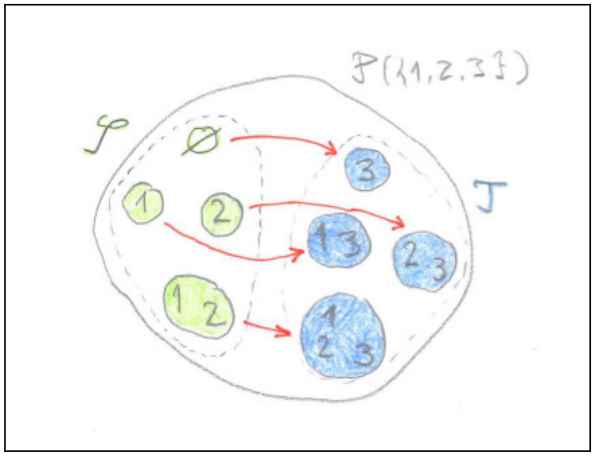
zu (iv) Der Beweis erfolgt durch vollständige Induktion über $n = |A|$. Ist $n = 0$, dann gilt $A = \varnothing$. Die leere Menge besitzt nur eine Teilmenge, nämlich $\varnothing$. Es gilt also $\mathscr{P}(A) = \{\varnothing\}$ und somit $|\mathscr{P}(A)| = 1 = 2^0$. Sei nun $n \in \mathbb{N}_0$, und setzen wir die Aussage für n voraus. Sei nun A eine $(n+1)$-elementige Menge. Zu zeigen ist $|\mathscr{P}(A)| = 2^{n+1}$. Dazu wählen wir ein beliebiges Element $a \in A$ und setzen $A' = A \setminus \{a\}$. Dann gilt $|A'| = n$, und nach Induktionsvoraussetzung gilt $|\mathscr{P}(A')| = 2^n$. Wir betrachten nun die disjunkte Zerlegung $\mathscr{P}(A) = \mathscr{S} \cup \mathscr{T}$ mit

$$\mathscr{S} \quad = \quad \{B \in \mathscr{P}(A) \mid a \notin B\} \qquad \text{und} \qquad \mathscr{T} \quad = \quad \{B \in \mathscr{P}(A) \mid a \in B\}.$$

Nach Definition gilt $\mathscr{S} = \mathscr{P}(A')$, denn die Teilmengen von A' sind genau die Teilmengen $B \subseteq A$ mit $a \notin B$. Zwischen den Mengen $\mathscr{S}$ und $\mathscr{T}$ ist durch $\phi : \mathscr{S} \to \mathscr{T}$, $B \mapsto B \cup \{a\}$ eine Bijektion gegeben, denn $\psi : \mathscr{T} \to \mathscr{S}$, $B \mapsto B \setminus \{a\}$ ist offenbar die Umkehrabbildung von ϕ. Nach Proposition (4.13) folgt daraus $|\mathscr{S}| = |\mathscr{T}|$. Wir erhalten nun

$$|\mathscr{P}(A)| \quad = \quad |\mathscr{S}| + |\mathscr{T}| \quad = \quad 2|\mathscr{S}| \quad = \quad 2|\mathscr{P}(A')| \quad = \quad 2 \cdot 2^n \quad = \quad 2^{n+1}.$$

Damit ist der Induktionsschritt abgeschlossen. □



zum Induktionsschritt im Beweis von (4.7) (iv)

(4.16) Definition Für jede Menge B und jedes $k \in \mathbb{N}_0$ sei $\mathscr{P}_k(B)$ jeweils die Anzahl der k-elementigen Teilmengen von B, also

$$\mathscr{P}_k(B) \quad = \quad \left\{ A \in \mathscr{P}(B) \;\middle|\; |A| = k \right\}.$$

Für alle $k, n \in \mathbb{N}_0$ definieren wir $\binom{n}{k} = |\mathscr{P}_k(M_n)|$ und bezeichnen diese Zahl als den ***Binomialkoeffizienten*** von n über k.

Beispielsweise ist $\binom{5}{3} = 10$, denn $M_5 = \{1,2,3,4,5\}$ hat genau zehn dreielementige Teilmengen, nämlich

$$\{1,2,3\}\ ,\ \{1,2,4\}\ ,\ \{1,2,5\}\ ,\ \{1,3,4\}\ ,\ \{1,3,5\}\ ,\ \{1,4,5\}\ ,\ \{2,3,4\}\ ,\ \{2,3,5\}\ ,\ \{2,4,5\}\ ,\ \{3,4,5\}.$$

Einige Binomialkoeffizienten lassen sich direkt angeben. Für alle $k, n \in \mathbb{N}_0$ gilt

$$\binom{n}{0} = 1 \quad , \quad \binom{n}{1} = n \quad \text{und} \quad \binom{n}{k} = \binom{n}{n-k} \quad \text{falls } k \leq n, \quad \text{außerdem} \quad \binom{n}{k} = 0 \text{ falls } k > n.$$

Die Gleichung $\binom{n}{0} = 1$ ergibt sich aus der Feststellung, dass M_n nur eine nullelementige Teilmenge besitzt, nämlich die leere Menge. Für $n \in \mathbb{N}_0$ mit $n \geq 1$ sind die einelementigen Teilmengen von M_n offenbar genau die Mengen $\{1\}$, $\{2\}$, ..., $\{n\}$, daraus folgt $\binom{n}{n} = 1$. Sind $k, n \in \mathbb{N}_0$ mit $k > n$, dann gibt es nach Satz (4.15) (i) keine k-elementigen Teilmengen von $|M_n|$. Daraus folgt $\binom{n}{k} = 0$ für $k > n$.

Die Gleichung $\binom{n}{k} = \binom{n}{n-k}$ ist für $k \leq n$ ergibt sich durch folgende Überlegung: Ist $A \subseteq M_n$ eine k-elementige Teilmenge, dann ist $M_n \setminus A$ nach Satz (4.15) (ii) eine $n-k$ elementige Teilmenge. Durch $\Phi : A \mapsto M_n \setminus A$ ist also eine Abbildung $\mathscr{P}_k(M_n) \to \mathscr{P}_{n-k}(M_n)$ gegeben. Diese besitzt $\mathscr{P}_{n-k}(M_n) \to \mathscr{P}_k(M_n)$, $B \mapsto M_n \setminus B$ als Umkehrabbildung. Denn wegen $n-(n-k) = k$ ist $M_n \setminus B$ für jedes $B \in \mathscr{P}_{n-k}(M_n)$ in $\mathscr{P}_k(M_n)$ enthalten, und wegen $M_n \setminus (M_n \setminus A) = A$, $M_n \setminus (M_n \setminus B) = B$ für alle $A \in \mathscr{P}_k(M_n)$ und $B \in \mathscr{P}_{n-k}(M_n)$ sind die beiden Abbildungen tatsächlich zueinander invers.

Die folgenden beiden Aussagen ermöglichen die Berechnung beliebiger Binomialkoeffizienten.

(4.17) Proposition Seien $k, n \in \mathbb{N}_0$, wobei $k \geq 1$ ist. Dann gilt

$$\binom{n+1}{k} \quad = \quad \binom{n}{k} + \binom{n}{k-1} \quad .$$

Beweis: Wir betrachten die disjunkte Zerlegung von $\mathscr{P}_k(M_{n+1}) = \mathscr{S} \cup \mathscr{T}$ in die Teilmengen

$$\mathscr{S} \quad = \quad \left\{ A \in \mathscr{P}_k(M_{n+1}) \;\middle|\; n+1 \in A \right\} \qquad \text{und} \qquad \mathscr{T} \quad = \quad \left\{ A \in \mathscr{P}_k(M_{n+1}) \;\middle|\; n+1 \notin A \right\} \quad ,$$

wobei $\mathscr{T} = \mathscr{P}_k(M_n)$ ist. Offenbar handelt es sich bei $\phi : \mathscr{P}_{k-1}(M_n) \to \mathscr{S}$, $A \mapsto A \cup \{n+1\}$ um eine Bijektion, denn $\psi : \mathscr{S} \to \mathscr{P}_{k-1}(M_n)$, $B \mapsto B \setminus \{n+1\}$ ist eine Umkehrabbildung von ϕ. Daraus folgt $|\mathscr{P}_{k-1}(M_n)| = |\mathscr{S}|$, und insgesamt erhalten wir $\binom{n+1}{k} = |\mathscr{P}_k(M_{n+1})| = |\mathscr{S}| + |\mathscr{T}| = |\mathscr{P}_{k-1}(M_n)| + |\mathscr{P}_k(M_n)| = \binom{n}{k-1} + \binom{n}{k}$. □

Aus dieser Formel ergibt sich als Berechnungsschema das sogenannte *Pascalsche Dreieck*. Ist $\binom{n}{\ell}$ für jedes $\ell \in \mathbb{N}_0$ bereits bekannt, dann lässt sich der Wert $\binom{n+}{k}$ dadurch berechnen, dass man die im Dreieck unmittelbar darüber stehenden Werte $\binom{n}{k-1}$ und $\binom{n}{k}$ einfach addiert.

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & &
\end{array}
\qquad\qquad
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & \mathbf{2} & & \mathbf{1} & & & & \\
 & 1 & & 3 & & \mathbf{3} & & 1 & & &
\end{array}$$

Um eine explizite, nicht-rekursive Formel für die Binomialkoeffizienten anzugeben, benötigen wir die sogenannte ***Fakultätsfunktion***. Es handelt sich dabei um eine Abbildung $\mathbb{N}_0 \to \mathbb{N}$, $n \mapsto n!$, die rekursiv definiert ist durch

$$0! \;=\; 1 \qquad \text{und} \qquad (n+1)! \;=\; (n+1)\cdot n! \qquad\qquad \text{für alle} \quad n \in \mathbb{N}_0.$$

Es gilt also $1! = 1 \cdot 0! = 1$, $2! = 2 \cdot 1! = 2$, $3! = 3 \cdot 2! = 6$, $4! = 4 \cdot 3! = 24$, $5! = 5 \cdot 4! = 120$ usw. Insgesamt handelt es sich um eine sehr schnell wachsende Funktion. Zum Beispiel ist die Fakultät von 30 gegeben durch $30! = 265.252.859.812.191.058.636.308.480.000.000$, das sind immerhin schon 33 Dezimalstellen.

(4.18) Satz Für alle $k, n \in \mathbb{N}_0$ mit $k \le n$ gilt

$$\binom{n}{k} \;=\; \frac{n!}{k!(n-k)!} \quad .$$

Beweis: Wir beweisen die Aussage durch vollständige Induktion über $n \in \mathbb{N}_0$, jeweils für alle $k \in \mathbb{N}_0$ mit $k \le n$. Für $n = k = 0$ folgt die Gleichung aus $\binom{0}{0} = 1 = \frac{0!}{0!\cdot 0!}$ erfüllt. Sei nun $n \in \mathbb{N}_0$ beliebig vorgegeben, und setzen wir die Gleichung für dieses n und alle $k \in \mathbb{N}_0$ mit $k \le n$ voraus. Unter dieser Voraussetzung beweisen wir die Gleichung für $n+1$ und $1 \le k \le n+1$. Ist $k = 0$, so gilt $\binom{n+1}{0} = 1 = \frac{(n+1)!}{0!(n+1)!}$. Für $1 \le k \le n$ folgt die Gleichung mit Hilfe von Proposition (4.17) aus der Rechnung

$$\binom{n+1}{k} \;=\; \binom{n}{k} + \binom{n}{k-1} \;=\; \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \;=$$

$$\frac{n!(n-k+1)}{k!(n-k)!(n-k+1)} + \frac{n!k}{k(k-1)!(n-k+1)!} \;=\; \frac{n!((n-k+1)+k)}{k!(n-k+1)!} \;=\; \frac{(n+1)!}{k!(n+1-k)!}.$$

Der einzige verbleibende Fall ist $k = n+1$. Weil M_{n+1} die einzige $(n+1)$-elementige Menge von M_{n+1} ist, gilt $\binom{n+1}{n+1} = |\mathscr{P}_{n+1}(M_{n+1})| = 1$, und ebenso ist $\frac{(n+1)!}{(n+1)!0!}$ gleich 1. □

Nachdem wir uns bis jetzt mit der Mächtigkeit *endlicher* Mengen beschäftigt haben, wenden wir uns nun den *unendlichen* Mengen zu. Durch Proposition (4.13) wird folgende Definition nahegelegt.

(4.19) Definition Wir bezeichnen zwei Mengen A und B als ***gleichmächtig*** (oder als Mengen mit gleicher Mächtigkeit) und schreiben $|A| = |B|$, wenn eine Bijektion $\phi : A \to B$ existiert.

Mit Hilfe dieser Definition können nun auch verschiedene Arten von unendlichen Mengen gegeneinander abgegrenzt werden.

(4.20) Definition Eine Menge A wird ***abzählbar unendlich*** genannt, wenn sie die gleiche Mächtigkeit wie $\mathbb{N}$ besitzt. Eine Menge, die endlich oder abzählbar unendlich ist, nennen wir ***höchstens abzählbar***. Eine Menge, die nicht höchstens abzählbar ist, bezeichnet man als ***überabzählbar***.

Als erstes bemerken wir

(4.21) Proposition Abzählbar unendliche Mengen sind unendlich.

Beweis: Nehmen wir an, dass eine Menge A zugleich endlich und abzählbar unendlich ist. Dann gibt es einerseits ein $n \in \mathbb{N}_0$ mit $|A| = n$, also eine Bijektion $\varphi : M_n \to A$, und andererseits eine Bijektion $\psi : \mathbb{N} \to A$. Sei ψ_{n+1} die Einschränkung von ψ auf M_{n+1}; dann wäre $\varphi^{-1} \circ \psi_{n+1} : M_{n+1} \to M_n$ eine injektive Abbildung von M_{n+1} in eine echte Teilmenge von M_{n+1}. Aber eine solche Abbildung kann es nach Proposition (4.12) nicht geben. □

Genau wie bei den endlichen Mengen sehen wir uns nun an, unter welchen Mengenoperationen die Abzählbarkeit erhalten bleibt.

(4.22) Lemma Jede unendliche Teilmenge von $\mathbb{N}$ ist abzählbar unendlich.

Beweis: Sei $A \subseteq \mathbb{N}$ eine unendliche Teilmenge. Wir definieren eine injektive Abbildung $\varphi : \mathbb{N} \to A$ durch folgende Rekursionsvorschrift: Wie in den Übungen mit dem Induktionsprinzip gezeigt wurde, besitzt jede nichtleere Teilmenge von $\mathbb{N}$ ein kleinstes Element. Bezeichnet a_1 das kleinste Element in A, dann setzen wir $\varphi(1) = a_1$. Sei nun $n \in \mathbb{N}$ und nehmen wir nun an, dass $\varphi(k)$ für $1 \leq k \leq n$ bereits definiert wurde, und dass φ auf $M_n = \{1, ..., n\}$ injektiv ist.

Wäre die Menge $A \setminus \varphi(M_n)$ leer, dann würde daraus $\varphi(M_n) = A$ folgen. Damit wäre φ eine Bijektion zwischen M_n und A, was aber der Voraussetzung widerspricht, dass A unendlich ist. So aber können wir in $A \setminus \varphi(M_n)$ ein kleinstes Element b wählen und $\varphi(n+1) = b$ definieren. Offenbar ist φ auch auf M_{n+1} injektiv. Denn nehmen wir an, es gäbe Elemente $k, \ell \in M_{n+1}$ mit $k < \ell$ und $\varphi(k) = \varphi(\ell)$. Wegen der Injektivität von $\varphi|_{M_n}$ ist dies nur möglich, wenn $k \in M_n$ und $\ell = n+1$ ist. Aber dann ist $\varphi(\ell) = \varphi(n+1) = b \notin \varphi(M_n)$ und $\varphi(k) \in \varphi(M_n)$. Also können $\varphi(k)$ und $\varphi(\ell)$ nicht übereinstimmen.

Insgesamt erhalten wir so eine Abbildung $\varphi : \mathbb{N} \to A$. Auch diese ist injektiv. Sind nämlich $k, \ell \in \mathbb{N}$ mit $k < \ell$, dann folgt aus der Injektivität von $\varphi|_{M_\ell}$ sofort $\varphi(k) \neq \varphi(\ell)$. Es bleibt zu zeigen, dass φ auch surjektiv ist. Nehmen wir an, dies ist nicht der Fall. Dann existiert in A ein kleinstes Element a mit $a \notin \varphi(\mathbb{N})$. Seien $a_1, ..., a_r$ die endlich vielen Elemente in A, die kleiner als a sind. Für jedes $i \in \{1, ..., r\}$ gibt es ein $n_i \in \mathbb{N}$ mit $\varphi(n_i) = a_i$. Nach eventueller Vertauschung der Elemente $a_1, ..., a_r$ können wir annehmen, dass n_r unter den Zahlen $a_1, ..., a_r$ maximal ist. Daraus

folgt $\{a_1, ..., a_r\} \subseteq \varphi(M_n)$ für $n = n_r$. Wir behaupten nun, dass $\varphi(n+1) = a$ gelten muss, im Widerspruch zur Annahme. Wegen $A \setminus \{a_1, ..., a_r\} \supseteq A \setminus \varphi(M_n)$ ist a auch das kleinste Element in $A \setminus \varphi(M_n)$. Also ergibt sich die Gleichung $\varphi(n+1) = a$ direkt aus unserer Rekursionsvorschrift. □

(4.23) Proposition

(i) Teilmengen höchstens abzählbarer Mengen sind höchstens abzählbar.

(ii) Sind A, B Mengen, ist A höchstens abzählbar und $\phi : A \to B$ eine surjektive Abbildung, dann ist auch B höchstens abzählbar.

Beweis: zu (i) Sei B eine höchstens abzählbare Menge und $A \subseteq B$. Ist B endlich, dann ist A nach Satz (4.15) (i) ebenfalls endlich und damit höchstens abzählbar. Wir können deshalb annehmen, dass B abzählbar unendlich ist. Demnach gibt es eine Bijektion $\varphi : B \to \mathbb{N}$. Ist A endlich, dann ist A nach Definition höchstens abzählbar. Wir können also annehmen, dass A unendlich ist. Auf Grund der Bijektivität von φ ist $\varphi(A)$ eine unendliche Teilmenge von $\mathbb{N}$. Diese ist nach Lemma (4.22) abzählbar unendlich. Also ist auch A abzählbar unendlich, insbesondere höchstens abzählbar.

zu (ii) Nach Satz (4.8) (ii) existiert eine Abbildung $\psi : B \to A$ mit $\varphi \circ \psi = \mathrm{id}_B$, und nach Satz (4.8) (i) ist diese Abbildung injektiv. Wie unter (i) gezeigt, ist $\psi(B)$ als Teilmenge der höchstens abzählbaren Menge A ebenfalls höchstens abzählbar. Weil ψ als injektive Abbildung eine zwischen B und $\psi(B)$ bijektiv ist, ist auch B höchstens abzählbar. □

Abbildungen können genutzt werden, um Elemente einer Menge A durch Elemente einer anderen Menge I zu indizieren. In diesem Zusammenhang bezeichnet man eine Abbildung $\varphi : I \to A$ auch als ***Familie*** von Elementen der Menge A und I als ***Indexmenge*** der Familie. Man verwendet dann für die Abbildung φ die Notation $(a_i)_{i \in I}$, und das Element $\varphi(i) \in A$ bezeichnet man mit a_i. Ist $I = \mathbb{N}$ oder $\mathbb{N}_0$, dann nennt man die Familie auch eine ***Folge***.

Beispielsweise wird durch $a_1 = 3$, $a_2 = 5$, $a_3 = 97$, $a_4 = 3$ eine Familie $(a_i)_{i \in I}$ natürlicher Zahlen mit der Indexmenge $\{1, 2, 3, 4\}$ definiert. Durch die Festlegung $a_n = n^2$ für alle $n \in \mathbb{N}$ erhält man eine Folge $(a_n)_{n \in \mathbb{N}}$ natürlicher Zahlen, nämlich die Folge der Quadratzahlen.

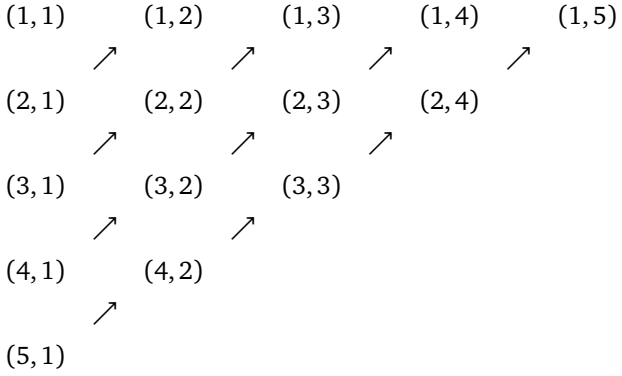
Familien werden verwendet, um auf die Elemente einer Menge A leichter zugreifen zu können (ähnlich wie die Seitennummern einen leichteren Zugriff auf die Seiten eines Buchs ermöglichen). Man kann auf diese Weise auch bestimmte Elemente von A auszeichnen oder sie (im Fall von $I = \mathbb{N}$) in eine bestimmte Reihenfolge bringen. Zu beachten ist dabei, dass die Abbildung $I \to A$, $i \mapsto a_i$ im allgemeinen weder injektiv noch surjektiv zu sein braucht. Beispielsweise kann dasselbe Element von A in einer Familie auch mehrfach vorkommen, also $a_i = a_j$ für verschiedene $i, j \in I$ gelten.

(4.24) Satz

(i) Sind A und B abzählbar unendliche Mengen, dann ist auch $A \times B$ abzählbar unendlich.

(ii) Ist I höchstens abzählbar, und ist $(A_i)_{i \in I}$ eine Familie bestehend aus lauter höchstens abzählbaren Mengen A_i, dann ist auch die Vereinigung $\bigcup_{i \in I} A_i$ höchstens abzählbar.

Beweis: zu (i) Zunächst führen wir den Beweis auf den Fall $A = B = \mathbb{N}$ zurück. Weil A und B abzählbar unendlich sind, gibt es Bijektionen $\varphi : \mathbb{N} \to A$ und $\psi : \mathbb{N} \to B$. Man überprüft leicht, dass dann die Abbildung $\mathbb{N} \times \mathbb{N} \to A \times B$, $(m,n) \mapsto (\varphi(m), \psi(n))$ ebenfalls bijektiv ist. Wenn also $\mathbb{N} \times \mathbb{N}$ abzählbar unendlich ist, dann gilt dasselbe für $A \times B$. Es genügt also nachzuweisen, dass $\mathbb{N} \times \mathbb{N}$ abzählbar unendlich ist. Dazu geben wir ein injektive Abbildung zwischen $\mathbb{N} \times \mathbb{N}$ und $\mathbb{N}$ an. Die grundlegende Idee besteht darin, die Paare in $\mathbb{N} \times \mathbb{N}$ nach dem folgenden Schema durchzunummerieren.



Dies wird realisiert durch die Abbildung $\phi : \mathbb{N}^2 \to \mathbb{N}$, $(m,n) \mapsto n + \frac{1}{2}(m+n-2)(m+n-1)$, die folgendermaßen zu Stande kommt: In jeder Diagonale des angegebenen Schemas befinden sich die Paare $(m,n) \in \mathbb{N}^2$ mit konstanter Summe $m+n$, wobei (m,n) jeweils auf der n-ten Position der $(m+n-1)$-ten Diagonale landet. Die r-te Diagonale hat für jedes $r \in \mathbb{N}$ jeweils genau r Einträge. Die Formel $1 + \ldots + r = \frac{1}{2}r(r+1)$, die in Satz (2.4) bewiesen wurde, zeigt, dass die $(m+n-2)$ vorausgehenden Diagonalen insgesamt die Länge $\frac{1}{2}(m+n-2)(m+n-1)$ haben. Also landet das Element (m,n) im Schema auf der Position $\frac{1}{2}(m+n-2)(m+n-1)+n$.

Wir beweisen nun die Injektivität der Abbildung ϕ. Dazu seien $(m_1,n_1),(m_2,n_2) \in \mathbb{N}^2$ mit $\phi(m_1,n_1) = \phi(m_2,n_2)$ vorgegeben. Zu zeigen ist $(m_1,n_1) = (m_2,n_2)$. Als erstes überprüfen wir, dass die Zahlen

$$r_1 = m_1 + n_1 - 2 \qquad \text{und} \qquad r_2 = m_2 + n_2 - 2$$

übereinstimmen. Nehmen wir an, dass dies nicht der Fall ist und zum Beispiel $r_1 < r_2$ gilt. Dann ist $\phi(m_1,n_1) \leq \frac{1}{2}r_1(r_1+1) + r_1$ und $\phi(m_2,n_2) \geq \frac{1}{2}r_2(r_2+1)$. Wir erhalten

$$\begin{aligned} \phi(m_2,n_2) - \phi(m_1,n_1) \quad &\geq \quad \tfrac{1}{2}r_2(r_2+1) - \left(\tfrac{1}{2}r_1(r_1+1) + r_1\right) \quad \geq \quad \tfrac{1}{2}(r_1+1)(r_1+2) - \left(\tfrac{1}{2}r_1(r_1+1) + r_1\right) \\ &= \quad \tfrac{1}{2}r_1^2 + \tfrac{3}{2}r_1 + 1 - \left(\tfrac{1}{2}r_1^2 + \tfrac{3}{2}r_1\right) \quad = \quad 1 \quad , \end{aligned}$$

was der Voraussetzung $\phi(m_1,n_1) = \phi(m_2,n_2)$ widerspricht. Also muss $r_1 = r_2$ gelten. Aus $r_1 = r_2$ folgt aber direkt $\frac{1}{2}r_1(r_1+1) = \frac{1}{2}r_2(r_2+1)$. Zusammen mit $\phi(m_1,n_1) = \phi(m_2,n_2) \Leftrightarrow \frac{1}{2}r_1(r_1+1) + n_1 = \frac{1}{2}r_2(r_2+1) + n_2$ folgt daraus $n_1 = n_2$ und damit auch $m_1 = m_2$. Damit ist die Injektivität bewiesen.

Wir haben somit gezeigt, dass $\mathbb{N}^2$ gleichmächtig zur Teilmenge $\psi(\mathbb{N}^2)$ von $\mathbb{N}$ ist. Nach Lemma (4.22) ist $\mathbb{N}^2$ höchstens abzählbar. Andererseits ist $\mathbb{N}_0 \times \mathbb{N}_0$ unendlich; wäre dies nicht so, dann würde aus der Injektivität der Abbildung $\mathbb{N} \to \mathbb{N}^2$, $m \mapsto (m,1)$ auch die Endlichkeit von $\mathbb{N}$ folgen, was nach Proposition (4.14) ausgeschlossen ist.

zu (ii) Da I höchstens abzählbar ist, gibt es eine injektive Abbildung $\varphi : I \to \mathbb{N}$. Auf Grund der Injektivität gibt es nach Satz (4.8) (i) eine Abbildung $\psi : \mathbb{N} \to I$ mit $\psi \circ \varphi = \mathrm{id}_I$. Diese ist nach Satz (4.8) (ii) surjektiv. Dasselbe Argument liefert uns für jedes $i \in I$ auch eine surjektive Abbildung $\varphi_i : \mathbb{N} \to A_i$. Wir behaupten nun, dass durch

$$\phi : \mathbb{N}^2 \longrightarrow \bigcup_{i \in I} A_i \quad , \quad (m,n) \mapsto \varphi_{\psi(m)}(n)$$

ebenfalls eine surjektive Abbildung gegeben ist. Ist nämlich $a \in \bigcup_{i \in I} A_i$ vorgegeben, dann gibt es $i \in I$ mit $a \in A_i$, ein $m \in \mathbb{N}_0$ mit $\psi(m) = i$ und ein $n \in \mathbb{N}_0$ mit $\varphi_i(n) = a$. Es folgt $\phi(m,n) = \varphi_{\psi(m)}(n) = \varphi_i(n) = a$. Nach Proposition (4.23) (ii) ist deshalb mit $\mathbb{N}^2$ auch die Menge $\bigcup_{i \in I} A_i$ höchstens abzählbar. □

§ 5. *Algebraische Grundstrukturen und Matrizen*

Inhaltsübersicht

In diesem Abschnitt definieren wir eine Reihe grundlegender algebraischer Strukturen, die im weiteren Verlauf der Vorlesung eine wichtige Rolle spielen werden: Halbgruppen, Monoide, Gruppen, Ringe und Körper. Ein konkretes Beispiel für einen Ring sind die ganzen Zahlen $\mathbb{Z}$. Bei den rationalen und reellen Zahlen, $\mathbb{Q}$ und $\mathbb{R}$, handelt es sich sogar um Körper. Mit Hilfe der in § 3 eingeführten Kongruenzrelationen und Kongruenzklassen werden wir sehen, dass es auch Ringe und Körper mit nur endlich vielen Elementen gibt.

Um weitere Beispiele für solche Strukturen zu erhalten (und weil wir sie als wichtiges Hilfsmittel der Linearen Algebra brauchen werden), führen wir in der zweiten Hälfte des Kapitels die Matrizen über einem beliebigen Ring ein, zusammen mit entsprechend angepassten Rechenoperationen, die man wie bei den Zahlen als „Addition“ und „Multiplikation“ bezeichnet. Die Matrizen unterscheiden sich von zuvor behandelten Strukturen unter anderem dadurch, dass die Multiplikation auf ihnen nicht mehr kommutativ ist, also in der Regel $AB \neq BA$ gilt.

Wichtige Begriffe und Sätze

- Definition der Verknüpfungen auf einer Menge, Eigenschaften „assoziativ“ und „kommutativ“
- Abgeschlossenheit einer Teilmenge unter einer Verknüpfung
- Halbgruppen, Monoide und Gruppen
- Neutralelement in einer Halbgruppe
- invertierbares Element in einem Monoid
- Ringe und Körper
- Restklassenringe und Restklassenkörper
- Matrizen, Nullmatrix, Einheitsmatrix, invertierbare Matrix

Unsere Einführung in das Thema dieses Kapitels beginnt mit dem Begriff der Verknüpfung.

(5.1) Definition Eine ***Verknüpfung*** auf einer Menge A ist eine Abbildung $A \times A \to A$.

Beispiele für Verknüpfungen sind die Addition, die Subtraktion und die Multiplikation auf der Menge $\mathbb{Z}$ der ganzen Zahlen, der Menge $\mathbb{Q}$ der rationalen Zahlen oder der Menge $\mathbb{R}$ der reellen Zahlen. Die Division ist *keine* Verknüpfung auf $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$, weil beispielsweise die Division durch 0 unzulässig ist. Um eine Verknüpfung zu erhalten, müsste man die Division geeignet einschränken. Sie wird zum Beispiel zu einer Verknüpfung auf der Teilmenge $\mathbb{Q}^\times = \mathbb{Q}\setminus\{0\}$. Ebenso sind Addition und Multiplikation Verknüpfungen auf $\mathbb{N}$ und $\mathbb{N}_0$, wohingegen Subtraktion und Division keine Verknüpfungen auf diesen Mengen sind. Beispielsweise liefert die Subtraktion zwar eine Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$, aber keine Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Als Bezeichnungen für eine Verknüpfung sind die Symbole $\cdot$, $\odot$, $*$, $+$, $\oplus$ und einige Varianten üblich. Wird eines der Symbole $\cdot$, $\odot$, $*$ verwendet, dann spricht man von einer ***multiplikativen*** Verknüpfung, bei $+$ oder $\oplus$ nennt man sie ***additiv***. Die beiden Typen unterscheiden sich aber außschließlich durch das verwendete Symbol, mathematisch gesehen besteht zwischen einer additiven und einer multiplikativen Verknüpfung keinerlei Unterschied.

Multiplikative Verknüpfungssymbole werden zur Vereinfachung der Notation häufig auch weggelassen, d.h. an Stelle von $a \cdot b$ schreibt man einfach ab. Sollen mehrere Elemente miteinander verknüpft werden, so ist die Verwendung von ***Klammern*** üblich, um die Reihenfolge der angewendeten Verknüpfungen anzuzeigen. So bedeutet zum Beispiel der Ausdruck $a(b(cd))$, dass zunächst das Element $x_1 = cd$ gebildet wird, anschließend $x_2 = bx_1$ und schließlich $x_3 = ax_2$.

(5.2) Definition Eine Verknüpfung $\cdot$ auf einer Menge A bezeichnet man als

(i) ***kommutativ***, wenn $ab = ba$ für alle $a, b \in A$

(ii) ***assoziativ***, wenn $a(bc) = (ab)c$ für alle $a, b, c \in A$ erfüllt ist.

Man bezeichnet eine Teilmenge $B \subseteq A$ als ***abgeschlossen*** unter der Verknüpfung $\cdot$, wenn für alle $b, b' \in B$ jeweils $bb' \in B$ gilt. Man erhält in diesem Fall eine Verknüpfung $\cdot_B$ auf B, indem man $b \cdot_B b' = bb'$ für alle $b, b' \in B$ setzt.

Bei assoziativen Verknüpfungen können die Klammern auch weggelassen werden. Für beliebige Elemente $a, b, c, d \in A$ ist dann zum Beispiel $abcd$ eine Kurzschreibweise für das Element $a(b(cd))$, welches auf Grund der Assoziativität mit jedem anders geklammerten Ausdruck, etwa $(ab)(cd)$ oder $a((bc)d)$, übereinstimmt.

Viele der bekannten Verknüpfungen sind assoziativ und kommutativ, beispielsweise die Addition und die Multiplikation auf den Zahlbereichen $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Die Subtraktion auf $\mathbb{Z}$ ist aber weder kommutativ noch assoziativ. Beispielsweise ist $2-1 = 1 \neq -1 = 1-2$, und $1-(1-1) = 1-0 = 1 \neq -1 = 0-1 = (1-1)-1$.

Auch Beispiele für abgeschlossene Teilmengen bezüglich der bekannten Verknüpfungen lassen sich in großer Zahl finden. Betrachtet man beispielsweise die Kette der Inklusionen $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, dann ist jede Teilmenge in dieser Kette bezüglich Addition und Multiplikation abgeschlossen in ihrem Nachfolger. Auch die Teilmenge $2\mathbb{Z}$ in $\mathbb{Z}$ ist abgeschlossen bezüglich Addition und Multiplikation, ebenso die einelementige Teilmenge $\{0\}$. Die Menge $\{1\}$ ist ebenfalls abgeschlossen bezüglich Multiplikation, aber nicht bezüglich Addition, denn es gilt $1+1 = 2 \notin \{1\}$.

Nach diesen Vorbereitungen können wir nun die ersten algebraischen Grundstrukturen definieren.

(5.3) Definition

(i) Eine ***Halbgruppe*** ist ein Paar $(G, \cdot)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $\cdot$ auf G.

(ii) Ein Element $e \in G$ in einer Halbgruppe wird ***Neutralelement*** genannt, wenn $g \cdot e = e \cdot g = g$ für alle $g \in G$ erfüllt ist.

(iii) Eine Halbgruppe $(G, \cdot)$, in der ein Neutralelement existiert, wird ***Monoid*** genannt.

Darauf aufbauend definieren wir weiter

(5.4) Definition

(i) Ein Element g in einem Monoid $(G, \cdot)$ mit Neutralelement e heißt ***invertierbar***, wenn ein $h \in G$ existierst, so dass die Gleichungen $g \cdot h = h \cdot g = e$ erfüllt sind.

(ii) Eine ***Gruppe*** ist ein Monoid, in dem jedes Element invertierbar ist.

(iii) Eine Halbgruppe, und ebenso ein Monoid und eine Gruppe, wird ***kommutativ*** oder ***abelsch*** genannt, wenn die zugehörige Verknüpfung kommutativ ist.

Auch für diese neuen Begriffe liefern die bekannten Zahlbereiche eine Vielzahl von Beispielen.

(i) Das Paar $(\mathbb{N}, +)$ ist eine Halbgruppe, aber kein Monoid; es existiert kein Neutralelement, weil für alle $a, b \in \mathbb{N}$ stets $a + b \neq a$ gilt. Das Paar $(\mathbb{N}, \cdot)$ ist ein Monoid, mit 1 als Neutralelement, denn es gilt $1 \cdot a = a \cdot 1 = a$ für alle $a \in \mathbb{N}$. Das Paar ist aber keine Gruppe, denn es gibt beispielsweise kein $a \in \mathbb{N}$ mit $2 \cdot a = 1$ (und wie wir gleich sehen werden, existiert in jedem Monoid immer nur ein Neutralelement).

(ii) Die Paare $(\mathbb{N}_0, +)$ ist ein Monoid, mit 0 als Neutralelement. Ebenso ist $(\mathbb{N}_0, \cdot)$ ein Monoid, das Neutralelement ist hier aber die 1. Beide Strukturen sind aber keine Gruppen.

(iii) Das Paar $(\mathbb{Z}, +)$ ist sogar eine Gruppe, denn die 0 ist Neutralelement, und für jedes $a \in \mathbb{Z}$ gilt $a + (-a) = (-a) + a = 0$. Das Paar $(\mathbb{Z}, \cdot)$ ist zwar ein Monoid, aber keine Gruppe.

(iv) Das Paar $(\mathbb{Q}, +)$ ist eine Gruppe, während $(\mathbb{Q}, \cdot)$ ein Monoid, aber keine Gruppe ist. Schränkt man die Verknüpfung $\cdot$ allerdings auf $\mathbb{Q}^\times$ ein, so erhält man eine Gruppe. Denn für jedes Element $a \in \mathbb{Q}^\times$ können wir den Kehrwert a^{-1} bilden, und es gilt $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(v) Beim Körper $\mathbb{R}$ der reellen Zahlen haben wir dieselben Verhältnisse: Das Paar $(\mathbb{R}, +)$ ist eine Gruppe, $(\mathbb{R}, \cdot)$ ist ein Monoid, aber keine Gruppe, und durch Einschränkung der Multiplikation auf $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ erhält man auch hier eine Gruppe.

Alle hier aufgezählten Halbgruppen, Monoide und Gruppen sind abelsch, weil die Addition und die Multiplikation auf allen Zahlbereichen kommutative Verknüpfungen sind.

(5.5) Lemma Sei $(G,\cdot)$ ein Monoid, und sei e ein Neutralelement des Monoids. Dann gilt:

(i) Das Monoid besitzt keine weiteren Neutralelemente. Man bezeichnet e deshalb als *das* Neutralelement des Monoids, und bezeichnet es mit e_G.

(ii) Zu jedem invertierbaren Element $a \in G$ gibt es genau ein Element $b \in G$ mit $ab = ba = e_G$. Man nennt b das zu a ***inverse Element***, und bezeichnet es mit a^{-1}.

(iii) Ist a invertierbar und $b \in G$ ein Element mit $ab = e_G$, dann folgt daraus bereits $b = a^{-1}$. Ebenso folgt bereits aus der Gleichung $ba = e_G$, dass b das Inverse von a ist.

(iv) Das Neutralelement ist invertierbar, und es gilt $e_G^{-1} = e_G$.

(v) Sind a und b invertierbare Elemente des Monoids, dann sind auch ab und a^{-1} invertierbar, und es gilt $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$.

Beweis: zu (i) Angenommen, e' ist ein weiteres Neutralelement des Monoids. Weil e ein Neutralelement ist, gilt $ee' = e'$. Weil e' Neutralelement ist, gilt auch $ee' = e$. Insgesamt gilt also $e = ee' = e'$.

zu (ii) Sei $a \in G$ invertierbar, und seien $b, c \in G$ Elemente mit $ab = ba = e_G$ und $ac = ca = e_G$. Dann gilt insgesamt $b = be_G = b(ac) = (ba)c = e_G c = c$.

zu (iii) Sei a invertierbar, und sei $b \in G$ mit $ab = e_G$. Dann gilt $a^{-1} = a^{-1}e_G = a^{-1}(ab) = (a^{-1}a)b = e_G b = b$. Setzen wir $ba = e_G$ voraus, dann erhalten wir ebenso $a^{-1} = e_G a^{-1} = (ba)a^{-1} = b(aa^{-1}) = be_G = b$.

zu (iv) Die Gleichung $e_G e_G = e_G$ zeigt, dass das Element e_G sein eigenes Inverses ist, also $e_G^{-1} = e_G$ gilt.

zu (v) Die Gleichungen $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = (ae_G)a^{-1} = aa^{-1} = e_G$ und $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e_G b) = b^{-1}b = e_G$ zeigen, dass $b^{-1}a^{-1}$ das Inverse von ab ist, also insbesondere $(ab)^{-1} = b^{-1}a^{-1}$ gilt. Ebenso zeigen die Gleichungen $aa^{-1} = e_G$ und $a^{-1}a = e_G$, dass a das Inverse von a^{-1} ist, also $(a^{-1})^{-1} = a$ gilt. □

(5.6) Folgerung Sei $(G,\cdot)$ ein Monoid, und sei $G^\times \subseteq G$ die Teilmenge der invertierbaren Elemente. Dann ist $G^\times$ bezüglich $\cdot$ abgeschlossen, und $(G^\times, \cdot_{G^\times})$ ist eine Gruppe.

Beweis: Die Abgeschlossenheit von $G^\times$ bezüglich $\cdot$ folgt direkt aus Teil (v) von Lemma (5.5). Somit können wir auf $G^\times$ durch $a \cdot_{G^\times} b = ab$ für alle $a, b \in G^\times$ eine Verknüpfung definieren; der einzige Unterschied zwischen den Abbildungen $\cdot$ und $\cdot_{G^\times}$ ist demnach der Definitions- und der Wertebereich. Die neue Verknüpfung $\cdot_{G^\times}$ ist assoziativ, denn für alle $a, b, c \in G^\times$ gilt

$$a \cdot_{G^\times} (b \cdot_{G^\times} c) \quad = \quad a(bc) \quad = \quad (ab)c \quad = \quad (a \cdot_{G^\times} b) \cdot_{G^\times} c.$$

Somit ist $(G^\times, \cdot_{G^\times})$ eine Halbgruppe. Nach Teil (iv) von Lemma (5.5) ist e_G in $G^\times$ enthalten. Außerdem gilt $a \cdot_{G^\times} e_G = ae_G = a$ und $e_G \cdot_{G^\times} a = e_G a = a$ für alle $a \in G^\times$. Dies zeigt, dass $(G^\times, \cdot_{G^\times})$ ein Monoid ist, mit e_G als Neutralelement. Für jedes $a \in G^\times$ liegt auf Grund des Lemmas auch a^{-1} in $G^\times$, und es gilt $a \cdot_{G^\times} a^{-1} = aa^{-1} = e_G$ und $a^{-1} \cdot_{G^\times} a = a^{-1}a = e_G$.

Das Element a ist also im Monoid $(G^\times, \cdot_{G^\times})$ invertierbar. Weil $a \in G^\times$ beliebig vorgegeben war, folgt daraus, dass jedes Element in dem Monoid invertierbar und $(G^\times, \cdot_{G^\times})$ somit eine Gruppe ist. □

Die Folgerung zeigt noch einmal, dass $\mathbb{Q}^\times$ und $\mathbb{R}^\times$ mit der Multiplikation jeweils eine Gruppe bilden, denn $(\mathbb{Q}, \cdot)$ und $(\mathbb{R}, \cdot)$ sind Monoide, und $\mathbb{Q}^\times$ bzw. $\mathbb{R}^\times$ sind genau die invertierbaren Elemente des Monoids. Im Monoid $(\mathbb{Z}, \cdot)$ gibt es nur zwei invertierbare Elemente, nämlich ± 1. In diesem Fall zeigt die Folgerung, dass durch $(\{\pm 1\}, \cdot)$ eine zweielementige Gruppe gegeben ist.

Monoide und Gruppen lassen sich zu komplexeren algebraischen Strukturen kombinieren.

(5.7) Definition Ein ***Ring*** ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$ auf R mit folgenden Eigenschaften.

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.
(ii) Das Paar $(R, \cdot)$ ist ein abelsches Monoid.
(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Das Neutralelement der Gruppe $(R, +)$ wird das ***Nullelement*** des Rings genannt und mit 0_R bezeichnet. Das Neutralelement des Monoids $(R, \cdot)$ nennt man das ***Einselement*** des Rings und bezeichnet es mit 1_R. Wenn die Menge $R^\times$ der invertierbaren Elemente des Monoids $(R, \cdot)$ mit $R \setminus \{0_R\}$ übereinstimmt, dann nennt man $(R, +, \cdot)$ auch einen ***Körper***.

Für jedes Element a in einem Ring R bezeichnen wir das Inverse von a in der Gruppe $(R, +)$ mit $-a$ und nennen es das ***Negative*** von a. Es gilt also $a + (-a) = (-a) + a = 0_R$ für alle $a \in R$. Ist a im Monoid $(R, \cdot)$ ein invertierbares Element, so bezeichnen wir das Inverse mit a^{-1} und nennen es den ***Kehrwert*** von a. Nach Definition gilt $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$ für dieses Elemente a. Auch für die Ringe stellen wir einige Rechenregeln zusammen.

(5.8) Proposition Sei $(R, +, \cdot)$ ein Ring, und seien $a, b \in R$. Dann gilt

(i) $-0_R = 0_R$, $-(-a) = a$ und $-(a + b) = (-a) + (-b)$,
(ii) $0_R \cdot a = 0_R$, $a(-b) = (-a)b = -(ab)$ und $ab = (-a)(-b)$,
(iii) $1_R^{-1} = 1_R$, $(a^{-1})^{-1} = a$ und $(ab)^{-1} = a^{-1}b^{-1}$, sofern a und b in $(R, \cdot)$ invertierbar sind.
(iv) Ist R sogar ein Körper, dann folgt aus $ab = 0_R$ immer $a = 0_R$ oder $b = 0_R$.

Beweis: Die Regeln (i) und (iii) erhält man unmittelbar durch Anwendung von Lemma (5.5) auf die Gruppe $(R, +)$ bzw. das Monoid $(R, \cdot)$. Zum Beweis der Regel (ii) seien $a, b \in R$ vorgegeben. Die erste Gleichung erhält man durch die Rechnung

$$\begin{aligned} 0_R \cdot a &= 0_R \cdot a + 0_R = 0_R \cdot a + 0_R \cdot a + (-0_R \cdot a) = (0_R + 0_R) \cdot a + (-0_R \cdot a) \\ &= 0_R \cdot a + (-0_R \cdot a) = 0_R. \end{aligned}$$

Die Gleichung $ab + a(-b) = a(b + (-b)) = a \cdot 0_R = 0_R$ zeigt, dass $a(-b)$ das Inverse von ab in der Gruppe $(R, +)$ ist, also $a(-b) = -(ab)$ gilt. Ebenso erhält man die Gleichung $(-a)b = -(ab)$. Die letzte Gleichung unter (ii) erhält man schließlich mit Hilfe der bereits hergeleiteten Regeln durch die Rechnung $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

Für den Beweis von (iv) setzen wir voraus, dass R ein Körper ist. Seien $a, b \in R$ mit $ab = 0_R$ vorgegben, und nehmen wir an, dass a ungleich 0_R ist. Dann ist a auf Grund der Körpereigenschaft ein invertierbares Elemente bezüglich der Multiplikation. Es folgt dann $b = 1_R \cdot b = (a^{-1}a) \cdot b = a^{-1}(ab) = a^{-1} \cdot 0_R = 0_R$. □

Allgemein ist es üblich, den Ausdruck $a + (-b)$ für $a, b \in R$ durch $a - b$ abzukürzen. Auf diese Weise erhält man eine neue Verknüpfung $-$ auf R. Wieder untersuchen wir die bekannten Zahlbereiche im Hinblick auf die soeben eingeführten Begriffe.

(i) Die Mengen $\mathbb{N}$ und $\mathbb{N}_0$ bilden mit der Addition und der Multiplikation keine Ringe, denn $(\mathbb{N}, +)$ und $(\mathbb{N}_0, +)$ sind keine Gruppen.

(ii) Die Menge $\mathbb{Z}$ der ganzen Zahlen bildet mit der Addition und der Multiplikation einen Ring. Es handelt sich aber um keinen Körper, denn wie wir oben festgestellt haben, ist die Menge der invertierbaren Elemente im Monoid $(\mathbb{Z}, \cdot)$ gleich $\{\pm 1\}$, sie stimmt also nicht mit $\mathbb{Z} \setminus \{0\}$ überein.

(iii) Die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ bilden mit der Addition und der Multiplikation Körper, und somit auch Ringe.

In einem Ring R kann es durchaus passieren, dass Eins- und Nullelement zusammenfallen, also $0_R = 1_R$ gilt. Dies ist aber nur möglich, wenn der Ring nur aus einem einzigen Element besteht, also $R = \{0_R\} = \{1_R\}$ gilt. Setzen wir nämlich $0_R = 1_R$ voraus und ist $a \in R$ ein beliebiges Element, dann folgt $a = 1_R \cdot a = 0_R \cdot a = 0_R$, nach Teil (ii) von Proposition (5.8). In einem Körper K gilt dagegen immer $0_K \neq 1_K$, weil Ringe R bestehend aus nur einem Element nach Definition keine Körper sind: Hier ist die Menge $R^\times$ der invertierbaren Elemente gleich $\{0_R\}$, während $R \setminus \{0_R\} = \varnothing$ ist. Die Gleichung $R^\times = R \setminus \{0_R\}$ ist hier also nicht erfüllt.

Um die Definition der Ringe noch besser illustrieren, führen wir eine weitere Klassen von Beispielen ein, die im Gegensatz zu den bisherigen nicht durch die aus der Schulmathematik bekannten Zahlbereiche zu Stande kommt.

Wir haben in § 3 die Mengen $\mathbb{Z}/n\mathbb{Z}$ bestehend aus den Kongruenzklassen $\bar{k} = [k]_n = k + n\mathbb{Z}$ mit $k \in \mathbb{Z}$ eingeführt. Dort haben wir auch gesehen, dass auf Grund der Äquivalenz $\bar{k} = \bar{\ell} \Leftrightarrow k \equiv_n \ell \Leftrightarrow n \mid (k - \ell)$ diese Menge aus n verschiedenen Elementen besteht, die durch $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ angegeben werden können. In der Algebra-Vorlesung werden wir zeigen, dass man auch auf $\mathbb{Z}/n\mathbb{Z}$ auf natürliche Weise eine Addition und eine Multiplikation definieren kann.

(5.9) Satz Sei $n \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Abbildungen $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ und $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z} \qquad \text{und} \qquad (a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = ab+n\mathbb{Z}$$

für alle $a, b \in \mathbb{Z}$.

Vollständig lassen sich diese Verknüpfungen durch ***Verknüpfungstabellen*** beschreiben, in denen jede Summe bzw. jedes Produkt von je zwei Elementen der Menge $\mathbb{Z}/n\mathbb{Z}$ angegeben ist. Für die Angabe wird dabei einheitlich die Darstellung der Elemente von $\mathbb{Z}/n\mathbb{Z}$ durch das Repräsentantensytem $\{0, 1, ..., n-1\}$ der Äquivalenzklassen verwendet. In $\mathbb{Z}/7\mathbb{Z}$ gilt beispielsweise $\bar{2}+\bar{2} = \bar{4}$, $\bar{3}+\bar{5} = \bar{8} = \bar{1}$ und $\bar{5}+\bar{6} = \overline{11} = \bar{4}$. Dabei wurde jeweils im ersten Schritt die Definition der Verknüpfung verwendet, und im zweiten Schritt wurde die Darstellung des Elements auf das angegebene Repräsentantensystem umgerechnet. Nach demselben Schema erhält man $\bar{2}\cdot\bar{3} = \bar{6}$, $\bar{3}\cdot\bar{5} = \overline{15} = \bar{1}$ und $\bar{5}\cdot\bar{6} = \overline{30} = \bar{2}$. Wir geben die Verknüpfungstabellen für $+$ und $\cdot$ auf $\mathbb{Z}/n\mathbb{Z}$ für $n = 4$ und $n = 7$ vollständig an.

Addition und Multiplikation auf $\mathbb{Z}/4\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Addition und Multiplikation auf $\mathbb{Z}/7\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Die Mengen $\mathbb{Z}/n\mathbb{Z}$ mit diesen beiden Verknüpfungen liefern uns neue Beispiele für Ringe, die nicht durch die bekannten Zahlbereiche gegeben sind und im Unterschied zu diesen aus nur endlich vielen Elementen bestehen.

(5.10) Satz Sei $n \in \mathbb{N}$. Dann bildet das Tripel $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ einen Ring, mit $\bar{0} = 0 + n\mathbb{Z}$ als Null- und $\bar{1} = 1 + n\mathbb{Z}$ als Einselement. Man bezeichnet ihn als ***Restklassenring*** modulo n.

Beweis: Zunächst zeigen wir, dass $(\mathbb{Z}/n\mathbb{Z},+)$ eine abelsche Gruppe ist, mit $\bar{0} = 0 + n\mathbb{Z}$ als Neutralelement. Zum Nachweis des Assoziativgesetzes seien $a+n\mathbb{Z}$, $b+n\mathbb{Z}$ und $c+n\mathbb{Z}$ vorgegeben, mit $a, b, c \in \mathbb{Z}$. Auf Grund der Definition der Verknüpfung $+$ auf $\mathbb{Z}/n\mathbb{Z}$, und auf Grund der Gültigkeit des Assoziativgesetzes fur die Addition auf den ganzen Zahlen, erhalten wir

$$\begin{aligned}((a+n\mathbb{Z})+(b+n\mathbb{Z}))+(c+n\mathbb{Z}) &= ((a+b)+n\mathbb{Z})+(c+n\mathbb{Z}) = ((a+b)+c)+n\mathbb{Z} = \\ (a+(b+c))+n\mathbb{Z} &= (a+n\mathbb{Z})+((b+c)+n\mathbb{Z}) = (a+n\mathbb{Z})+((b+n\mathbb{Z})+(c+n\mathbb{Z}))\end{aligned}$$

Für jedes Element $a+n\mathbb{Z}$ mit $a \in Z$ gilt $(a+n\mathbb{Z})+(0+n\mathbb{Z}) = (a+0)+n\mathbb{Z} = a+n\mathbb{Z}$ und $(0+n\mathbb{Z})+(a+n\mathbb{Z}) = (0+a)+n\mathbb{Z} = a+n\mathbb{Z}$. Dies zeigt, dass $\bar{0} = 0_n\mathbb{Z}$ in der Halbgruppe $(\mathbb{Z}/n\mathbb{Z},+)$ tatsächlich ein Neutralelement ist. Außerdem gilt jeweils $(a+n\mathbb{Z})+((-a)+n\mathbb{Z}) = (a+(-a))+n\mathbb{Z} = 0+n\mathbb{Z}$ und $((-a)+n\mathbb{Z})+(a+n\mathbb{Z}) = ((-a)+a)+n\mathbb{Z} = 0+n\mathbb{Z}$. Daran sehen wir, dass $(-a)+n\mathbb{Z}$ das Inverse von $\mathbb{Z}/n\mathbb{Z}$ im Monoid $(\mathbb{Z}/n\mathbb{Z},+)$ ist. Schließlich ist auch das Kommutativgesetz erfüllt, denn für alle $a+n\mathbb{Z}, b+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ mit $a, b \in \mathbb{Z}$ gilt

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z} = (b+a)+n\mathbb{Z} = (b+n\mathbb{Z})+(a+n\mathbb{Z}).$$

Insgesamt ist $(\mathbb{Z}/n\mathbb{Z},+)$ also tatsächlich eine abelsche Gruppe.

Als nächstes zeigen wir, dass durch $(\mathbb{Z}/n\mathbb{Z},\cdot)$ ein abelsches Monoid gegeben ist. Zur Überprüfung von Kommutativ- und Assozativgesetz seien $a+n\mathbb{Z}$, $b+n\mathbb{Z}$, $c+n\mathbb{Z}$ mit $a, b, c \in \mathbb{Z}$ vorgegeben. Dann gilt

$$(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = ab+n\mathbb{Z} = ba+n\mathbb{Z} = (b+n\mathbb{Z})\cdot(a+n\mathbb{Z}).$$

und

$$\begin{aligned}((a+n\mathbb{Z})\cdot(b+n\mathbb{Z}))\cdot(c+n\mathbb{Z}) &= (ab+n\mathbb{Z})\cdot(c+n\mathbb{Z}) = (ab)c+n\mathbb{Z} = \\ a(bc)+n\mathbb{Z} &= (a+n\mathbb{Z})\cdot(bc+n\mathbb{Z}) = (a+n\mathbb{Z})\cdot((b+n\mathbb{Z})\cdot(c+n\mathbb{Z})).\end{aligned}$$

Für jedes $a+n\mathbb{Z}$ mit $a \in \mathbb{Z}$ gilt außerdem $(a+n\mathbb{Z})\cdot(1+n\mathbb{Z}) = a\cdot 1+n\mathbb{Z} = a+n\mathbb{Z}$ und $(1+n\mathbb{Z})\cdot(a+n\mathbb{Z}) = 1\cdot a+n\mathbb{Z} = a+n\mathbb{Z}$. Dies zeigt, dass $\bar{1} = 1+n\mathbb{Z}$ in der Halbgruppe $(\mathbb{Z}/n\mathbb{Z},\cdot)$ ein Neutralelement ist. Insgesamt ist $(\mathbb{Z}/n\mathbb{Z},\cdot)$ also ein abelsches Monoid.

Um zu zeigen, dass $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ ein Ring ist, fehlt noch die Überprüfung des Distributivgesetzes. Seien dazu $a+n\mathbb{Z}, b+n\mathbb{Z}, c+n\mathbb{Z}$ vorgegeben, mit $a, b, c \in \mathbb{Z}$. Dann gilt

$$\begin{aligned}(a+n\mathbb{Z})\cdot((b+n\mathbb{Z})+(c+n\mathbb{Z})) &= (a+n\mathbb{Z})\cdot((b+c)+n\mathbb{Z}) = a(b+c)+n\mathbb{Z} = \\ (ab+ac)+n\mathbb{Z} &= (ab+n\mathbb{Z})+(ac+n\mathbb{Z}) = (a+n\mathbb{Z})\cdot(b+n\mathbb{Z})+(a+n\mathbb{Z})\cdot(c+n\mathbb{Z}).\end{aligned}$$

Damit ist die Verifikation der Ringeigenschaften abgeschlossen. □

Aus den Ringaxiomen folgt unter anderem, dass jedes Element $a \in \mathbb{Z}/n\mathbb{Z}$ ein ***Negatives*** besitzt, also ein $b \in \mathbb{Z}/n\mathbb{Z}$ mit $a+b = \bar{0}$. Das Negative von $c+n\mathbb{Z}$ (mit $c \in \mathbb{Z}$) ist jeweils gegeben durch $(-c)+n\mathbb{Z} = (n-c)+n\mathbb{Z}$. In $\mathbb{Z}/7\mathbb{Z}$ gilt beispielsweise $-\bar{0} = \bar{0}$, $-\bar{1} = \bar{6}$, $-\bar{2} = \bar{5}$, $-\bar{3} = \bar{4}$, $-\bar{4} = \bar{3}$, $-\bar{5} = \bar{2}$ und $-\bar{6} = \bar{1}$. Dementsprechend lässt sich auf $\mathbb{Z}/n\mathbb{Z}$ eine ***Subtraktion*** definieren, indem man für $a, b \in \mathbb{Z}/n\mathbb{Z}$ jeweils $a-b = a+(-b)$ setzt. In $\mathbb{Z}/7\mathbb{Z}$ gilt beispielsweise $\bar{3}-\bar{4} = \bar{3}+(-\bar{4}) = \bar{3}+\bar{3} = \bar{6}$.

Eine naheliegende Frage lautet, ob $\mathbb{Z}/n\mathbb{Z}$ nicht vielleicht sogar ein Körper ist. Dazu müsste unter anderem gezeigt werden, dass jedes Element $\neq \bar{0}$ in $\mathbb{Z}/n\mathbb{Z}$ einen Kehrwert besitzt. Aber dies ist, zumindest für beliebiges n, nicht der Fall. In $\mathbb{Z}/4\mathbb{Z}$ gilt beispielsweise $\bar{2}\cdot\bar{0}=\bar{0}$, $\bar{2}\cdot\bar{1}=\bar{2}$, $\bar{2}\cdot\bar{2}=\bar{4}=\bar{0}$ und $\bar{2}\cdot\bar{3}=\bar{6}=\bar{2}$. Es existiert also kein $a\in\mathbb{Z}/4\mathbb{Z}$ mit $\bar{2}\cdot a=\bar{1}$, das Element $\bar{2}$ besitzt also keinen Kehrwert. Außerdem sehen wir, dass es in $\mathbb{Z}/4\mathbb{Z}$ Elemente ungleich $\bar{0}$ gibt, deren Produkt gleich $\bar{0}$ ist, nämlich $\bar{2}\cdot\bar{2}=\bar{0}$. Wie wir aus Teil (iv) von Proposition (5.8) wissen, ist dies in einem Körper nicht möglich.

Wir werden aber sehen, dass $\mathbb{Z}/n\mathbb{Z}$ in einige Fälle doch ein Körper ist. Um zu sehen, für welche natürlichen Zahlen n dies gilt, benötigen wir noch etwas Vorbereitung. Wir bezeichnen zwei natürliche Zahlen m und n als ***teilerfremd***, wenn kein $d\in\mathbb{N}$ mit $d>1$, $d\mid m$ und $d\mid n$ existiert.

(5.11) Lemma Sind $m,n\in\mathbb{N}$ teilerfremd, dann gibt es $a,b\in\mathbb{Z}$ mit $am+bn=1$.

Beweis: Sei $S=\{am+bn\mid a,b\in\mathbb{Z}\}$. Zu zeigen ist, dass $1\in S$ gilt. Sei $d\in\mathbb{N}$ die kleinste natürliche Zahl in S. Dann gilt $d\mid s$ für alle $s\in S$. Denn nehmen wir an, dies ist nicht der Fall, d.h. es gilt $d\nmid s$ für ein $s\in S$. Durch Division mit Rest erhalten wir dann $q,r\in\mathbb{Z}$ mit $s=qd+r$, wobei $0<r<d$ gilt. Wir zeigen, dass r in S enthalten ist. Wegen $d\in S$ gibt es $a_0,b_0\in\mathbb{Z}$ mit $d=a_0m+b_0n$. Wegen $s\in S$ existieren ebenso $a_1,b_1\in\mathbb{Z}$ mit $s=a_1m+b_1n$. Es folgt

$$r \quad = \quad s-qd \quad = \quad (a_1m+b_1n)-q(a_0m+b_0n) \quad = \quad (a_1-qa_0)m+(b_1-qb_0)n \quad ,$$

wegen $a_1-qa_0, b_1-qb_0\in\mathbb{Z}$ also tatsächlich $r\in S$. Aber $r\in S$, $r\in\mathbb{N}$ und $r<d$ stehen im Widerspruch zur Minimalität von d.

Damit ist gezeigt, dass $d\mid s$ für alle $s\in S$ erfüllt ist. Wegen $m,n\in S$ folgt $d\mid m$ und $d\mid n$. Weil m und n aber nach Voraussetzung teilerfremd sind, muss $d=1$ sein. Damit ist $1\in S$ nachgewiesen. Nach Definition von S existieren also $a,b\in\mathbb{Z}$ mit $1=am+bn$. □

Wie in der Schulmathematik bezeichnen wir eine natürliche Zahl p als ***Primzahl***, wenn $p>1$ ist und keine $r,s\in\mathbb{N}$ mit $p=rs$ und $1<r,s<p$ existieren, die Zahl also nicht in zwei echt kleinere Faktoren zerlegbar ist.

(5.12) Satz Für jedes $n\in\mathbb{N}$ ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis: „⇐“ Sei $p\in\mathbb{N}$ eine Primzahl. Wir zeigen, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist und müssen dazu nachweisen, dass jedes Element ungleich $\bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ einen Kehrtwert besitzt. Sei $c+p\mathbb{Z}$ ein solches Element, mit $c\in\{1,\ldots,p-1\}$. Weil p eine Primzahl ist, besitzt p in $\mathbb{N}$ nur die beiden Teiler 1 und p. Daraus folgt, dass c und p teilerfremd sind. Nach Lemma (5.11) existieren deshalb $a,b\in\mathbb{Z}$ mit $ac+bp=1$. In $\mathbb{Z}/p\mathbb{Z}$ gilt deshalb die Gleichung

$$(a+p\mathbb{Z})(c+p\mathbb{Z})+(b+p\mathbb{Z})(p+p\mathbb{Z}) \quad = \quad 1+p\mathbb{Z}.$$

Wegen $p+p\mathbb{Z}=\bar{0}$ und $1+p\mathbb{Z}=\bar{1}$ erhalten wir in $\mathbb{Z}/p\mathbb{Z}$ die Gleichung $(a+p\mathbb{Z})(c+p\mathbb{Z})=\bar{1}$. Das Element $c+p\mathbb{Z}$ besitzt in $\mathbb{Z}/p\mathbb{Z}$ also das Element $a+p\mathbb{Z}$ als Kehrwert.

„⇒“ Ist n keine Primzahl, dann gilt entweder $n = 1$, oder es gibt $r,s \in \mathbb{N}$ mit $1 < r,s < n$ und $n = rs$. Wir zeigen, dass $\mathbb{Z}/n\mathbb{Z}$ in beiden Fällen kein Körper ist. Im Fall $n = 1$ gilt $\bar{1} = 1 + 1\mathbb{Z} = 0 + 1\mathbb{Z} = \bar{0}$, Null- und Einselement stimmen in $\mathbb{Z}/n\mathbb{Z}$ also überein. Wie wir oben gesehen haben, ist das in einem Körper ausgeschlossen. Betrachten wir nun noch den Fall $n = rs$ mit r und s wie oben angegeben. Setzen wir $a = r + n\mathbb{Z}$ und $b = s + n\mathbb{Z}$, dann gilt einerseits $a \neq \bar{0}$ und $b \neq \bar{0}$, andererseits aber $ab = (r + n\mathbb{Z})(s + n\mathbb{Z}) = rs + n\mathbb{Z} = n + n\mathbb{Z} = \bar{0}$. Nach Teil (iv) von Proposition (5.8) folgt daraus, dass $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist. □

Ist p eine Primzahl, dann verwendet man an Stelle von $\mathbb{Z}/p\mathbb{Z}$ für den Restklassenring auch die Notation $\mathbb{F}_p$. (Dabei steht das $\mathbb{F}$ für die englische Bezeichnung der algebraischen Struktur „Körper“. Diese lautet „field“.)

Beispielsweise ist $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ ein Körper, denn für jedes $a \in \mathbb{F}_7$ gibt es ein $b \in \mathbb{F}_7$ mit $ab = \bar{1}$: Es gilt $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{6} \cdot \bar{6} = \bar{1}$, $\bar{2} \cdot \bar{4} = \bar{1}$ und $\bar{3} \cdot \bar{5} = \bar{1}$. Insgesamt sind die Kehrwerte in $\mathbb{F}_7$ also durch folgende Tabelle gegeben:

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
a^{-1}	–	$\bar{1}$	$\bar{4}$	$\bar{5}$	$\bar{2}$	$\bar{3}$	$\bar{6}$

Für den Körper $\mathbb{F}_{13}$ erhält man auf gleiche Weise

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
a^{-1}	–	$\bar{1}$	$\bar{7}$	$\bar{9}$	$\overline{10}$	$\bar{8}$	$\overline{11}$	$\bar{2}$	$\bar{5}$	$\bar{3}$	$\bar{4}$	$\bar{6}$	$\overline{12}$

Bisher haben wir nur Strukturen kennengelernt, in denen die zugehörigen Verknüpfungen kommutativ sind. Bei den Objekten, die wir nun einführen, ist das Kommutativgesetz in der Regel nicht erfüllt. Sie werden später für uns ein wichtiges Hilfsmittel bei der Untersuchung und Lösung von Linearen Gleichungssystemen sein.

(5.13) Definition Seien $m,n \in \mathbb{N}$, und sei R ein Ring. Eine ***m×n - Matrix*** über R ist eine Abbildung

$$A : \{1,...,m\} \times \{1,...,n\} \longrightarrow R.$$

Dabei nennt man $A(i,j)$ den ***Eintrag*** von A an der Stelle (i,j). Die Menge aller $m \times n$-Matrizen über R wird mit $\mathscr{M}_{m\times n,R}$ bezeichnet. An Stelle von $\mathscr{M}_{n\times n,R}$ schreibt man auch kürzer $\mathscr{M}_{n,R}$. Die Elemente dieser Menge werden als ***quadratische*** Matrizen bezeichnet.

Durch die Gleichung $A = (a_{ij})$ ordnet man dem Eintrag $A(i,j)$ der Matrix A die Bezeichnung a_{ij} zu. Allgemein legen wir folgende Konvention fest: Bezeichnet ein Großbuchstabe wie zum Beispiel A,B,C eine Matrix, dann bezeichnen die indizierten Kleinbuchstaben a_{ij}, b_{ij}, c_{ij} immer automatisch die Einträge dieser Matrix. Man kann eine Matrix auch auf übersichtliche Weise als rechteckiges Schema der Form

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

Allgemein nennt man $a_{i\bullet} = (a_{i1}, ..., a_{in}) \in R^n$ die ***i-te Zeile*** und $a_{\bullet j} = (a_{1j}, ..., a_{mj}) \in R^m$ die ***j-te Spalte*** von A.

Offenbar existiert eine natürliche Bijektion zwischen Matrizen mit nur einer Zeile (also Elementen aus $\mathscr{M}_{1\times n,R}$), Matrizen mit nur einer Spalte (Elementen der Menge $\mathscr{M}_{n\times 1,R}$) und dem R^n. Dabei entspricht $(a_1, ..., a_n) \in R^n$ den beiden Matrizen

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} \in \mathscr{M}_{1\times n,R} \quad \text{und} \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathscr{M}_{n\times 1,R}.$$

Zur Beschreibung der Einträge verwendet man häufig als hilfreiche Abkürzung das sogenannte ***Kronecker-Delta***. Für jeden Ring R und beliebige $m, n \in \mathbb{N}$ definiert man

$$\delta_{mn} \quad = \quad \delta_{mn,R} \quad = \quad \begin{cases} 1_R & \text{falls} \quad m = n \\ 0_R & \text{falls} \quad m \neq n. \end{cases}$$

Falls aus dem Kontext geschlossen werden kann, welcher Ring gemeint ist, wird der Index R auch oft weggelassen. Die folgenden konkreten Beispiele für Matrizen werden uns in den Anwendungen immer wieder begegnen.

(i) die ***Nullmatrix*** $0^{(m\times n)}$ in $\mathscr{M}_{m\times n,R}$, deren sämtliche Einträge gleich 0_R sind
(Mit $0^{(n)} = 0^{(n\times n)}$ bezeichnen wir die quadratische Nullmatrix.)

(ii) die ***Einheitsmatrix*** $E = E^{(n)}$ in $\mathscr{M}_{n,R}$ mit den Einträgen δ_{ij} für $1 \leq i \leq m$ und $1 \leq j \leq n$
(Die Einheitsmatrix ist also immer quadratisch.)

(iii) die ***Basismatrizen*** $B_{k\ell} = B_{k\ell}^{(m\times n)}$ mit den Einträgen $b_{ij} = \delta_{ik}\delta_{j\ell}$ für $1 \leq i \leq m$ und $1 \leq j \leq n$

Beispielsweise ist

$$0^{(2\times 3)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad , \quad E^{(3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{und} \qquad B_{12}^{(3\times 2)} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Wir definieren nun eine Reihe von Rechenoperationen auf Matrizen. Weiterhin sei R ein beliebiger Ring. Um die Rechenoperationen definieren zu können, verwenden wir zum ersten Mal das ***Summenzeichen*** als Hilfsmittel. In allgemeiner Form werden wir dieses erst in § 11 einführen. Momentan genügt es zu wissen, dass für beliebige Ringelemente $a_1, ..., a_n \in R$ der Ausdruck

$$\sum_{k=1}^{n} a_k \qquad \text{eine Kurzschreibweise für} \qquad a_1 + ... + a_n \qquad \text{ist.}$$

Den Buchstaben k bezeichnet man dabei als *Laufindex* der Summe. Welchen Buchstaben man dafür verwendet, spielt letztlich keine Rolle; beispielsweise haben $\sum_{j=1}^{n} a_j$ und $\sum_{k=1}^{n} a_k$ denselben Wert. Ist $A = (a_{ij})$ eine Matrix in $\mathscr{M}_{m\times n,R}$, so kann über eine Zeile oder eine Spalte summiert werden: Für $1 \leq k \leq m$ und $1 \leq \ell \leq n$ gilt

$$\sum_{j=1}^{n} a_{kj} = a_{k1} + ... + a_{kn} \qquad \text{und} \qquad \sum_{i=1}^{m} a_{i\ell} = a_{1\ell} + ... + a_{m\ell}.$$

Der erste Ausdruck ist die Summe über die k-te Zeile von A, und beim zweiten Ausdruck handelt es sich um die Summe über die ℓ-te Spalte. Kommen wir nun zur Definition der Rechenoperationen für Matrizen.

(i) Seien $m, n \in \mathbb{N}$ und $A, B \in \mathscr{M}_{m\times n,R}$ mit Einträgen $A = (a_{ij})$ und $B = (b_{ij})$. Dann nennt man die Matrix $C = (c_{ij})$ mit $c_{ij} = a_{ij} + b_{ij}$ für $1 \le i \le m$ und $1 \le j \le n$ die ***Summe*** von A und B. Wir bezeichnen diese Matrix mit $A + B$. Beispielsweise gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} -1 & 5 & -2 \\ 3 & 0 & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 & 7 & 1 \\ 7 & 5 & 7 \end{pmatrix}.$$

(ii) Sei $A \in \mathscr{M}_{m\times n,R}$ mit $A = (a_{ij})$ und $\lambda \in K$. Dann ist die Matrix $C = (c_{ij})$ mit $c_{ij} = \lambda a_{ij}$ ein ***skalares Vielfaches*** von A, das wir mit λA bezeichnen. Beispielsweise ist

$$7 \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad = \quad \begin{pmatrix} 7 & 14 & 21 \\ 28 & 35 & 42 \end{pmatrix}.$$

(iii) Seien nun $m, n, r \in \mathbb{N}$ und $A \in \mathscr{M}_{m\times n,R}$, $B \in \mathscr{M}_{n\times r,R}$. Dann heißt die Matrix $C \in \mathscr{M}_{m\times r,R}$ mit den Einträgen

$$c_{ij} \quad = \quad \sum_{k=1}^{n} a_{ik} b_{kj}$$

Produkt der Matrizen A und B und wird mit AB bezeichnet. Auch hierzu ein konkretes Beispiel:

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & -1 & -3 \\ 3 & 6 & 9 & 12 \end{pmatrix}$$

Den Eintrag an der Position $(2, 2)$ erhält man zum Beispiel durch Multiplikation der zweiten Zeile der ersten Matrix mit der zweiten Spalte der zweiten Matrix, also durch die Rechung $(-1) \cdot 2 + 1 \cdot 3 = 1$. Der Eintrag an der Position $(3, 3)$ kommt entsprechend durch $3 \cdot 3 + 0 \cdot 2 = 9$ zu Stande.

(iv) Sei $A \in \mathscr{M}_{m\times n,R}$. Die Matrix $B \in \mathscr{M}_{n\times m,R}$ mit den Einträgen $b_{ij} = a_{ji}$ für $1 \le i \le n$ und $1 \le j \le m$ wird die zu A ***transponierte*** Matrix ${}^{\mathrm{t}}A$ genannt. Zum Beispiel ist

$${}^{\mathrm{t}}\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

Um den Eintrag c_{ij} der Produktmatrix $C = AB$ an der Position (i, j) zu erhalten, muss die i-te Zeile der Matrix A mit der j-ten Spalte der Matrix B multipliziert werden. Man beachte, dass das Produkt AB nur gebildet werden kann, wenn die Spaltenzahl von A mit der Zeilenzahl von B übereinstimmt. Die Summe $A + B$ ist nur dann definiert, wenn A und B dasselbe Format, also dieselbe Anzahl Zeilen *und* Spalten besitzen.

Die neu eingeführten Rechenoperationen erfüllen eine Reihe von Rechenregeln. Wir beginnen mit der Summe von Matrizen.

(5.14) Proposition Sei R ein Ring, und seien $m, n \in \mathbb{N}$. Dann bildet die Menge $\mathscr{M}_{m\times n,R}$ mit der Addition von Matrizen eine abelsche Gruppe. Dabei ist $0^{(m\times n)}$ das Neutralelement, und für jedes $A \in \mathscr{M}_{m\times n,R}$ ist $(-1_R)A$ das Inverse von A. Dieses Inverse wird das ***Negative*** von A genannt und mit $-A$ bezeichnet.

Beweis: Zunächst zeigen wir, dass die Addition von Matrizen das Assoziativ- und das Kommutativgesetz erfüllt. Seien dazu $A,B,C \in \mathscr{M}_{m\times n,R}$ vorgegeben. Für $1 \le i \le m$ und $1 \le j \le n$ stimmt wegen $(a_{ij}+b_{ij})+c_{ij} = a_{ij}+(b_{ij}+c_{ij})$ der Eintrag der Matrix $(A+B)+C$ an der Stelle (i,j) überein mit dem Eintrag der Matrix $A+(B+C)$ an derselben Position.

Ebenso zeigt die Gleichung $a_{ij}+b_{ij} = b_{ij}+a_{ij}$, dass die Matrizen $A+B$ und $B+A$ an der Position (i,j) übereinstimmen. Insgesamt sind damit die Gleichungen $(A+B)+C = A+(B+C)$ und $A+B = B+A$ bewiesen. Das Paar $(\mathscr{M}_{m\times n,R},+)$ ist also eine abelsche Halbgruppe.

Die Matrizen $A+0^{(m\times n)}$ und $0^{(m\times n)}+A$ haben an der Position (i,j) jeweils den Eintrag $a_{ij}+0_R = 0_R+a_{ij} = a_{ij}$. Es gilt also $A+0^{(m\times n)} = 0^{(mtimesn)}+A = A$. Dies zeigt, dass die Nullmatrix in der Halbgruppe $(\mathscr{M}_{m\times n,R},+)$ ein Neutralelement ist und somit ein abelsches Monoid vorliegt. Die Matrix $(-1_R)A$ hat an der Stelle (i,j) den Eintrag $(-1_R)a_{ij} = -a_{ij}$. Dadurch ist die Bezeichnung $-A$ für diese Matrix gerechtfertigt. Die Matrizen $A+(-A)$ und $(-A)+A$ haben an der Position (i,j) beide den Eintrag $a_{ij}+(-a_{ij}) = (-a_{ij})+a_{ij} = 0_R$. Dies zeigt, dass $-A$ im Monoid $(\mathscr{M}_{m\times n,R},+)$ ein zu A inverses Element ist. Jedes Element in diesem Monoid ist also invertierbar. Dies zeigt insgesamt, dass $(\mathscr{M}_{m\times n,R},+)$ eine abelsche Gruppe ist. □

(5.15) Proposition Sei R ein Ring, und seien $m,n,r,s \in \mathbb{N}$. Weiter seien $A,A' \in \mathscr{M}_{m\times n,R}$, $B,B' \in \mathscr{M}_{n\times r,R}$ und $C \in \mathscr{M}_{r\times s,R}$. Dann gelten die folgenden Rechenregeln.

(i) $A(B+B') = AB+AB'$ und $(A+A')B = AB+A'B$ (ii) $A(\lambda B) = (\lambda A)B = \lambda(AB)$

(iii) $E^{(m)}A = AE^{(n)} = A$ (iv) $(AB)C = A(BC)$ (v) ${}^{t}(AB) = {}^{t}B\,{}^{t}A$

Beweis: zu (i) Wir beschränken uns auf den Beweis der zweiten Gleichung, da der Beweis der ersten vollkommen analog verläuft. Es sei $C' = A+A'$, $D = C'B$, $F = AB$, $G = A'B$ und $H = F+G$. Dann ist $D = H$ zu zeigen. Für $1 \le i \le m$ und $1 \le j \le n$ gilt jeweils $c'_{ij} = a_{ij}+a'_{ij}$. Die Einträge d_{ij} der Matrix D (für $1 \le i \le m$, $1 \le j \le r$) sind gegeben durch

$$d_{ij} \quad = \quad \sum_{k=1}^{n} c'_{ik}b_{kj} \quad = \quad \sum_{k=1}^{n}(a_{ik}+a'_{ik})b_{kj} \quad = \quad \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a'_{ik}b_{kj}.$$

Für die Einträge f_{ij} und g_{ij} der Matrizen F und G (mit $1 \le i \le m$, $1 \le j \le r$) erhalten wir

$$f_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} \qquad \text{und} \qquad g_{ij} = \sum_{k=1}^{n} a'_{ik}b_{kj}.$$

Es folgt

$$h_{ij} \quad = \quad f_{ij}+g_{ij} \quad = \quad \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a'_{ik}b_{kj} \quad = \quad d_{ij}$$

für $1 \le i \le m$, $1 \le j \le r$, also insgesamt $D = H$.

zu (ii) Wir definieren $C' = \lambda B$, $D = AC'$, $F = \lambda A$, $G = FB$, $H = AB$ und $U = \lambda H$. Zu zeigen ist dann $D = G = U$. Nach Definition gilt $c'_{ij} = \lambda b_{ij}$ für $1 \le i \le n$, $1 \le j \le r$ und

$$d_{ij} \quad = \quad \sum_{k=1}^{n} a_{ik}c'_{kj} \quad = \quad \sum_{k=1}^{n} \lambda a_{ik}b_{kj}$$

für $1 \le i \le m$ und $1 \le j \le r$. Andererseits gilt auch $f_{ij} = \lambda a_{ij}$ für $1 \le i \le m$,$1 \le j \le n$ und $g_{ij} = \sum_{k=1}^{n} f_{ik} b_{kj} = \sum_{k=1}^{n} \lambda a_{ik} b_{kj} = d_{ij}$ für $1 \le i \le m$,$1 \le j \le r$, womit die Gleichung $D = G$ bewiesen ist. Nun gilt außerdem $h_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$ für $1 \le i \le m$ und $1 \le j \le r$, und

$$u_{ij} \quad = \quad \lambda h_{ij} \quad = \quad \sum_{k=1}^{n} \lambda a_{ik} b_{kj} \quad = \quad d_{ij}$$

für dieselben Paare (i, j), wodurch auch die Gleichung $U = D$ bewiesen ist.

zu (iii) Wir beschränken uns auf den Beweis der Gleichung $E^{(m)}A = A$. Bezeichnen wir das Matrixprodukt $E^{(m)}A \in \mathscr{M}_{m\times n,K}$ mit B, dann ist der Eintrag $b_{k\ell}$ von B an der Position (k, ℓ) für $1 \le k \le m$ und $1 \le \ell \le n$ gegeben durch

$$b_{k\ell} \quad = \quad \sum_{j=1}^{m} \delta_{kj} a_{j\ell} \quad = \quad \delta_{kk} a_{k\ell} \quad = \quad a_{k\ell}.$$

Dies zeigt, dass B mit der Matrix A übereinstimmt.

zu (iv) Wir definieren $D = AB$, $F = DC$, $G = BC$ und $H = AG$. Dann gilt für $1 \le k \le m$ und $1 \le \ell \le r$ jeweils $d_{k\ell} = \sum_{i=1}^{n} a_{ki} b_{i\ell}$, und für die Einträge der Matrix F erhalten wir

$$f_{k\ell} \quad = \quad \sum_{i=1}^{r} d_{ki} c_{i\ell} \quad = \quad \sum_{i=1}^{r} \sum_{j=1}^{n} a_{kj} b_{ji} c_{i\ell} \quad ,$$

für $1 \le k \le m$ und $1 \le \ell \le s$. Andererseits hat G die Einträge $g_{k\ell} = \sum_{i=1}^{r} b_{ki} c_{i\ell}$ für $1 \le k \le n$ und $1 \le \ell \le s$, und für die Einträge $h_{k\ell}$ der Matrix H ($1 \le k \le m$, $1 \le \ell \le s$) gilt

$$h_{k\ell} \quad = \quad \sum_{i=1}^{n} a_{ki} g_{i\ell} \quad = \quad \sum_{i=1}^{n} \sum_{j=1}^{r} a_{ki} b_{ij} c_{j\ell} \quad , \quad \text{also insgesamt} \quad F = H.$$

zu (v) Hier definieren wir die Hilfsmatrizen $C = AB$, $D = {}^{\mathrm{t}}C$, $F = {}^{\mathrm{t}}A$, $G = {}^{\mathrm{t}}B$ und $H = GF$. Dann müssen wir $D = H$ nachrechnen. Es gilt Für $1 \le i \le m$ und $1 \le j \le r$ gilt

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \text{ für } 1 \le i \le m, 1 \le j \le r \qquad \text{und} \qquad d_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk} b_{ki} \text{ für } 1 \le i \le r, 1 \le j \le m.$$

Wegen $f_{ij} = a_{ji}$ und $g_{ij} = b_{ji}$ für $1 \le i \le n$ und $1 \le j \le m$ bzw. $1 \le i \le r$ und $1 \le j \le n$ gilt außerdem

$$h_{ij} \quad = \quad \sum_{k=1}^{n} g_{ik} f_{kj} \quad = \quad \sum_{k=1}^{n} b_{ki} a_{jk} \quad = \quad d_{ij}$$

für $1 \le i \le r$ und $1 \le j \le m$, also $H = D$ wie gewünscht. □

(5.16) Folgerung Sei R ein Ring, und seien $n \in \mathbb{N}$. Dann bildet die Menge $\mathscr{M}_{n,R}$ mit der Multiplikation von Matrizen ein Monoid, mit $E^{(n)}$ als Neutralelement.

Beweis: Nach Teil (iv) von Proposition (5.15) ist die Multiplikation von Matrizen eine assoziative Verknüpfung auf $\mathscr{M}_{n,R}$. Aus Teil (iii) folgt, dass $E^{(n)}$ ein Neutralelement in der Halbgruppe $(\mathscr{M}_{n,R}, \cdot)$ ist. Insgesamt handelt es sich bei $(\mathscr{M}_{n,R}, \cdot)$ also um ein Monoid. □

Das Monoid $(\mathscr{M}_{n,R}, \cdot)$ ist in der Regel nicht kommutativ. Ist beispielsweise $n = 2$, und stimmen im Ring R das Nullelement 0_R und das Einselement 1_R nicht überein, dann zeigt das Beispiel

$$\begin{pmatrix} 0_R & 1_R \\ 1_R & 0_R \end{pmatrix}\begin{pmatrix} 1_R & 1_R \\ 0_R & 1_R \end{pmatrix} = \begin{pmatrix} 0_R & 1_R \\ 1_R & 1_R \end{pmatrix} \quad , \quad \begin{pmatrix} 1_R & 1_R \\ 0_R & 1_R \end{pmatrix}\begin{pmatrix} 0_R & 1_R \\ 1_R & 0_R \end{pmatrix} = \begin{pmatrix} 1_R & 1_R \\ 1_R & 0_R \end{pmatrix}$$

dass die Gleichung $AB = BA$ nicht für alle $A, B \in \mathscr{M}_{n,R}$ erfüllt ist.

Wir bemerken auch, dass das Tupel $(\mathscr{M}_{n,R}, +, \cdot)$ alle Eigenschaften eines Rings besitzt, mit Ausnahme des Kommutativgesetzes der Multiplikation. Eine solche Struktur wird in der Algebra als ***Schiefring*** bezeichnet.

Eine Matrix $A \in \mathscr{M}_{n,R}$ wird ***invertierbar*** genannt, wenn eine Matrix $B \in \mathscr{M}_{n,R}$ mit $AB = BA = E^{(n)}$ existiert. Wir werden in einem späteren Kapitel sehen, wie man herausfindet, ob eine Matrix invertierbar ist, und wie sich gegebenenfalls das Inverse berechnen lässt.

(5.17) Folgerung Die Menge der invertierbaren $n \times n$-Matrizen über einem Körper K bildet mit der Multiplikation von Matrizen eine Gruppe. Man nennt sie die ***allgemeine lineare Gruppe*** und bezeichnet sie mit $\mathrm{GL}_n(K)$.

Beweis: Dies erhält man unmittelbar durch Anwendung von Folgerung (5.6) auf das Monoid $(\mathscr{M}_{n,R}, \cdot)$. □

§ 6. *Vektorräume, lineare Abbildungen und lineare Gleichungssysteme*

Inhaltsübersicht

Der Begriff des Vektorrraums über einem Körper K ist für die Lineare Algebra von zentraler Bedeutung. Es handelt sich dabei um eine Menge V mit einer Verknüpfung, der *Vektoraddition*, und einer Abbildung $K \times V \to V$, der *skalaren Multiplikation*. Das wichtigstes Beispiel sind die Vektorräume der Form K^n, mit $m \in \mathbb{N}$. Aber auch viele weitere Objekte der Mathematik besitzen eine Vektorraumstruktur, zum Beispiel die Menge $\mathscr{M}_{m\times n,K}$ der $(m \times n)$-Matrizen über einem Körper K. Auf gewissen Teilmengen eines Vektorraums, den sog. *Untervektorräumen*, lässt sich ebenfalls eine Vektorraumstruktur definieren.

Eine Abbildung $V \to W$ zwischen Vektorräumen bezeichnet man als *lineare Abbildung*, wenn sie „verträglich“ mit der Vektoraddition und der skalaren Multiplikation der beiden Vektorräume ist. Wichtigstes Beispiel einer linearen Abbildung ist für uns zunächst die Matrix-Vektor-Multiplikation. Oft haben lineare Abbildungen eine geometrische Interpretation; zum Beispiel ist die Spiegelung im $\mathbb{R}^2$ an einer Gerade durch den Koordinatenursprung $(0,0)$ eine lineare Abbildung, ebenso jede Drehung um den Ursprung.

Desweiteren führen wir in diesem Kapitel den Begriff des *linearen Gleichungssystems* ein. Wir werden sehen, wie sich solche Systeme und ihre Lösungsmengen mit Hilfe der Untervektorräume und der linearen Abbildungen auf übersichtliche Weise beschreiben lassen. Dies dient auch zur Vorbereitung des nächsten Kapitels, wo wir uns dann mit der Berechnung von Lösungsmengen linearer Gleichungssysteme befassen.

Wichtige Begriffe und Sätze

- Vektorraum über einem Körper K
- Untervektorraum, affiner Unterraum
- lineare Abbildung, affin-lineare Abbildung, Affinität
- allgemeine lineare Gruppe $\mathrm{GL}(V)$ zu einen Vektorraum V
- Kern und Bild einer linearen Abbildung
- homogenes und inhomogenes lineares Gleichungssystem
- (erweiterte) Koeffizientenmatrix eines linearen Gleichungssystems
- Lösungsmenge eines linearen Gleichungssystems
- (eindeutige) Lösbarkeit eines linearen Gleichungssystems
- Vektorraum $\mathrm{Hom}_K(V,W)$ der linearen Abbildungen $V \to W$

(6.1) Definition Sei K ein Körper. Ein K-***Vektorraum*** ist ein Tripel $(V,+,\cdot)$ bestehend aus einer nichtleeren Menge V und Abbildungen $+ : V\times V \to V$ und $\cdot : K\times V \to V$ genannt ***Vektoraddition*** und ***skalare Multplikation***, so dass folgende Bedingungen erfüllt sind.

(i) Das Paar $(V,+)$ ist eine abelsche Gruppe.

(ii) Für alle $v,w \in V$ und $\lambda,\mu \in K$ gelten die Rechenregeln

(a) $(\lambda+\mu)\cdot v = (\lambda\cdot v)+(\mu\cdot v)$

(b) $\lambda\cdot(v+w) = (\lambda\cdot v)+(\lambda\cdot w)$

(c) $(\lambda\mu)\cdot v = \lambda\cdot(\mu\cdot v)$

(d) $1_K\cdot v = v$

Die Elemente der Menge V werden ***Vektoren*** genannt.

Bei der skalaren Multiplikation wird häufig auf das Abbildungssymbol $\cdot$ verzichtet. Das Neutralelement der Gruppe $(V,+)$ bezeichnet man als den ***Nullvektor*** 0_V des Vektorraums. Das Inverse eines Vektors $v \in V$ bezüglich der Vektoraddition bezeichnet man mit $-v$ und verwendet $v-w$ als abkürzende Schreibweise für $v+(-w)$. Per Konvention bindet die skalare Multiplikation stärker als die Vektoraddition, d.h. der Ausdruck $\lambda v + w$ ist gleichbedeutend mit $(\lambda v)+w$ für $\lambda \in K$, $v,w \in V$.

(6.2) Proposition Sei K ein Körper. Die folgenden Strukturen sind Beispiele für K-Vektorräume.

(i) das Tripel $(K^n,+,\cdot)$ $(n\in\mathbb{N})$, wobei die Abbildung $+ : K^n\times K^n \to K^n$ und $\cdot : K\times K^n \to K^n$ definiert sind durch

$$(a_1,...,a_n)+(b_1,...,b_n) = (a_1+b_1,...,a_n+b_n) \quad \text{und} \quad \lambda\cdot(a_1,...,a_n) = (\lambda a_1,...,\lambda a_n).$$

Insbesondere ist $K^1 = K$ selbst ein K-Vektorraum. Hier ist die Vektoraddition die Addition auf K, und die skalare Multiplikation ist die Multiplikation auf K.

(ii) das Tripel $(\{0_K\},+,\cdot)$, mit den Abbildungen $+ : \{0_K\}\times\{0_K\} \to \{0_K\}$ und $\cdot : K\times\{0_K\} \to \{0_K\}$ gegeben durch $0_K+0_K = 0_K$ und $\lambda\cdot 0_K = 0_K$ für alle $\lambda\in K$

(iii) das Tripel $(\mathscr{M}_{m\times n,K},+,\cdot)$ $(m,n\in\mathbb{N})$ wobei $+$ die Addition von Matrizen und $\cdot : K\times \mathscr{M}_{m\times n,K} \to \mathscr{M}_{m\times n,K}$ durch $(\lambda,A)\mapsto \lambda A$ gegeben ist

(iv) Jeder $\mathbb{C}$-Vektorraum $(V,+,\cdot)$ besitzt auch eine Struktur als $\mathbb{R}$-Vektorraum, gegeben durch $(V,+,\cdot_{\mathbb{R}})$, wobei die Abbildung $\cdot_{\mathbb{R}} : \mathbb{R}\times V \to V$ durch Einschränkung der Abbildung $\cdot : \mathbb{C}\times V \to V$ auf $\mathbb{R}\times V$ zu Stande kommt.

Beweis: In jedem Fall können die Vektorraum-Eigenschaften unmittelbar überprüft werden. Wir beschränken uns auf den Nachweis im Fall (iii). Aus Proposition (5.14) wissen wir bereits, dass $(\mathscr{M}_{m\times n,K},+)$ eine abelsche Gruppe ist.

Zum Nachweis der übrigen Regeln seien $A, B \in \mathscr{M}_{m\times n,K}$ und $\lambda, \mu \in K$ vorgegeben. Es gilt $(\lambda+\mu)A = \lambda A + \mu A$, denn für $1 \le i \le m$ und $1 \le j \le n$ ist der Eintrag der Matrix an der Position (i,j) jeweils gleich $(\lambda+\mu)a_{ij} = \lambda a_{ij} + \mu a_{ij}$. Es gilt $\lambda(A+B) = \lambda A + \lambda B$, weil der Eintrag an der Stelle j jeweils mit $\lambda(a_{ij} + b_{ij}) = \lambda a_{ij} + \lambda b_{ij}$ übereinstimmt. Beide Matrixgleichungen ergeben sich also direkt aus dem Distributivgesetz des Körpers K. Die Gleichung $(\lambda\mu)A = \lambda(\mu A)$ ergibt sich direkt aus dem Assoziativgesetz der multiplikativen Verknüpfung des Körpers K, denn für den Eintrag an der Stelle (i,j) gilt jeweils $(\lambda\mu)a_{ij} = \lambda(\mu a_{ij})$. Schließlich gilt auch $1_K \cdot A = A$, denn der Eintrag der Matrix an der Stelle (i,j) ist gleich $1_K \cdot a_{ij} = a_{ij}$. □

(6.3) Lemma Sei $(V,+,\cdot)$ ein K-Vektorraum. Dann gilt für alle $\lambda \in K$ und $v \in V$ die Äquivalenz

$$\lambda v = 0_V \quad \Leftrightarrow \quad \lambda = 0_K \text{ oder } v = 0_V \quad ,$$

außerdem $(-1_K)v = -v$ für alle $v \in V$.

Beweis: Zunächst beweisen wir die Äquivalenz. „⇐“ Ist $\lambda = 0_K$, dann gilt $\lambda v = 0_K v = (0_K + 0_K)v = 0_K v + 0_K v = \lambda v + \lambda v$. Addition von $-\lambda v$ auf beiden Seiten dieser Gleichung liefert

$$\lambda v + (-\lambda v) = \lambda v + \lambda v + (-\lambda v) \quad \Leftrightarrow \quad 0_V = \lambda v + 0_V \quad \Leftrightarrow \quad 0_V = \lambda v.$$

Setzen wir nun $v = 0_V$ voraus, dann erhalten wir $\lambda v = \lambda 0_V = \lambda(0_V + 0_V) = \lambda 0_V + \lambda 0_V = \lambda v + \lambda v$. Wieder führt die Addition von $-\lambda v$ auf beiden Seiten zum gewünschten Ergebnis.

„⇒“ Setzen wir $\lambda v = 0_V$ voraus, und nehmen wir an, es ist $\lambda \neq 0_K$. Dann gilt

$$v \quad = \quad 1_K v \quad = \quad (\lambda^{-1}\lambda)v \quad = \quad \lambda^{-1}(\lambda v) \quad = \quad \lambda^{-1} 0_V \quad = \quad 0_V \quad ,$$

wobei im letzten Schritt die bereits bewiesene Rechenregel $\mu 0_V = 0_V$ für alle $\mu \in K$ verwendet wurde. Beweisen wir nun noch die Gleichung $(-1_K)v = -v$. Es gilt $v + (-1_K)v = 1_K v + (-1_K)v = (1_K + (-1_K))v = 0_K v = 0_V$. Addition von $-v$ auf beiden Seiten liefert

$$v + (-1_K)v + (-v) = 0_V + (-v) \quad \Leftrightarrow \quad v + (-v) + (-1_K)v = -v \quad \Leftrightarrow$$

$$0_V + (-1_K)v = -v \quad \Leftrightarrow \quad (-1_K)v = -v$$ □

(6.4) Definition Sei V ein K-Vektorraum. Eine Teilmenge $U \subseteq V$ wird ***Untervektorraum*** von V genannt, wenn folgende Bedingungen erfüllt sind.

(i) $0_V \in U$
(ii) $v + w \in U$ für alle $v, w \in U$
(iii) $\lambda v \in U$ für alle $\lambda \in K$ und $v \in U$

Motiviert ist die Definition des Untervektorraumbegriffs durch den Wunsch, auf gewissen Teilmengen eines Vektoraums ebenfalls eine Vektorraumstruktur zu erhalten. Der folgende Satz zeigt, dass die Definition die gewünschte Funktion erfüllt.

(6.5) Satz Sei $(V,+,\cdot)$ ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum von V. Definieren wir Abbildungen $+_U : U \times U \to V$ und $\cdot_U : K \times U \to V$ durch

$$v +_U w \quad = \quad v + w \qquad \text{und} \qquad \lambda \cdot_U v \quad = \quad \lambda \cdot v \qquad \text{für} \quad v, w \in U \text{ und } \lambda \in K,$$

dann ist durch $(U, +_U, \cdot_U)$ ein K-Vektorraum gegeben.

Beweis: Weil U ein Untervektorraum ist, gilt $v + w \in U$ für alle $v, w \in U$, also auch $v +_U w = v + w \in U$. Dies zeigt, dass $+_U$ eine Abbildung $U \times U \to U$, also eine Verknüpfung auf U gegeben ist. Ebenso gilt $\lambda \cdot_U v = \lambda \cdot v \in U$ für alle $v \in U$ und $\lambda \in K$. Somit ist $\cdot_U$ eine Abbildung $\cdot_U : K \times U \to U$. Wir müssen nun überprüfen, dass $(U, +_U, \cdot_U)$ die Vektorraum-Bedingungen aus Definition (6.1) erfüllt.

Zunächst überprüfen wir, dass $(U, +_U)$ eine abelsche Gruppe ist. Für alle $u, v, w \in U$ gilt $(u +_U v) +_U w = (u + v) + w = u + (v + w) = u +_U (v +_U w)$, also ist das Assoziativgesetz erfüllt. Nach Voraussetzung liegt 0_V in U, und für alle $v \in U$ gilt $u +_U 0_V = u + 0_V = u$ und $0_V +_U u = 0_V + u = u$. Damit besitzt 0_V die Eigenschaften des Neutralelements in $(U, +_U)$. Sei nun $v \in U$ vorgegeben. Nach Voraussetzung liegt der Vektor $-v = (-1)v$ in U. Außerdem gilt $v +_U (-v) = v + (-v) = 0_V$ und $(-v) +_U v = (-v) + v = 0_V$. Also besitzt jedes $v \in U$ in $(U, +_U)$ ein Inverses, nämlich $-v$. Ingesamt bedeutet dies, dass $(U, +_U)$ eine Gruppe ist. Das Kommutativgesetz erhält man durch die Rechnung $v +_U w = v + w = w + v = w +_U v$ für alle $v, w \in U$.

Nun müssen wir noch die Eigenschaften (ii) (a)-(d) aus Definition (6.1) überprüfen. Seien dazu $v, w \in U$ und $\lambda, \mu \in K$ vorgegeben. Es gilt $(\lambda + \mu) \cdot_U v = (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v = \lambda \cdot_U v +_U \mu \cdot_U v$. Ebenso erhält man $\lambda \cdot_U (v +_U w) = \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w = \lambda \cdot_U v +_U \lambda \cdot_U w$. Weiter gilt $(\lambda\mu) \cdot_U v = (\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v) = \lambda \cdot_U (\mu \cdot_U v)$ und schließlich $1_K \cdot_U v = 1_K \cdot v = v$. □

Man sieht, dass das Nachrechnen der Vektorraum-Axiome in $(U, +_U, \cdot_U)$ eine ziemliche Routineangelegenheit war: Überall wurden nur die Symbole $+_U$ und $\cdot_U$ durch $+$ und $\cdot$ ersetzt und anschließend verwendet, dass die Axiome im Vektorraum V gültig sind.

Folgende konkrete Beispiele lassen sich für Untervektorräume angeben.

(i) Ist V ein beliebiger K-Vektorraum, dann sind $\{0_V\}$ und V Untervektorräume von V.

(ii) Für jedes $v \in V$ ist $\langle v \rangle_K = \{\lambda v \mid \lambda \in K\}$ ein Untervektorraum. Im Fall $v \neq 0_V$ bezeichnet man ihn als ***lineare Gerade***. Für beliebige v, w ist auch durch

$$\langle v, w \rangle_K \quad = \quad \{\lambda v + \mu w \mid \lambda, \mu \in K\}$$

ein Untervektorraum gegeben. Ist $v \neq 0_V$ und $w \notin \langle v \rangle_K$ (oder äquivalent, $v \notin \langle w \rangle_K$ und $w \notin \langle v \rangle_K$), dann nennt man $\langle v, w \rangle_K$ eine ***lineare Ebene***.

(6.6) Definition Eine Teilmenge $A \subseteq V$ wird ***affiner Unterraum*** von V genannt, wenn entweder $A = \emptyset$ gilt oder ein Untervektorraum U und ein Vektor $v \in V$ existieren, so dass

$$A \quad = \quad v + U \quad = \quad \{v + u \mid u \in U\} \qquad \text{erfüllt ist.}$$

Betrachten wir einige konkrete Beispiele für affine Unterräume.

(i) Seien $u, v \in V$. Dann ist $u + \langle v \rangle_K = \{u + \lambda v \mid \lambda \in K\}$ ein affiner Unterraum. Im Fall $v \neq 0_V$ bezeichnet man ihn als ***affine Gerade***.

(ii) Für beliebige $u, v, w \in V$ ist durch $u + \langle v, w \rangle_K = \{u + \lambda v + \mu w \mid \lambda, \mu \in K\}$ ein affiner Unterraum gegeben. Ist $v \neq 0_V$ und w kein skalares Vielfaches von v (also $w \neq \lambda v$ für alle $\lambda \in K$), dann nennt man $u + \langle v, w \rangle_K$ eine ***affine Ebene***.

(6.7) Proposition Sei V ein K-Vektorraum und $\emptyset \neq A \subseteq V$ ein affiner Unterraum.

(i) Es gibt *genau einen* Untervektorraum U von V, so dass die Gleichung $A = v + U$ für ein $v \in V$ erfüllt ist.
(ii) Für jeden Vektor $w \in A$ erfüllt der Untervektorraum U aus Teil (i) die Gleichung $A = w + U$.

Wir nennen U den ***zu*** A ***gehörenden Untervektorraum*** und bezeichnen ihn mit $\mathscr{L}(A)$.

Beweis: zu (i) Nehmen wir an, dass $v, v' \in V$ Vektoren und U, U' Untervektorräume von V mit $v + U = A = v' + U'$ sind. Wegen $v \in A$ gilt $v = v' + u_0$ für ein $u_0 \in U'$, und wegen $v' \in A$ gilt $v' = v + u_1$ für ein $u_1 \in U$. Der Differenzvektor $v' - v$ ist also sowohl in U als auch in U' enthalten. Wir beweisen nun die Gleichung $U = U'$.

„$\subseteq$“ Ist $u \in U$, dann liegt $v + u$ in A, und folglich gibt es ein $u' \in U'$ mit $v + u = v' + u'$. Es folgt $u = (v' - v) + u' \in U'$. „$\supseteq$“ Ist $u' \in U'$ vorgegeben, dann gilt $v' + u'$ in A, es gibt also ein $u \in U$ mit $v' + u' = v + u$. Daraus folgt $u' = (v - v') + u \in U$.

zu (ii) Sei $U = \mathscr{L}(A)$, $v \in V$ ein Vektor mit $A = v + U$ und $w \in A$ ein beliebiges Element. Dann gibt es ein $u \in U$ mit $w = v + u$. Wir beweisen nun die Gleichung $v + U = w + U$. „$\subseteq$“ Ist $v_1 \in v + U$, dann gibt es ein $u_1 \in U$ mit $v_1 = v + u_1$, und es folgt $v_1 = (w - u) + u_1 = w + (u_1 - u) \in w + U$. „$\supseteq$“ Ist $w_1 \in w + U$, dann existiert ein $u_1 \in U$ mit $w_1 = w + u_1$. Es folgt $w_1 = w + u_1 = (v + u) + u_1 = v + (u + u_1) \in v + U$. □

(6.8) Definition Seien $(V, +_V, \cdot_V)$ und $(W, +_W, \cdot_W)$ K-Vektorräume. Eine Abbildung $\phi : V \to W$ heißt ***K-lineare Abbildung*** oder ***Homomorphismus*** von K-Vektorräumen, wenn folgende Bedingungen erfüllt sind.

(i) $\phi(v +_V w) = \phi(v) +_W \phi(w)$ für alle $v, w \in V$
(ii) $\phi(\lambda \cdot_V v) = \lambda \cdot_W \phi(v)$ für alle $v \in V$ und $\lambda \in K$

Wenn aus dem Zusammenhang heraus klar ist, über welchem Körper die Vektorräume V und W definiert sind, wird statt von einer K-linearen auch einfach von einer linearen Abbildung gesprochen.

(6.9) Lemma Ist $\phi : V \to W$ eine lineare Abbildung. Dann gilt $\phi(0_V) = 0_W$, $\phi(-v) = -\phi(v)$ und $\phi(v-w) = \phi(v) - \phi(w)$ für alle $v, w \in V$.

Beweis: Die erste Gleichung erhält man mit Hilfe der Eigenschaft (ii) von linearen Abbildungen durch $\phi(0_V) = \phi(0_K \cdot_V 0_V) = 0_K \cdot_W \phi(0_V) = 0_W$. Die zweite ergibt sich durch die Rechnung

$$\phi(-v) \quad = \quad \phi((-1_K) \cdot_V v) \quad = \quad (-1)_K \cdot_W \phi(v) \quad = \quad -\phi(v).$$

Die dritte Gleichung schließlich erhält man durch

$$\phi(v-w) \quad = \quad \phi(v +_V (-w)) \quad = \quad \phi(v) +_W \phi(-w) \quad = \quad \phi(v) +_W (-\phi(w)) \quad = \quad \phi(v) - \phi(w). \qquad \square$$

Sei V ein K-Vektorraum, $n \in \mathbb{N}$, und seien $v_1, ..., v_n \in V$ beliebige Vektoren. Wir verwenden den Ausdruck $\sum_{k=1}^{n} v_k$ als Kurzschreibweise für die Summe $v_1 + ... + v_n$ in V.

(6.10) Lemma Seien V, W K-Vektorräume, $n \in \mathbb{N}$, außerdem $v_1, ..., v_n \in V$ und $\phi : V \to W$ eine lineare Abbildung. Dann gilt

$$\phi\left(\sum_{k=1}^{n} v_k\right) \quad = \quad \sum_{k=1}^{n} \phi(v_k).$$

Beweis: Wir beweisen die Aussage durch vollständige Induktion über n. Im Fall $n = 1$ lautet die Behauptung nur $\phi(v_1) = \phi(v_1)$ für alle $v_1 \in V$ und ist offensichtlich erfüllt. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für dieses n voraus. Seien $v_1, ..., v_{n+1} \in V$ beliebige Vektoren. Dann erhalten wir

$$\phi\left(\sum_{k=1}^{n+1} v_k\right) \quad = \quad \phi\left(\sum_{k=1}^{n} v_k + v_{n+1}\right) \quad = \quad \phi\left(\sum_{k=1}^{n} v_k\right) + \phi(v_{n+1}) \quad \stackrel{(*)}{=}$$

$$\sum_{k=1}^{n} \phi(v_k) + \phi(v_{n+1}) \quad = \quad \sum_{k=1}^{n+1} \phi(v_k) \quad ,$$

wobei an der Stelle (*) die Induktionsvoraussetzung angewendet wurde. $\square$

Wir haben in § 5 angemerkt, dass jedes $v \in K^n$ auf natürliche Weise mit einer Matrix in $\mathscr{M}_{1\times n,K}$ und auch mit einer Matrix in $\mathscr{M}_{n\times 1,K}$ identifiziert werden kann. Ist nun $A \in \mathscr{M}_{n,K}$ und betrachten wir $v \in K^n$ gemäß der zweiten Möglichkeit als Matrix mit einer Spalte und n Einträgen, dann können wir das Matrixprodukt $Av \in K^m$ bilden. Man bezeichnet den Vektor $w = Av$ dann als ***Matrix-Vektor-Produkt*** von A und v. Aus der Definition des Matrixprodukts ergibt sich, dass die Komponenten des Vektors w durch $w_i = \sum_{j=1}^{n} a_{ij} v_j$ gegeben sind, für $1 \le i \le m$.

(6.11) Proposition Seien $m, n \in \mathbb{N}$ und $A \in \mathscr{M}_{m\times n,K}$. Dann ist durch $\phi_A : K^n \to K^m$, $v \mapsto Av$ eine lineare Abbildung gegeben.

Beweis: Seien $v, w \in K^n$ und $\lambda \in K$ vorgegeben. Auf Grund der Rechenregeln für das Matrixprodukt aus Teil (i) von Proposition (5.15) gilt

$$\phi_A(v+w) = A(v+w) = Av + Aw = \phi_A(v) + \phi_A(w)$$

und $\phi_A(\lambda v) = A(\lambda v) = \lambda Av = \lambda \phi_A(v)$. $\square$

(6.12) Proposition Seien U, V, W drei K-Vektorräume und $\phi : U \to V$, $\psi : V \to W$ lineare Abbildungen. Dann ist $\psi \circ \phi$ eine lineare Abbildung von U nach W. Ist ϕ bijektiv, dann ist ϕ^{-1} eine lineare Abbildung von V nach U.

Beweis: Wir überprüfen die Linearität der Abbildung $\psi \circ \phi$. Seien dazu $v, w \in U$ und $\lambda \in K$ vorgegeben. Dann gilt

$$\begin{aligned}(\psi \circ \phi)(v +_U w) &= \psi(\phi(v +_U w)) = \psi(\phi(v) +_V \phi(w)) = \psi(\phi(v)) +_W \psi(\phi(w)) \\ &= (\psi \circ \phi)(v) +_W (\psi \circ \phi)(w)\end{aligned}$$

und $(\psi \circ \phi)(\lambda v) = \psi(\phi(\lambda v)) = \psi(\lambda\phi(v)) = \lambda\psi(\phi(v)) = \lambda(\psi \circ \phi)(v)$. Setzen wir nun voraus, dass ϕ bijektiv ist. Um zu zeigen, dass die Abbildung ϕ^{-1} linear ist, seien $v, w \in V$ und $\lambda \in K$ vorgegeben. Sei $v' = \phi^{-1}(v)$ und $w' = \phi^{-1}(w)$. Unter Verwendung der Linearität von ϕ erhalten wir

$$\begin{aligned}\phi^{-1}(v) +_U \phi^{-1}(w) &= v' +_U w' = \mathrm{id}_U(v' +_U w') = (\phi^{-1} \circ \phi)(v' +_U w') \\ &= \phi^{-1}(\phi(v' +_U w')) = \phi^{-1}(\phi(v') +_V \phi(w')) = \phi^{-1}(v +_V w).\end{aligned}$$

Ebenso gilt $\lambda\phi^{-1}(v) = \lambda v' = \mathrm{id}_U(\lambda v') = (\phi^{-1} \circ \phi)(\lambda v') = \phi^{-1}(\phi(\lambda v')) = \phi^{-1}(\lambda\phi(v')) = \phi^{-1}(\lambda v)$. □

(6.13) Definition Eine lineare Abbildung $\phi : V \to W$ heißt

(i) ***Monomorphismus*** (von K-Vektorräumen), wenn ϕ injektiv ist,
(ii) ***Epimorphismus***, wenn ϕ surjektiv ist,
(iii) ***Isomorphismus***, wenn ϕ bijektiv ist.

Eine lineare Abbildung $\phi : V \to V$ bezeichnet man als ***Endomorphismus*** von V, und ist sie außerdem bijektiv, dann spricht man von einem ***Automorphismus***. Zwei K-Vektorräume V, W werden ***isomorph*** genannt, wenn ein Isomorphismus $\phi : V \to W$ existiert.

(6.14) Folgerung Die Menge der Automorphismen eines K-Vektorraums V ist mit der Komposition $\circ$ von Abbildungen als Verknüpfung eine Gruppe. Man bezeichnet sie mit $\mathrm{GL}(V)$ und nennt sie die ***allgemeine lineare Gruppe*** des Vektorraums V.

Beweis: Proposition (6.12) zeigt, dass für gegebene Automorphismen ϕ, ψ des K-Vektorraums V auch die Abbildungen $\psi \circ \phi$ und ϕ^{-1} Automorphismen von V sind. Die Assoziativität ergibt sich aus der allgemeinen Regel $h \circ (g \circ f) = (h \circ g) \circ f$ für beliebige Abbildungen zwischen Mengen. Die identische Abbildung id_V besitzt die definierende Eigenschaft des Neutralelements (es gilt $\phi \circ \mathrm{id}_V = \mathrm{id}_V \circ \phi = \phi$ für jeden Automorphismus ϕ von V), und die Umkehrabbildung ϕ^{-1} von ϕ erfüllt die Bedingung $\phi^{-1} \circ \phi = \phi \circ \phi^{-1} = \mathrm{id}_V$ für das inverse Element. □

(6.15) Definition Eine Abbildung $\psi : V \to W$ zwischen zwei K-Vektorräumen wird ***affin-lineare*** Abbildung genannt, wenn eine lineare Abbildung $\phi : V \to W$ und ein Vektor $w \in W$ existieren, so dass $\psi(v) = w + \phi(v)$ für alle $v \in V$ erfüllt ist. Eine bijektive affin-lineare Abbildung $\psi : V \to V$ wird ***Affinität*** von V genannt.

(6.16) Proposition Seien V, W K-Vektorräume und $\phi : V \to W$ eine lineare Abbildung. Ferner seien $V' \subseteq V$ und $W' \subseteq W$ Untervektorräume. Dann sind die Teilmengen

$$\phi(V') = \{\phi(v) \mid v \in V'\} \qquad \text{und} \qquad \phi^{-1}(W') = \{v \in V \mid \phi(v) \in W'\}$$

Untervektorräume von W bzw. von V.

Beweis: Wir rechnen die Untervektorraum-Axiome für beide Teilmengen direkt nach. Seien $w, w' \in \phi(V')$ und $\lambda \in K$. Dann gibt es nach Definition von $\phi(V')$ Vektoren $v, v' \in V'$ mit $w = \phi(v)$ und $w' = \phi(v')$. Da V' ein Untervektorraum ist, gilt $v + v' \in V'$ und damit

$$w + w' = \phi(v) + \phi(v') = \phi(v + v') \quad \in \quad \phi(V').$$

Ebenso gilt $\lambda v \in V'$ auf Grund der Untervektorraum-Eigenschaft und somit $\lambda w = \lambda\phi(v) = \phi(\lambda v) \in \phi(V')$.

Nun zeigen wir, dass auch $\phi^{-1}(W')$ ein Untervektorraum ist. Seien dazu $v, v' \in \phi^{-1}(W')$ und $\lambda \in K$ vorgegeben. Dann gilt $\phi(v), \phi(v') \in W'$ und $\phi(v)+\phi(v') \in W'$, da W' ein Untervektorraum von W ist. Aus $\phi(v+v') = \phi(v)+\phi(v') \in W'$ folgt $v + v' \in \phi^{-1}(W')$. Da auch $\lambda\phi(v)$ in W' liegt, erhalten wir $\phi(\lambda v) = \lambda\phi(v) \in W'$ und somit $\lambda v \in \phi^{-1}(W')$. □

(6.17) Definition Seien V, W zwei K-Vektorräume und $\phi : V \to W$ eine lineare Abbildung. Dann nennt man

(i) $\ker(\phi) = \phi^{-1}(\{0_W\}) = \{\, v \in V \mid \phi(v) = 0_W \,\}$ den ***Kern*** und

(ii) $\mathrm{im}(\phi) = \phi(V) = \{\, \phi(v) \mid v \in V \,\}$ das ***Bild*** von ϕ.

Nach Prop. (6.16) ist $\ker(\phi)$ ein Untervektorraum von V und $\mathrm{im}(\phi)$ ein Untervektorraum von W.

(6.18) Proposition Seien V, W K-Vektorräume und $\phi : V \to W$ eine lineare Abbildung.

(i) Die Abbildung ϕ ist genau dann surjektiv, wenn $\mathrm{im}(\phi) = W$ gilt.

(ii) Sie ist genau dann injektiv, wenn $\ker(\phi) = \{0_V\}$ erfüllt ist.

Beweis: Aussage (i) ist nach Definition der Surjektivität unmittelbar klar. Zum Beweis von (ii) setzen wir zunächst voraus, dass ϕ injektiv ist. Die Inklusion $\{0_V\} \subseteq \ker(\phi)$ ist erfüllt, weil der Kern ein Untervektorraum von V ist. Zum Nachweis von $\ker(\phi) \subseteq \{0_V\}$ sei $v \in \ker(\phi)$ vorgegeben. Dann gilt $\phi(v) = 0_W = \phi(0_V)$, und aus der Injektivität von ϕ folgt $v = 0_V$.

Setzen wir nun umgekehrt die Gleichung $\ker(\phi) = \{0_V\}$ voraus, und beweisen wir die Injektivität von ϕ. Seien dazu $v, v' \in V$ mit $\phi(v) = \phi(v')$ vorgegeben. Dann gilt $\phi(v'-v) = \phi(v') - \phi(v) = 0_W$ und somit $v'-v \in \ker(\phi)$. Aus der Voraussetzung an den Kern folgt $v'-v = 0_V \Leftrightarrow v = v'$. □

(6.19) Definition Sei K ein Körper, und seien $m, n \in \mathbb{N}$. Ein ***lineares Gleichungssystem*** über K bestehend aus m Gleichungen in n Unbekannten $x_1, ..., x_n$ ist ein System von Gleichungen der Form

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ \vdots & & \vdots & & & & \vdots & = & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}$$

wobei $a_{ij} \in K$ und $b_i \in K$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ ist. Gilt $b_i = 0$ für $1 \leq i \leq m$, dann spricht man von einem ***homogenen***, ansonsten von einem ***inhomogenen*** LGS.

Mit Hilfe der Matrixschreibweise lässt sich ein lineares Gleichungssystem in deutlich kompakterer Form darstellen.

(6.20) Definition Die Matrix $A = (a_{ij})_{m \times n, K}$ in Definition (6.19) wird ***Koeffizientenmatrix*** des LGS genannt. Die Matrix $\tilde{A} = (\tilde{a}_{ij})_{m \times (n+1), K}$ gegeben durch $\tilde{a}_{ij} = a_{ij}$ für $1 \leq i \leq m$, $1 \leq j \leq n$ und $\tilde{a}_{i,n+1} = b_i$ für $1 \leq i \leq m$ heißt ***erweiterte Koeffizientenmatrix***. Bezeichnet x die $n \times 1$-Matrix mit den Einträgen $x_1, ..., x_n$, dann kann das lineare Gleichungssystem in der Form $Ax = b$ dargestellt werden. Die Menge

$$\mathscr{L} \quad = \quad \mathscr{L}_{A,b} \quad = \quad \{c \in K^n \mid Ac = b\}$$

bezeichnet man als ***Lösungsmenge***, deren Elemente als ***Lösungen*** des linearen Gleichungssystems. Ist $\mathscr{L}_{A,b} \neq \emptyset$, dann bezeichnet man $Ax = b$ als ***lösbar***. Besteht $\mathscr{L}_{A,b}$ aus einem einzigen Element, dann spricht man von ***eindeutiger Lösbarkeit***.

Wir zwei konkrete Beispiele über dem Körper $K = \mathbb{R}$ der reellen Zahlen. Das lineare Gleichungssystem

$$\begin{array}{ccccccccc} 3x & & & + & 2z & = & 8 \\ -x & + & 2y & + & 5z & = & -3 \\ & & 7y & - & 2z & = & -23 \end{array}$$

hat in Matrixschreibweise die Form $Ax = b$ mit

$$A = \begin{pmatrix} 3 & 0 & 2 \\ -1 & 2 & 5 \\ 0 & 7 & -2 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 8 \\ -3 \\ -23 \end{pmatrix}.$$

Die erweiterte Koeffizientenmatrix des Systems ist also gegeben durch

$$\tilde{A} = \begin{pmatrix} 3 & 0 & 2 & 8 \\ -1 & 2 & 5 & -3 \\ 0 & 7 & -2 & -23 \end{pmatrix}.$$

Mit den Methoden, die im nächsten Kapitel beschrieben werden, kann man ausrechnen, dass die Lösungsmenge des Systems durch $\mathscr{L}_{A,b} = \{(2,-3,1)\}$ gegeben ist. Das System ist also eindeutig lösbar. Betrachtet man dagegen das lineare Gleichungssystem

$$\begin{array}{rcrcrcr} 3x & + & 5y & - & 3z & = & -4 \\ 2x & - & 8y & + & 7z & = & 11 \\ 5x & - & 3y & + & 4z & = & 7 \end{array}$$

dann ist die Lösungsmenge gegeben durch

$$\mathscr{L} \quad = \quad \left\{ \begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 11 \\ -27 \\ -34 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}.$$

In diesem Fall liegt also Lösbarkeit, aber keine eindeutige Lösbarkeit vor.

(6.21) Satz Seien K ein Körper, $m,n \in \mathbb{N}$, $A \in \mathscr{M}_{m\times n,K}$ und $b \in K^m$. Dann ist $\mathscr{L}_{A,b}^{\text{hom}} = \mathscr{L}_{A,0}$ ein Untervektorraum des K^n. Ist das lineare Gleichungssystem $Ax = b$ lösbar und ist $c \in K^n$ eine Lösung, dann gilt $\mathscr{L}_{A,b} = c + \mathscr{L}_{A,b}^{\text{hom}}$. Die Lösungsmenge $\mathscr{L}_{A,b} \subseteq K^n$ ist also ein affiner Unterraum des K^n.

Beweis: Nach Proposition (6.11) ist $K^n \to K^m$, $v \mapsto Av$ eine lineare Abbildung, und $\mathscr{L}_{A,b}^{\text{hom}}$ ist der Kern dieser linearen Abbildung. Als Kern einer linearen Abbildung ist $\mathscr{L}_{A,b}^{\text{hom}}$ ein Untervektorraum im K^n. Für den Beweis der Gleichung $\mathscr{L}_{A,b} = c + \mathscr{L}_{A,b}^{\text{hom}}$ bemerken wir zunächst, dass $Ac = b$ gilt, weil c eine Lösung des Systems $Ax = b$ ist. Um die Inklusion „$\supseteq$“ nachzuweisen, sei $v \in c + \mathscr{L}_{A,b}^{\text{hom}}$, also $v = c + w$ für ein $w \in \mathscr{L}_{A,b}^{\text{hom}}$. Es gilt dann $Aw = 0_{K^m}$, und wir erhalten $Av = A(c+w) = Ac + Aw = b + 0_{K^m} = b$. Dies zeigt, dass v in $\mathscr{L}_{A,b}$ enthalten ist. Für den Nachweis von „$\subseteq$“ sei $v \in \mathscr{L}_{A,b}$. Dann gilt $Av = b$. Setzen wir $w = v - c$, dann folgt $Aw = A(v-c) = Av - Ac = b - b = 0_{K^m}$, also $w \in \mathscr{L}_{A,b}^{\text{hom}}$. Es folgt $v = c + w \in c + \mathscr{L}_{A,b}^{\text{hom}}$. □

Für die Anwendungen in den späteren Kapiteln führen wir noch einen weiteres wichtiges Beispiel für einen K-Vektorraum ein, den Vektorraum der linearen Abbildungen.

Sei K ein Körper, X eine Menge und V ein K-Vektorraum. Weiter sei $\text{Abb}(X,V)$ die Menge der Abbildungen $X \to V$. Wir definieren auf $\text{Abb}(X,V)$ eine Verknüpfung $+$, in dem wir $\varphi, \psi \in \text{Abb}(X,V)$ das Element $\varphi + \psi \in \text{Abb}(X,V)$ gegeben durch $(\varphi+\psi)(x) = \varphi(x) + \psi(x)$ für alle $x \in X$ zuordnen. Außerdem definieren wir eine Abbildung

$$\cdot : K \times \text{Abb}(X,V) \to \text{Abb}(X,V)\,,$$

indem wir für $\lambda \in K$ und $\varphi \in \text{Abb}(X,V)$ die das Element $\lambda \cdot \varphi$ gegeben durch $(\lambda\varphi)(x) = \lambda\varphi(x)$ für alle $x \in X$ definieren.

(6.22) Proposition Das Tripel $(\mathrm{Abb}(X,V),+,\cdot)$ ist ein K-Vektorraum.

Beweis: Wir müssen überprüfen, dass $(\mathrm{Abb}(X,V),+,\cdot)$ die in Definition (6.1) aufgezählten Eigenschaften besitzt. Zunächst überprüfen wir, dass es sich bei $(\mathrm{Abb}(X,V),+)$ um eine abelsche Gruppe handelt. Die Verknüpfung $+$ auf $\mathrm{Abb}(X,V)$, denn für alle $\varphi,\psi,\phi\in\mathrm{Abb}(X,V)$ und alle $x\in X$ gilt

$$\begin{aligned}((\varphi+\psi)+\phi)(x) &= (\varphi+\psi)(x)+\phi(x) = (\varphi(x)+\psi(x))+\phi(x) = \varphi(x)+(\psi(x)+\phi(x))\\ &= \varphi(x)+(\psi+\phi)(x) = (\varphi+(\psi+\phi))(x)\quad,\end{aligned}$$

also $(\varphi+\psi)+\phi=\varphi+(\psi+\phi)$. Ebenso gilt $(\varphi+\psi)(x)=\varphi(x)+\psi(x)=\psi(x)+\varphi(x)=(\psi+\varphi)(x)$ und somit $\varphi+\psi=\psi+\varphi$. Das Paar $(\mathrm{Abb}(X,V),+)$ ist somit eine abelsche Halbgruppe. Definieren wir $0_{\mathrm{Abb}(X,V)}$ durch $0_{\mathrm{Abb}(X,V)}(x)=0_V$ für alle $x\in X$, dann gilt für alle $\varphi\in\mathrm{Abb}(X,V)$ und alle $x\in X$ jeweils $(0_{\mathrm{Abb}(X,V)}+\varphi)(x)=0_{\mathrm{Abb}(X,V)}(x)+\varphi(x)=0_V+\varphi(x)=\varphi(x)$, also $0_{\mathrm{Abb}(X,V)}+\varphi=\varphi$. Auf Grund des bereits bewiesenen Kommutativgesetzes folgt daraus auch $\varphi+0_{\mathrm{Abb}(X,V)}=\varphi$. Damit ist gezeigt, dass $0_{\mathrm{Abb}(X,V)}$ in der Halbgruppe $(\mathrm{Abb}(X,V),+)$ ein Neutralelement ist, es sich also um ein Monoid handelt.

Sei schließlich $\varphi\in\mathrm{Abb}(X,V)$ vorgegeben und $-\varphi\in\mathrm{Abb}(X,V)$ gegeben durch $(-\varphi)(x)=-\varphi(x)$ für alle $x\in X$. Für jedes $x\in X$ gilt dann $((-\varphi)+\varphi)(x)=(-\varphi)(x)+\varphi(x)=(-\varphi(x))+\varphi(x)=0_V=0_{\mathrm{Abb}(X,V)}(x)$, also $\varphi+(-\varphi)=0_{\mathrm{Abb}(X,V)}$. Auf Grund des Kommutativgesetzes gilt auch $(-\varphi)+\varphi=0_{\mathrm{Abb}(X,V)}$. Jedes Element im Monoid $(\mathrm{Abb}(X,V),+)$ ist also invertierbar, somit ist $(\mathrm{Abb}(X,V),+)$ insgesamt eine abelsche Gruppe.

Nun überprüfen wir noch die übrigen in Definition (6.1) genannten Rechenregeln. Seien dazu $\lambda,\mu\in K$ und $\varphi,\psi\in\mathrm{Abb}(X,V)$ vorgegeben. Für jedes $x\in X$ gelten die Gleichungen

$$((\lambda+\mu)\cdot\varphi)(x) = (\lambda+\mu)\varphi(x) = \lambda\varphi(x)+\mu\varphi(x) = (\lambda\cdot\varphi)(x)+(\mu\cdot\varphi)(x) = ((\lambda\cdot\varphi)+(\mu\cdot\varphi))(x)$$

und

$$\begin{aligned}(\lambda\cdot(\varphi+\psi))(x) &= \lambda(\varphi+\psi)(x) = \lambda(\varphi(x)+\psi(x)) = \lambda\varphi(x)+\lambda\psi(x) =\\ &(\lambda\cdot\varphi)(x)+(\lambda\cdot\psi)(x) = (\lambda\cdot\varphi+\lambda\cdot\psi)(x)\quad,\end{aligned}$$

ebenso

$$((\lambda\mu)\cdot\varphi)(x) = (\lambda\mu)\varphi(x) = \lambda(\mu\varphi(x)) = \lambda((\mu\cdot\varphi)(x)) = (\lambda\cdot(\mu\cdot\varphi))(x)$$

und schließlich $(1_K\cdot\varphi)(x)=1_K\varphi(x)=\varphi(x)$. Es ist also $(\lambda+\mu)\cdot\varphi=\lambda\cdot\varphi+\mu\cdot\varphi$, $\lambda\cdot(\varphi+\psi)=\lambda\cdot\varphi+\lambda\cdot\psi$, $(\lambda\mu)\cdot\varphi=\lambda\cdot(\mu\cdot\varphi)$ und $1_K\cdot\varphi=\varphi$. □

(6.23) Satz Sei K ein Körper, und seien V und W zwei K-Vektorräume. Wir bezeichnen mit $\mathrm{Hom}_K(V,W)$ die Menge der linearen Abbildungen $V\to W$. Für vorgegebene $\varphi,\psi\in\mathrm{Hom}_K(V,W)$ und $\lambda\in K$ seien die Abbildungen $\varphi+\psi:V\to W$ und $\lambda\cdot\varphi:V\to W$ definiert durch $(\varphi+\psi)(v)=\varphi(v)+\psi(v)$ und $(\lambda\cdot\varphi)(v)=\lambda\varphi(v)$ für alle $v\in V$. Dann ist $(\mathrm{Hom}_K(V,W),+,\cdot)$ ein K-Vektorraum.

Beweis: Nach Proposition (6.22) ist $\mathrm{Abb}(V,W)$ ein K-Vektorraum. Nach Satz (6.5) genügt es zu zeigen, dass $\mathrm{Hom}_K(V,W)$ ein Untervektorraum dieses K-Vektorraums ist. Wie wir im Beweis der Proposition gesehen haben, ist der Nullvektor von $\mathrm{Abb}(V,W)$ gegeben durch $0_{\mathrm{Abb}(V,W)}(v) = 0_W$ für alle $v \in V$. Es handelt sich dabei um eine lineare Abbildung $V \to W$, also um ein Element von $\mathrm{Hom}_K(V,W)$, denn für alle $v, v' \in V$ und alle $\alpha \in V$ gilt $0_{\mathrm{Abb}(V,W)}(v+v') = 0_W = 0_W + 0_W = 0_{\mathrm{Abb}(V,W)}(v) + 0_{\mathrm{Abb}(V,W)}(v')$ und $0_{\mathrm{Abb}(V,W)}(\alpha v) = 0_W = \alpha 0_W = \alpha 0_{\mathrm{Abb}(V,W)}(v)$.

Seien nun $\varphi, \psi \in \mathrm{Hom}_K(V,W)$ und $\lambda \in K$ vorgegeben. Zu zeigen ist $\varphi + \psi \in \mathrm{Hom}_K(V,W)$ und $\lambda \cdot \varphi \in \mathrm{Hom}_K(V,W)$. Für den Nachweis seien $v, v' \in V$ und $\alpha \in K$ vorgegeben. Es gilt $(\varphi+\psi)(\alpha v) = \varphi(\alpha v) + \psi(\alpha v) = \alpha\varphi(v) + \alpha\psi(v) = \alpha(\varphi(v)+\psi(v)) = \alpha(\varphi+\psi)(v)$, wobei im zweiten Schritt verwendet wurde, dass φ und ψ lineare Abbildungen sind. Die Verträglichkeit von $\varphi + \psi$ mit der Vektoraddition erhält man durch die Rechnung

$$\begin{aligned}(\varphi+\psi)(v+v') \quad &= \quad \varphi(v+v') + \psi(v+v') \quad = \quad \varphi(v) + \varphi(v') + \psi(v) + \psi(v') \quad = \\ &\varphi(v) + \psi(v) + \varphi(v') + \psi(v') \quad = \quad (\varphi+\psi)(v) + (\varphi+\psi)(v').\end{aligned}$$

Damit ist insgesamt $\varphi + \psi \in \mathrm{Hom}_K(V,W)$ nachgewiesen. Ebenso erhält man $(\lambda\cdot\varphi)(v+v') = \lambda\varphi(v+v') = \lambda(\varphi(v) + \varphi(v')) = \lambda\varphi(v) + \lambda\varphi(v') = (\lambda\cdot\varphi)(v) + (\lambda\cdot\varphi)(v')$ und $(\lambda\cdot\varphi)(\alpha v) = \lambda\varphi(\alpha v) = \lambda\alpha\varphi(v) = \alpha\lambda\varphi(v) = \alpha(\lambda\cdot\varphi)(v)$. Also gilt auch $\lambda \cdot \varphi \in \mathrm{Hom}_K(V,W)$. □

§ 7. *Die Lösung linearer Gleichungssysteme*

Inhaltsübersicht

In diesem Kapitel behandeln wir ein allgemeines Verfahren, dass die Bestimmung der Lösungsmenge von beliebig großen LGS ermöglichst. Dabei gehen wir davon aus, dass das LGS durch seine erweiterte Koeffizientenmatrix (siehe § 6) gegeben ist. Diese Matrix bringt man durch eine fest vorgegebene Folge von Umformungsschritten auf eine sog. normierte Zeilenstufenform. Die Lösungsmenge kann dann auf einfache Weise von der Matrix abgelesen werden, egal ob diese leer oder einelementig ist, oder aus mehreren Elementen besteht. Neben dem Gaußschen Eliminationsverfahren beschäftigen wir uns mit Rechenoperationen für Matrizen und untersuchen, wie diese mit den elementaren Umformungen eines LGS aus dem ersten Kapitel zusammenhängen.

Wichtige Begriffe und Sätze

- (normierte) Zeilenstufenform (ZSF)
- Kennzahlen der ZSF, Zeilenköpfe, Rang einer Matrix in ZSF
- Einheitsvektoren
- Elementarmatrix, elementare Zeilen- bzw. Spaltenumformung
- Blockschreibweise für Matrizen
- Gauß'sches Eliminationsverfahren
- Invertierbarkeitskriterium für Matrizen

(7.1) Definition Eine Matrix $A \in \mathscr{M}_{m\times n,K}$ befindet sich in ***Zeilenstufenform*** (kurz ZSF), wenn $A = \mathbf{0}^{(\mathbf{m}\times\mathbf{n})}$ gilt oder folgende Bedingung erfüllt ist: Es gibt ein $r \in \{1,...,m\}$ und $j_1,...,j_r \in \{1,...,n\}$ mit $j_1 < j_2 < ... < j_r$, so dass

(i) $a_{ij_i} \neq 0_K$ für $1 \leq i \leq r$ und
(ii) $a_{ij} = 0_K$ für $j < j_i$ oder $i > r$

erfüllt ist. Man nennt r den ***Zeilenrang*** einer solchen Matrix. Das Tupel $(r, j_1, ..., j_r)$ bezeichnen wir insgesamt als die ***Kennzahlen*** der ZSF.

Die Positionen (i, j_i) mit $1 \leq i \leq r$ in der Matrix werden ***Zeilenköpfe*** genannt. Die Bedingung (i) besagt, dass die Einträge in den Zeilenköpfen ungleich Null sind. Nach Bedingung (ii) befinden sich links von den Zeilenköpfen nur Nulleinträge; in den „kopflosen" Zeilen sind alle Einträge gleich Null. Der Zeilenrang kann offenbar nie größer als $\min\{m, n\}$ werden.

(7.2) Definition Eine Matrix $A \in \mathscr{M}_{m\times n,K}$ befindet sich in ***normierter*** ZSF, wenn $A = \mathbf{0}^{(\mathbf{m\times n})}$ gilt oder wenn sie in ZSF mit den Kennzahlen $(r, j_1, ..., j_r)$ vorliegt und außerdem die folgenden Bedingungen erfüllt sind: Es gilt $a_{ij_i} = 1_K$ für $1 \le i \le r$ und $a_{kj_i} = 0_K$ für $1 \le i \le r$ und $1 \le k < i$.

Bei der normierten ZSF kommen also folgende Bedingungen hinzu: Die Einträge in den Zeilenköpfen sind gleich 1_K, und oberhalb der Zeilenköpfe befinden sich nur Nulleinträge. Bei einer Matrix A in normierter ZSF gilt also insgesamt $a_{ij} = 0$ in jedem der drei Fälle

$$(1) \quad i > r \qquad (2) \quad i \le r \text{ und } j < j_i \qquad (3) \quad j = j_k \text{ für ein } k \in \{1, ..., r\} \setminus \{i\};$$

in Worten, die Einträge der Matrix sind Null (1) unterhalb der r-ten Zeile, (2) links von den Spaltenköpfen und (3) in jeder Spalte, in der sich ein Zeilenkopf befindet, sind alle anderen Einträge gleich Null. Abgesehen davon können aber durchaus noch weitere Einträge von A gleich Null sein. Wir bemerken außerdem, dass eine Matrix $A \in \mathscr{M}_{m\times n,K}$ in normierter ZSF mit Zeilenrang $r = n$ in den oberen n Zeilen mit der Einheitsmatrix $E^{(n)}$ übereinstimmt, denn in diesem Fall muss $j_k = k$ für $1 \le k \le n$ gelten.

Wir geben einige konkrete Beispiele für Matrizen in Zeilenstufenform an.

$$A = \begin{pmatrix} 0 & 2 & 3 & 4 & 0 & 6 \\ 0 & 0 & 3 & 0 & 8 & 1 \\ 0 & 0 & 0 & 2 & 2 & 9 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Diese Matrix liegt in Zeilenstufenform vor, mit zugehörigen Kennzahlen $r = 4$, $j_1 = 2$, $j_2 = 3$, $j_3 = 4$ und $j_4 = 6$. Es besteht aber keine normierte Zeilenstufenform, denn beispielsweise sind die Einträge in den Zeilenköpfen $(1, 2)$, $(2, 3)$, $(3, 4)$ und $(4, 6)$ ungleich 1. Außerdem gibt es Einträge ungleich Null oberhalb der Zeilenköpfe.

$$B = \begin{pmatrix} 1 & 0 & 7 & 0 & 5 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Dies ist eine Matrix in normierter Zeilenstufenform, mit den Kennzahlen $r = 3$, $j_1 = 1$, $j_2 = 2$ und $j_3 = 4$. Auch die Einheitsmatrix

$$E^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

liegt in normierter Zeilenstufenform vor. Die Kennzahlen lauten $r = 4$ und $j_i = i$ für $1 \le i \le 4$.

Unser Ziel besteht darin, die Lösungsmenge eines linearen Gleichungssystems $Ax = b$ (mit $A \in \mathscr{M}_{n,K}$ und $b \in K^n$) zu bestimmen. Dabei konzentrieren wir uns zunächst auf den Fall, dass die erweiterte Koeffizientenmatrix $\tilde{A} = \left(Ab\right)$ in normierter Zeilenstufenform vorliegt. Nach Satz (6.21) genügt es, den Untervektorraum $\mathscr{L}_{A,b}^{\text{hom}} = \mathscr{L}_{A,0}$ von K^n und ein Element $c \in \mathscr{L}_{A,b}$ zu berechnen, denn dann gilt $\mathscr{L}_{A,b} = c + \mathscr{L}_{A,b}^{\text{hom}}$. Wir befassen uns als erstes mit der Bestimmung von $\mathscr{L}_{A,b}^{\text{hom}}$.

(7.3) Definition Für $1 \leq \ell \leq n$ bezeichnet $e_\ell \in K^n$ jeweils den ***ℓ-ten Einheitsvektor*** mit den Einträgen $e_{\ell j} = \delta_{\ell j}$.

In K^3 sind die drei Einheitsvektoren beispielsweise gegeben durch

$$e_1 = (1_K, 0_K, 0_K) \quad , \quad e_2 = (0_K, 1_K, 0_K) \quad \text{und} \quad e_3 = (0_K, 0_K, 1_K).$$

Sei nun A eine Matrix in normierter ZSF mit Kennzahlen $(r, j_1, ..., j_r)$. Um die Lösungsmenge $\mathscr{L}_{A,0}$ von $Ax = 0_{K^m}$ anzugeben, definieren wir

$$S = \{1, ..., n\} \setminus \{j_1, ..., j_r\}$$

und definieren für jede Zahl $\ell \in S$ einen Vektor $v_\ell \in K^m$ durch

$$v_\ell \quad = \quad e_\ell - \sum_{k=1}^{r} a_{k\ell} e_{j_k}.$$

Der Vektor v_ℓ entsteht also aus dem Nullvektor dadurch, dass man die ℓ-te Komponente auf 1_K setzt und die Einträge $-a_{1\ell}, ..., -a_{r\ell}$ der ℓ-ten Spalte auf die Positionen $j_1, ..., j_r$ des Vektors verteilt. Es gilt also

$$v_{\ell j_k} = -a_{k\ell} \text{ für } 1 \leq k \leq r \quad \text{und} \quad v_{\ell j} = \delta_{\ell j} \text{ für alle } \ell \in S.$$

Mit Hilfe dieser Vektoren lässt sich nun die Lösungsmenge folgendermaßen darstellen.

(7.4) Satz Sei $\mathscr{L}^{\text{hom}} \subseteq K^n$ die Lösungsmenge eines homogenen LGS mit Koeffizientenmatrix A, und seien S und die Vektoren v_ℓ für $\ell \in S$ definiert wie oben.

(i) Im Fall $S = \varnothing$ gilt $\mathscr{L}^{\text{hom}} = \{\, 0_{K^n} \,\}$.

(ii) Ist S nichtleer, dann ist die Lösungsmenge gegeben durch

$$\mathscr{L}^{\text{hom}} \quad = \quad \left\{ \sum_{\ell \in S} \lambda_\ell v_\ell \;\middle|\; \lambda_\ell \in K \;\forall\; \ell \in S \right\}.$$

Beweis: zu (i) Unter dieser Vorausssetzung gilt $\{j_1, ..., j_r\} = \{1, ..., n\}$, woraus wiederum $r = n$ und somit $m \geq n$ folgt. Wie oben ausgeführt, stimmen bei Zeilenrang n die ersten n Zeilen von A mit der Einheitsmatrix $E^{(n)}$ überein. Es gilt also $a_{ij} = \delta_{ij}$ für $1 \leq i, j \leq n$ und $a_{ij} = 0_K$ falls $i > n$. Wir erinnern außerdem daran, dass nach Definition $\mathscr{L}^{\text{hom}} = \{w \in K^n \mid Aw = 0_{K^m}\}$ gilt. Für jeden Vektor $w \in K^n$ erhalten wir die Äquivalenz

$$w \in \mathscr{L}^{\text{hom}} \quad \Leftrightarrow \quad Aw = 0_{K^m} \quad \Leftrightarrow \quad (Aw)_k = 0 \text{ für } 1 \leq k \leq m \quad \Leftrightarrow \quad \sum_{j=1}^{n} a_{kj} w_j = 0_K \text{ für } 1 \leq k \leq m$$
$$\Leftrightarrow \quad \sum_{j=1}^{n} \delta_{kj} w_j = 0_K \text{ für } 1 \leq k \leq n \quad \Leftrightarrow \quad w_k = 0_K \text{ für } 1 \leq k \leq n \quad \Leftrightarrow \quad w = 0_{K^n}.$$

zu (ii) Hier beschränken wir uns auf den Nachweis, dass für jedes $\ell \in S$ der Vektor v_ℓ in $\mathscr{L}^{\text{hom}}$ enthalten ist, also $\phi_A(v_\ell) = Av_\ell = 0_{K^m}$ gilt. Daraus ergibt sich zumindest die Inklusion „$\supseteq$“ der angegebenen Gleichung, denn für alle $\lambda_\ell \in K$ mit $\ell \in S$ folgt dann mit Lemma (6.10) jeweils

$$A\left(\sum_{\ell\in S}\lambda_\ell v_\ell\right) \quad = \quad \phi_A\left(\sum_{\ell\in S}\lambda_\ell v_\ell\right) \quad = \quad \sum_{\ell\in S}\phi_A(\lambda_\ell v_\ell) \quad = \quad \sum_{\ell\in S}\lambda_\ell \phi_A(v_\ell) \quad = \quad \sum_{\ell\in S}\lambda_\ell \cdot 0_{K^m} \quad = \quad 0_{K^m}.$$

Später werden wir dann sehen, wie man anhand der ℓ-ten Komponente erkennt, dass die Vektoren v_ℓ linear unabhängig sind und somit einen $(n-r)$-dimensionalen Untervektorraum des K^n bilden. Außerdem werden wir aus dem sog. *Dimensionssatz* für lineare Abbildungen herleiten, dass $\mathscr{L}^{\text{hom}}$ ebenfalls $(n-r)$-dimensional ist, wodurch aus der Inklusion „$\supseteq$“ die Übereinstimmung der beiden Mengen folgt.

Seien nun $\ell \in S$ und $i \in \{1, ..., m\}$ beliebig vorgegeben. Nach Definition der normierten Zeilenstufenform gilt $a_{ij_k} = \delta_{ik}$ für $1 \le k \le r$. Nach Definition des Vektors v_ℓ gilt $(v_\ell)_{j_k} = -a_{k\ell}$ für $1 \le k \le r$, $(v_\ell)_\ell = 1_K$ und $(v_\ell)_j = 0_K$ für alle übrigen $j \in \{1, ..., r\}$. Es folgt

$$\begin{aligned}(Av_\ell)_i \quad &= \quad \sum_{j=1}^{n} a_{ij}(v_\ell)_j \quad = \quad a_{i\ell}(v_\ell)_\ell + \sum_{k=1}^{r} a_{ij_k}(v_\ell)_{j_k} \quad = \quad a_{i\ell} + \sum_{k=1}^{r}\delta_{ik}\cdot(v_\ell)_{j_k} \\ &= \quad a_{i\ell} + (v_\ell)_{j_i} \quad = \quad a_{i\ell} + (-a_{i\ell}) \quad = \quad 0_K.\end{aligned}$$

Insgesamt gilt also tatsächlich $Av_\ell = 0_{K^m}$. □

Wir diskutieren eine Reihe von Anwendungsbeispielen für die soeben bewiesene Lösungsformel.

(i) Das homogene lineare Gleichungssystem $x_1 = 0$, $x_2 + 2x_3 = 0$ hat die Koeffizientenmatrix

$$A \quad = \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Es handelt sich um eine Matrix in normierter Zeilenstufenform mit den Kennzahlen $r = 2$, $j_1 = 1$, $j_2 = 2$. Es ist $S = \{1, 2, 3\} \setminus \{j_1, j_2\} = \{3\}$. Die Lösungsmenge ist somit $\mathscr{L}^{\text{hom}} = \{\lambda_3 v_3 \mid \lambda_3 \in \mathbb{R}\}$ mit dem Lösungsvektor

$$v_3 \quad = \quad \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}.$$

(ii) Das homogene lineare Gleichungssystem $x_1 = 0$, $x_3 = 0$ hat die Koeffizientenmatrix

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

Die Kennzahlen dieser normierten Zeilenstufenform lauten $r = 2$, $j_1 = 1$, $j_2 = 3$. Es ist $S = \{2\}$, und die Lösungsmenge ist gegeben durch $\mathscr{L}^{\text{hom}} = \{\lambda_2 v_2 \mid \lambda_2 \in \mathbb{R}\}$ mit

$$v_2 \quad = \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

(iii) Das homogene lineare Gleichungssystem $x_1 - 4x_3 + 5x_5 = 0$, $x_2 + 2x_3 = 0$, $x_4 = 0$ hat die Koeffizientenmatrix

$$A \quad = \quad \begin{pmatrix} 1 & 0 & -4 & 0 & 5 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

eine normierte ZSF mit den Kennzahlen $r = 3$, $j_1 = 1$, $j_2 = 2$, $j_3 = 4$. Hier ist $S = \{1, ..., 5\} \setminus \{j_1, j_2, j_3\} = \{3, 5\}$. Der Lösungsraum $\mathscr{L}^{\text{hom}} = \{\lambda_3 v_3 + \lambda_5 v_5 \mid \lambda_3, \lambda_5 \in K\}$ wird diesmal aufgespannt von den Vektoren

$$v_3 = \begin{pmatrix} 4 \\ -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad , \quad v_5 = \begin{pmatrix} -5 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(7.5) Satz Sei $\tilde{A} = (A \; b) \in \mathscr{M}_{m\times(n+1),K}$ die erweiterte Koeffizientenmatrix eines LGS und $\mathscr{L} \subseteq K^n$ dessen Lösungsmenge. Wir setzen voraus, dass $\tilde{A}$ in normierter ZSF vorliegt, mit den Kennzahlen r und $j_1, ..., j_r$.

(i) Ist $j_r = n + 1$, dann gilt $\mathscr{L} = \emptyset$.

(ii) Sei nun $j_r \leq n$. Wir definieren einen Vektor $w \in K^n$ durch $w = \sum_{k=1}^{r} b_k e_{j_k}$.
Dann gilt $w \in \mathscr{L}$.

Der spezielle Lösungsvektor w entsteht also einfach dadurch, dass man die Werte $b_1, ..., b_r$ auf die Positionen $j_1, ..., j_r$ verteilt und die übrigen Komponenten auf Null setzt. Es gilt also $w_{j_k} = b_k$ für $1 \leq k \leq r$ und $w_\ell = 0$ für alle $\ell \in S$.

Beweis: zu (i) Nehmen wir an, dass $\mathscr{L}$ nichtleer und w ein Element aus $\mathscr{L}$ ist. Dann gilt insbesondere $\sum_{j=1}^{n} a_{rj} w_j = b_r$. Wegen $j_r = n + 1$ gilt aber $a_{rj} = 0_K$ für $1 \leq j \leq n$ und $b_r = a_{r,n+1} = a_{r,j_r} = 1_K$. Setzen wir dies in die Gleichung ein, so erhalten wir $\sum_{j=1}^{n} 0_K w_j = 1_K$. Der Widerspruch $0_K = 1_K$ zeigt, dass unsere Annahme falsch war.

zu (ii) Zu zeigen ist $\sum_{j=1}^{n} a_{kj} w_j = b_k$ für $1 \leq k \leq m$. Sei $k \in \{1, ..., r\}$. Nach Definition der normierten ZSF gilt $a_{kj} = 0$ für $j < j_k$, und für $k \leq \ell \leq r$ ist $a_{\ell j_\ell} = 1$ der einzige Eintrag ungleich Null in der j_ℓ-ten Spalte. Es gilt also auch $a_{kj_\ell} = 0$ für $j > j_\ell$. Nach Definition des Vektors w erhalten wir für $1 \leq k \leq r$ somit

$$\sum_{j=1}^{n} a_{kj} w_j \quad = \quad \sum_{j=j_k}^{n} a_{kj} w_j \quad = \quad \sum_{\ell=k}^{r} a_{kj_\ell} b_\ell \quad = \quad a_{kj_k} b_k \quad = \quad 1 \cdot b_k \quad = \quad b_k.$$

Für $r < k \leq m$ gilt nach Eigenschaft (1) der normierten ZSF (Einträge unterhalb der r-ten Zeile gleich Null) sowohl $a_{kj} = 0$ für $1 \leq j \leq n$ als auch $b_k = 0$, also ebenfalls $\sum_{j=1}^{n} a_{kj} w_j = 0 = b_k$. Insgesamt ist die Gleichung $\sum_{j=1}^{n} a_{kj} w_j = b_k$ also tatsächlich für $1 \leq k \leq m$ erfüllt. □

Wir demonstrieren die Anwendung der Lösungsformel an einem konkreten Beispiel. Das inhomogene LGS $x_1 - 4x_3 + 5x_5 = -2$, $x_2 + 2x_3 = 7$, $x_4 = 5$ besitzt die erweiterte Koeffizientenmatrix

$$\tilde{A} \quad = \quad \begin{pmatrix} 1 & 0 & -4 & 0 & 5 & -2 \\ 0 & 1 & 2 & 0 & 0 & 7 \\ 0 & 0 & 0 & 1 & 0 & 5 \end{pmatrix}.$$

Es handelt sich um eine normierte Zeilenstufenform mit den Kennzahlen $r = 3$ und $j_1 = 1$, $j_2 = 2$, $j_3 = 4$. Nach Satz (7.5) ist $w = (-2, 7, 0, 5, 0) \in \mathbb{R}^5$ ein Lösungsvektor, was man durch Einsetzen in die Gleichungen des Systems unmittelbar überprüft: Es ist $(-2) - 4 \cdot 0 + 5 \cdot 0 = -2$, $7 + 2 \cdot 0 = 7$ und $5 = 5$.

Die Lösung linearer Gleichungssysteme mit Koeffizientenmatrix in normierter Zeilenstufenform haben wir damit vollständig geklärt. Dass die Lösung linearer Gleichungssysteme mit *beliebiger* Koeffizientenmatrix darauf zurückgeführt werden kann, beruht auf der folgenden einfachen Beobachtung.

> **(7.6) Proposition** Sei K ein Körper, und seien $m, n \in \mathbb{N}$. Sei $A \in \mathscr{M}_{m\times n,K}$ und $b \in K^m$. Dann gilt $\mathscr{L}_{A,b} = \mathscr{L}_{TA,Tb}$ für jede Matrix $T \in \mathrm{GL}_m(K)$. Mit anderen Worten, die Lösungsmenge eines LGS ändert sich nicht, wenn man beide Seiten der Gleichung $Ax = b$ von links mit einer invertierbaren Matrix multipliziert.

Beweis: Für jeden Vektor $c \in K^n$ gilt die Äquivalenz

$$c \in \mathscr{L}_{A,b} \quad \Leftrightarrow \quad Ac = b \quad \Leftrightarrow \quad TAc = Tb \quad \Leftrightarrow \quad c \in \mathscr{L}_{TA,Tb}.$$

Dabei kommt die Richtung „$\Leftarrow$“ im zweiten Schritt durch die Rechnung

$$TAc = Tb \quad \Rightarrow \quad T^{-1}TAc = T^{-1}Tb \quad \Rightarrow \quad E^{(m)}Ac = E^{(m)}b \quad \Rightarrow \quad Ac = b$$

zu Stande. □

Man beachte, dass sich die Lösungsmenge bei Multiplikation der Gleichung $Ax = b$ mit einer *nicht-invertierbaren* Matrix durchaus verändern kann. Multipliziert man beide Seiten zum Beispiel mit der Nullmatrix $0^{(m)}$, dann erhält man die Gleichung $0^{(m\times n)}x = 0_{K^m}$. Die Lösungsmenge dieses linearen Gleichungssystems ist der gesamte K^n (weil jeder Vektor $c \in K^n$ die Gleichung $0^{(m\times n)}c = 0_{K^m}$ erfüllt), unabhängig davon, wie die Lösungsmenge von $Ax = b$ ausgesehen hat.

Um nun ein Lösungsverfahren für beliebige LGS zu erhalten, brauchen wir also nur noch ein Verfahren, mit dem wir beliebige Matrizen in normierte Zeilenstufenform überführen können. Dazu verwenden wir die Rechenoperationen für Matrizen, die in § 7 eingeführt wurden. Bei Rechnungen mit Matrizen ist es oft günstig, diese in mehrere Bereiche aufzuteilen. Sei $A \in \mathscr{M}_{m\times n,K}$, seien k_1, k_2, ℓ_1, ℓ_2 natürliche Zahlen mit $1 \le k_1 \le k_2 \le m$, $1 \le \ell_1 \le \ell_2 \le n$, und außerdem $r = k_2 - k_1 + 1$, $s = \ell_2 - \ell_1 + 1$. Dann nennt man die Matrix $B \in \mathscr{M}_{r\times s,K}$ mit den Einträgen $b_{ij} = a_{k_1+i-1,\ell_1+j-1}$ für $1 \le i \le r$, $1 \le j \le s$ eine ***Teilmatrix*** von A; es handelt sich um einen „rechteckigen Ausschnitt“ der Matrix A.

Häufig verwendet man die sogenannte ***Blockschreibweise***, um Matrizen darzustellen, die aus bestimmten Teilmatrizen aufgebaut sind. So steht beispielsweise der Ausdruck

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

für die Matrix, deren linker oberer Teil aus den Einträgen von A und entsprechend in den übrigen drei Bereichen aus den Einträgen von B, C und D besteht. Dabei wird voraussetzt, dass untereinander stehende Matrizen (hier: A, C bzw. B, D) stets dieselbe Spaltenzahl und nebeneinander stehende Matrizen (A, B bzw. C, D) dieselbe Zeilenzahl haben. Das Rechnen mit Matrizen in Blockschreibweise wird durch eine Reihe von Rechenregeln vereinfacht.

(7.7) Proposition Seien A, B, C, D Matrizen über K.

(i) Stimmt die Spaltenzahl von A und B mit der Zeilenzahl von C überein, dann gilt

$$\begin{pmatrix} A \\ B \end{pmatrix} C \quad = \quad \begin{pmatrix} AC \\ BC \end{pmatrix}.$$

(ii) Stimmt die Spaltenzahl von A mit der Zeilenzahl von B und C überein, dann gilt

$$A\begin{pmatrix} B & C \end{pmatrix} \quad = \quad \begin{pmatrix} AB & AC \end{pmatrix}.$$

(iii) Stimmt die Spaltenzahl von A mit der Zeilenzahl von C und die Spaltenzahl von B mit der Zeilenzahl von D überein, dann gilt

$$\begin{pmatrix} A & B \end{pmatrix}\begin{pmatrix} C \\ D \end{pmatrix} \quad = \quad AC + BD.$$

Beweis: Wir beschränken uns auf den Beweis von (iii). Nach Voraussetzung gilt $A \in \mathscr{M}_{m\times n_1,K}$, $B \in \mathscr{M}_{m\times n_2,K}$, $C \in \mathscr{M}_{n_1\times r,K}$ und $D \in \mathscr{M}_{n_2\times r,K}$ für geeignete $m, n_1, n_2, r \in \mathbb{N}$. Die Matrix $AC + BD$ auf der rechten Seite ist in $\mathscr{M}_{m\times r,K}$ enthalten. Seien nun k, ℓ mit $1 \le k \le m$ und $1 \le \ell \le r$ vorgegeben. Zu zeigen ist, dass der Eintrag des Matrixprodukts links an der Position (k, ℓ) mit dem Eintrag der Matrix $AC + BD$ an derselben Stelle übereinstimmt. Um den Eintrag auf der linken Seite auszurechnen, muss die k-te Zeile des Faktors $(A \;\; B)$ mit der ℓ-ten Spalte des zweiten Faktors multipliziert werden. Dies liefert den Wert

$$\sum_{j=1}^{n_1} a_{kj}c_{j\ell} + \sum_{j=1}^{n_2} b_{kj}d_{j\ell}.$$

Die erste Summe entspricht dem Eintrag von AC an der Stelle (k, ℓ), die zweite Summe dem Eintrag von BD an derselben Position. Insgesamt erhalten wir also den Eintrag von $AC + BD$ an der Stelle (k, ℓ). □

Wir demonstrieren die Funktionsweise der Rechenregel (7.7) (iii) für Blockmatrizen anhand eines Beispiels und betrachten dazu die vier Matrizen

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad , \quad B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \quad , \quad C = \begin{pmatrix} 9 & 10 \\ 11 & 12 \end{pmatrix} \quad , \quad D = \begin{pmatrix} 13 & 14 \\ 15 & 16 \end{pmatrix}.$$

Es gilt

$$AC = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 9 & 10 \\ 11 & 12 \end{pmatrix} = \begin{pmatrix} 31 & 34 \\ 71 & 78 \end{pmatrix} \qquad \text{und} \qquad BD = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 13 & 14 \\ 15 & 16 \end{pmatrix} = \begin{pmatrix} 155 & 166 \\ 211 & 226 \end{pmatrix}$$

und somit

$$AC + BD \quad = \quad \begin{pmatrix} 155 & 166 \\ 211 & 226 \end{pmatrix} + \begin{pmatrix} 31 & 34 \\ 71 & 78 \end{pmatrix} \quad = \quad \begin{pmatrix} 186 & 200 \\ 282 & 304 \end{pmatrix}.$$

Eine direkte Multiplikation der zusammengesetzten Matrizen liefert dasselbe Ergebnis:

$$\Big(AB\Big)\begin{pmatrix} C \\ D \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 2 & 5 & 6 \\ 3 & 4 & 7 & 8 \end{pmatrix}\begin{pmatrix} 9 & 10 \\ 11 & 12 \\ 13 & 14 \\ 15 & 16 \end{pmatrix} \quad = \quad \begin{pmatrix} 186 & 200 \\ 282 & 304 \end{pmatrix}.$$

Allgemeiner kann gezeigt werden, dass man Matrizen mit beliebiger Aufteilung „blockweise“ multiplizieren kann, wobei lediglich vorausgesetzt werden muss, dass die Teilmatrizen, die dabei multipliziert werden sollen, „zusammenpassen“.

(7.8) Proposition Seien $m, n, r \in \mathbb{N}$, seien $A^{(i,j)}$ für $1 \leq i \leq m$, $1 \leq j \leq n$ und $B^{(j,k)}$ für $1 \leq j \leq n$ und $1 \leq k \leq r$ Matrizen mit der Eigenschaft, dass die Spaltenzahl von $A^{(i,j)}$ jeweils mit der Zeilenzahl von $B^{(j,k)}$ übereinstimmt, für alle i, j, k. Außerdem setzen wir voraus, dass die Zeilenzahlen von $A^{(i,j)}$ für festes i und die Spaltenzahlen von $B^{(j,k)}$ für festes k jeweils gleich sind. Dann gilt

$$\begin{pmatrix} A^{(1,1)} & \cdots & A^{(1,n)} \\ \vdots & & \vdots \\ A^{(m,1)} & \cdots & A^{(m,n)} \end{pmatrix}\begin{pmatrix} B^{(1,1)} & \cdots & B^{(1,r)} \\ \vdots & & \vdots \\ B^{(n,1)} & \cdots & B^{(n,r)} \end{pmatrix} \quad = \quad \begin{pmatrix} C^{(1,1)} & \cdots & C^{(1,r)} \\ \vdots & & \vdots \\ C^{(m,1)} & \cdots & C^{(m,r)} \end{pmatrix}$$

mit $C^{(i,k)} = \sum_{j=1}^{n} A^{(i,j)} B^{(j,k)}$ für $1 \leq i \leq m$ und $1 \leq k \leq r$.

Beweis: Wir geben den Beweis nur der Vollständigkeit halber an, für den weiteren Verlauf ist er ohne Belang. Für alle i, j, k sei $m_i \times n_j$ jeweils das Format der Matrix $A^{(i,j)}$ und $n_j \times r_k$ das Format der Matrix $B^{(j,k)}$. Dann hat die Matrix $C^{(i,k)}$ jeweils das Format $m_i \times r_k$. Wir bezeichnen die Matrix auf der rechten Seite der zu beweisenden Gleichung mit D und die Matrix auf der linken Seite mit C. Beide Matrizen haben das Format $m_0 \times r_0$ mit $m_0 = \sum_{i=1}^{m} m_i$ und $r_0 = \sum_{k=1}^{r} r_k$. Außerdem sei A die Matrix mit den Blöcken $A^{(i,j)}$ und B die Matrix mit den Blöcken $B^{(j,k)}$. Nach Definition gilt $D = AB$.

Seien nun $p \in \{1, ..., m_0\}$ und $q \in \{1, ..., r_0\}$ vorgegeben. Zu zeigen ist $c_{pq} = d_{pq}$. Der Eintrag d_{pq} kommt dadurch zu Stande, dass die p-te Zeile von A mit der q-ten Spalte von B multipliziert wird. Wir nehmen nun an, dass $i \in \{1, ..., m\}$ und $k \in \{1, ..., r\}$ so gewählt sind, dass die p-te Zeile der Matrix A durch die f-ten Zeilen der Matrizen $A^{(i,1)}, A^{(i,2)}, ..., A^{(i,n)}$ läuft, und ebenso die q-te Spalte von B durch die g-ten Spalten der Matrizen $B^{(1,k)}, B^{(2,k)}, ..., B^{(n,k)}$. Dabei ist $f \in \{1, ..., m_i\}$ und $g \in \{1, ..., r_k\}$. Setzen wir $n_0 = \sum_{j=1}^{n} n_j$, dann gilt

$$d_{pq} \quad = \quad \sum_{j=1}^{n_j} a_{pj} b_{jq} \quad = \quad \sum_{j=1}^{n} \sum_{\ell=1}^{n_j} a_{f\ell}^{(i,j)} b_{\ell g}^{(j,k)}.$$

Nun läuft die p-te Zeile von C auch durch die f-ten Zeilen der Matrizen $C^{(i,1)}, C^{(i,2)}, ..., C^{(i,n)}$, und die q-te Spalte von C entsprechend durch die g-ten Spalten der Matrizen $C^{(1,k)}, C^{(2,k)}, ..., C^{(n,k)}$. Wegen $C^{(i,k)} = \sum_{j=1}^{n} A^{(i,j)}B^{(j,k)}$ für $1 \leq i \leq m$ und $1 \leq k \leq r$ erhalten wir dann wie gewünscht

$$c_{pq} \quad = \quad c_{fg}^{(i,k)} \quad = \quad \sum_{j=1}^{n} (A^{(i,j)}B^{(j,k)})_{fg} \quad = \quad \sum_{j=1}^{n}\sum_{\ell=1}^{n_j} a_{f\ell}^{(i,j)} b_{\ell g}^{(j,k)} \quad = \quad d_{pq}. \qquad \square$$

(7.9) Definition Eine Matrix aus $\mathscr{M}_{m,K}$ der Form $\mathrm{M}_{k,\lambda} = E^{(m)} + (\lambda - 1)B_{kk}^{(m\times m)}$ mit $k \in \{1, ..., m\}$ und $\lambda \in K^\times$ oder der Form $\mathrm{A}_{k,\ell,\lambda} = E^{(m)} + \lambda B_{\ell k}^{(m\times m)}$ mit $k, \ell \in \{1, ..., m\}$ und $\lambda \in K$ wird ***Elementarmatrix*** genannt.

In Blockschreibweise hat die Elementarmatrix $\mathrm{M}_{k,\lambda}$ die Form

$$\mathrm{M}_{k,\lambda} \quad = \quad \begin{pmatrix} E^{(k-1)} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E^{(m-k)} \end{pmatrix}$$

wobei die Einträge $\mathbf{0}$ jeweils für Nullmatrizen der passenden Größe stehen. Die Elementarmatrix $\mathrm{A}_{k,\ell,\lambda}$ hat im Fall $k < \ell$ bzw. $k > \ell$ die Form

$$\mathrm{A}_{k,\ell,\lambda} \quad = \quad \begin{pmatrix} E^{(k-1)} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E^{(\ell-k-1)} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \lambda & \mathbf{0} & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & E^{(m-\ell)} \end{pmatrix}$$

beziehungsweise

$$\mathrm{A}_{k,\ell,\lambda} \quad = \quad \begin{pmatrix} E^{(\ell-1)} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 1 & \mathbf{0} & \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E^{(k-\ell-1)} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & E^{(m-k)} \end{pmatrix}$$

(7.10) Proposition Sei $A \in \mathscr{M}_{m\times n,K}$.

(i) Sei $\lambda \in K^\times$ und $k \in \{1, ..., m\}$. Multipliziert man die Matrix A von links mit der Elementarmatrix $\mathrm{M}_{k,\lambda}$, so bewirkt dies eine Multiplikation der k-ten Zeile mit dem Wert λ.

(ii) Seien $k, \ell \in \{1, ..., m\}$ mit $k \neq \ell$ und $\lambda \in K$. Multipliziert man die Matrix A mit der Elementarmatrix $\mathrm{A}_{k,\ell,\lambda}$, dann wird das λ-fache der k-ten Zeile zur ℓ-ten Zeile von A addiert.

Beweis: zu (i) Sei $B \in \mathscr{M}_{(k-1)\times n,K}$ die Teilmatrix bestehend aus den oberen $k-1$ und $C \in \mathscr{M}_{(m-k)\times n,K}$ die Teilmatrix bestehend aus den unteren $m-k$ Zeilen von A. Ferner sei $z \in \mathscr{M}_{1\times n,K}$ die k-te Zeile von A. Dann gilt

$$\mathrm{M}_{k,\lambda}A = \begin{pmatrix} E^{(k-1)} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E^{(m-k)} \end{pmatrix}\begin{pmatrix} B \\ z \\ C \end{pmatrix} = \begin{pmatrix} E^{(k-1)}B + \mathbf{0z} + \mathbf{0C} \\ \mathbf{0B} + \lambda\mathbf{z} + \mathbf{0C} \\ \mathbf{0B} + \mathbf{0z} + \mathbf{E^{(m-k)}C} \end{pmatrix} = \begin{pmatrix} B \\ \lambda z \\ C \end{pmatrix}$$

zu (ii) Hier beschränken wir uns auf den Fall $k < \ell$ und teilen die Matrix A auf in die Matrix $B \in \mathscr{M}_{(k-1)\times n,K}$ bestehend aus den ersten $k-1$ Zeilen, der Matrix $C \in \mathscr{M}_{(\ell-k-1)\times n,K}$ bestehend aus der $(k+1)$-ten bis zur $(\ell-1)$-ten Zeile und der Matrix $D \in \mathscr{M}_{(m-\ell)\times n,K}$ bestehend aus den unteren $m-\ell$ Zeilen. Ferner seien $z_k, z_\ell \in \mathscr{M}_{1\times n,K}$ die k-te und ℓ-te Zeile von A. Dann erhalten wir

$$\mathrm{A}_{k,\ell,\lambda}A = \begin{pmatrix} E^{(k-1)} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E^{(\ell-k-1)} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \lambda & \mathbf{0} & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & E^{(m-\ell)} \end{pmatrix}\begin{pmatrix} B \\ z_k \\ C \\ z_\ell \\ D \end{pmatrix} = \begin{pmatrix} B \\ z_k \\ C \\ \lambda z_k + z_\ell \\ D \end{pmatrix}$$

□

Wir zeigen anhand zweier Beispiele, dass die Multiplikation mit Elementarmatrizen tatsächlich den angegebenen Effekt hat. Die Multiplikation einer dreizeiligen Matrix mit $\mathrm{M}_{2,3}$ von links bewirkt eine Multiplikation der zweiten Zeile mit dem Wert 3. Zum Beispiel gilt

$$\mathrm{M}_{2,3}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 15 & 18 & 21 & 24 \\ 9 & 10 & 11 & 12 \end{pmatrix}.$$

Ebenso bewirkt die Multiplikation mit $\mathrm{A}_{1,3,2}$ von links, dass das zweifache der ersten Zeile zur dritten addiert wird, zum Beispiel

$$\mathrm{A}_{1,3,2}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 11 & 14 & 17 & 20 \end{pmatrix}.$$

Die in der Proposition beschriebenen Umformungen werden ***elementare Zeilenumformungen*** genannt. Jede elementare Zeilenumformung einer Matrix A lässt sich also durch Multiplikation mit einer Elementarmatrix von links realisieren. Dementsprechend führt die Multiplikation von A mit einem Produkt $E_m \cdot E_{m-1} \cdot \ldots \cdot E_1$ von Elementarmatrizen dazu, dass A einer Folge von m Zeilenumformungen unterworfen wird. Wir bezeichnen die Menge aller Matrizen in $\mathscr{M}_{m,K}$, die sich als Produkt von Elementarmatrizen schreiben lassen, mit $\mathscr{E}_m(K)$. Übrigens lässt sich auch die Vertauschung von Zeilen durch eine Folge von elementaren Umformungen wie oben beschrieben bewerkstelligen, wie man an dem Schema

$$\begin{pmatrix} a_{k\bullet} \\ a_{\ell\bullet} \end{pmatrix} \xrightarrow{\mathrm{A}_{k,\ell,1}} \begin{pmatrix} a_{k\bullet} \\ a_{k\bullet} + a_{\ell\bullet} \end{pmatrix} \xrightarrow{\mathrm{M}_{k,-1}} \begin{pmatrix} -a_{k\bullet} \\ a_{k\bullet} + a_{\ell\bullet} \end{pmatrix} \xrightarrow{\mathrm{A}_{\ell,k,1}} \begin{pmatrix} a_{\ell\bullet} \\ a_{k\bullet} + a_{\ell\bullet} \end{pmatrix} \xrightarrow{\mathrm{A}_{k,\ell,-1}} \begin{pmatrix} a_{\ell\bullet} \\ a_{k\bullet} \end{pmatrix}$$

erkennt. Mit Hilfe des Matrixkalküls werden wir nun zeigen, dass sich jede Matrix durch eine endliche Anzahl von Zeilenumformungen auf normierte Zeilenstufenform bringen lässt.

(7.11) Lemma Sei $A \in \mathscr{M}_{m\times 1,K}$ eine Matrix, die aus einer einzigen Spalte besteht, also eine Matrix der Form $A = {}^{t}(a_1\ a_2\ \ldots\ a_m)$. Sind nicht alle Einträge von A gleich Null, dann gibt es ein Produkt $E \in \mathscr{E}_m(K)$ von Elementarmatrizen mit $EA = {}^{t}(1_K\ 0_K\ 0_K\ \ldots\ 0_K)$.

Beweis: Auf Grund unserer Vorbemerkung genügt es zu zeigen, dass A durch eine endliche Abfolge von elementaren Zeilenumformungen auf die Gestalt ${}^{t}(1\ 0\ \ldots\ 0)$ gebracht werden kann. Auch Vertauschungen von Zeilen sind zulässig, weil diese (wie oben gesehen) durch endlich viele elementare Umformungen realisierbar sind. Nach Voraussetzung gibt es ein $k \in \{1,\ldots,m\}$ mit $a_k \neq 0_K$. Nach Multiplikation der k-ten Zeile mit a_k^{-1} und Vertauschung der k-ten mit der ersten Zeile gilt $a_1 = 1_K$. Nun addieren wir für $\ell = 2,\ldots,m$ jeweils das $(-a_\ell)$-fache der ersten Zeile zur ℓ-ten. Dies führt dazu, dass sämtliche Einträge der Matrix mit Ausnahme des ersten zu Null werden. □

(7.12) Satz Jede Matrix $A \in \mathscr{M}_{m\times n,K}$ kann durch endlich viele elementare Zeilenumformungen auf normierte ZSF gebracht werden. Eine äquivalente Formulierung dieser Aussage lautet: Es gibt eine Matrix $E \in \mathscr{E}_m(K)$, so dass EA in normierter ZSF vorliegt.

Beweis: Wir zeigen zunächst, dass A auf ZSF gebracht werden kann und führen den Beweis durch vollständige Induktion über die Anzahl n der Spalten. Der Fall $n = 1$ ist mit Lemma (7.11) bereits erledigt, denn nach Definition ist ${}^{t}(1_K\ 0_K\ \ldots\ 0_K)$ eine Matrix in ZSF (mit den Kennzahlen $r = j_1 = 1$). Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für dieses n voraus. Sei außerdem $A \in \mathscr{M}_{m\times(n+1),K}$ eine beliebige Matrix. Wir müssen zeigen, dass A auf ZSF gebracht werden kann und unterscheiden dafür zwei Fälle.

1. Fall: Die erste Spalte von A hat nur Nulleinträge.
Dann hat A die Form $(\mathbf{0}^{(\mathbf{m\times 1})}\ \mathbf{B})$ mit einer Matrix $B \in \mathscr{M}_{m\times n,K}$. Nach Induktionsvoraussetzung gibt es eine Matrix $E \in \mathscr{E}_m(K)$, so dass $B' = EB$ in ZSF vorliegt, mit gewissen Kennzahlen $r, j_1, \ldots, j_r$. Es gilt

$$EA \quad = \quad E(\mathbf{0}^{(\mathbf{m\times 1})}\ \mathbf{B}) \quad = \quad (\mathbf{0}^{(\mathbf{m\times 1})}\ \mathbf{EB}) \quad = \quad (\mathbf{0}^{(\mathbf{m\times 1})}\ \mathbf{B}').$$

Wie man leicht überprüft, liegt auch $(\mathbf{0}^{(\mathbf{m\times 1})}\ \mathbf{B}')$ die Matrix in ZSF vor, mit den Kennzahlen $r, j_1 + 1, \ldots, j_r + 1$.

2. Fall: Die erste Spalte von A hat Einträge ungleich Null.
In diesem Fall kann A in der Blockgestalt

$$A \quad = \quad \begin{pmatrix} a_{11} & z \\ s & C \end{pmatrix}$$

dargestellt werden, mit $a_{11} \in K$, $z \in \mathscr{M}_{1\times n,K}$, $s \in \mathscr{M}_{(m-1)\times 1,K}$ und $C \in \mathscr{M}_{(m-1)\times n,K}$, wobei die Teilmatrix ${}^{t}(a_{11}s)$ nicht nur Nulleinträge enthält. Nach Lemma (7.11) gibt es eine Matrix $E \in \mathscr{E}_m(K)$ mit

$$E\begin{pmatrix} a_{11} \\ s \end{pmatrix} \quad = \quad \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix}$$

und wir erhalten

$$EA \quad = \quad \begin{pmatrix} 1 & z' \\ \mathbf{0} & C' \end{pmatrix}$$

mit geeigneten Matrizen $z' \in \mathscr{M}_{1\times n,K}$ und $C' \in \mathscr{M}_{(m-1)\times n,K}$. Nach Induktionsvoraussetzung existiert nun eine Matrix $E' \in \mathscr{E}_{m-1}(K)$, so dass $E'C'$ in ZSF vorliegt, mit gewissen Kennzahlen $r, j_1, ..., j_r$. Außerdem gilt

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & E' \end{pmatrix}\begin{pmatrix} 1 & z' \\ \mathbf{0} & C' \end{pmatrix} = \begin{pmatrix} 1 & z' \\ \mathbf{0} & E'C' \end{pmatrix}$$

Wieder überprüft man, dass sich die Matrix rechts in ZSF befindet, mit Kennzahlen $r+1, 1, j_1+1, ..., j_r+1$. Anhand der Gleichung

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & U \end{pmatrix}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & V \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & UV \end{pmatrix}$$

für Blockmatrizen sieht man, dass mit E' auch die Matrix

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & E' \end{pmatrix}$$

als Produkt von Elementarmatrizen darstellbar ist.

Zu zeigen bleibt, dass jede Matrix in ZSF durch elementare Zeilenumformungen auf *normierte* ZSF gebracht werden kann. Dazu setzen wir voraus, dass A bereits in ZSF mit den Kennzahlen $r, j_1, ..., j_r$ vorliegt. Um $a_{ij_i} = 1$ für $1 \leq i \leq r$ zu erreichen, dividiert man einfach für jedes i die i-te Zeile durch a_{ij_i}. Die ZSF der Matrix wird durch diese Operation nicht zerstört, da die Eigenschaft eines Eintrages, gleich Null oder ungleich Null zu sein, dadurch nicht verändert wird.

Die Bedingung $a_{kj_i} = 0$ für $k < i$ kann dadurch erfüllt werden, dass man nacheinander für die Zeilennummern $i = r, r-1, r-2, ..., 1$ jeweils das a_{kj_i}-fache der i-ten Zeile von der k-ten Zeile subtrahiert, für $1 \leq k < i$. Dabei ist darauf zu achten, dass in keinem Schritt die ZSF beeinträchtigt wird und die erreichte Form für die Spalten j_ℓ mit $\ell > i$ erhalten bleibt. Die ZSF bleibt erhalten, da die i-te Zeile ihren ersten Eintrag $\neq 0$ erst in der Spalte j_i hat und $j_i > j_k$ für $1 \leq k < i$ gilt. Somit werden weder die Zeilenköpfe der darüberliegenden Zeilen noch die Einträge links davon verändert. Die Zeilen unterhalb der i-ten bleiben völlig unverändert. Auch die Bedingung $a_{kj_\ell} = 0$ für $\ell > i$ und $k < \ell$ bleibt erhalten, da der einzige Eintrag ungleich Null in der j_ℓ-ten Spalte der Eintrag $a_{\ell j_\ell} = 1$ ist, und dieser spielt wegen $\ell > i$ bei der Zeilenumformung keine Rolle. □

Man kann sich an diesem „induktiven“ Beweisschema orientieren, um eine beliebige, konkret vorgegebene Matrix $A \in \mathscr{M}_{m\times n,K}$ zunächst auf Zeilenstufenform und dann auf normierte Zeilenstufenform zu bringen.

Damit haben wir nun insgesamt ein vollständiges Verfahren zur Verfügung, um die Lösungsmenge eines beliebigen linearen Gleichungssystems der Form $Ax = b$ (mit $A \in \mathscr{M}_{m\times n,K}$ und $b \in K^n$) vollständig zu bestimmen. Dieses Verfahren wird auch als ***Gauß'sches Eliminationsverfahren*** bezeichnet.

Zunächst bringt man die erweiterte Koeffizientenmatrix $\tilde{A} = \begin{pmatrix} A & b \end{pmatrix} \in \mathscr{M}_{m\times(n+1),K}$ durch eine Folge von Zeilenumformungen auf normierte Zeilenstufenform. Durch Proposition (7.6) ist gewährleistet, dass sich die Lösungsmenge des Systems durch die Umformungen nicht ändert. An der umgeformten Matrix liest man eine spezielle Lösung $c \in L_{A,b}$ des Systems ab, und an der linken $m \times n$-Teilmatrix den Lösungsraum $\mathscr{L}^{\text{hom}}_{A,b}$. Wie oben erläutert, gilt dann $\mathscr{L}_{A,b} = c + \mathscr{L}^{\text{hom}}_{A,b}$.

Wir illustrieren die Vorgehensweise anhand der beiden linearen Gleichungssysteme

$$\begin{array}{rcrcrcr} 3x & & & + & 2z & = & 8 \\ -x & + & 2y & + & 5z & = & -3 \\ & & 7y & - & 2z & = & -23 \end{array} \qquad \text{und} \qquad \begin{array}{rcrcrcr} 3x & + & 5y & - & 3z & = & -4 \\ 2x & - & 8y & + & 7z & = & 11 \\ 5x & - & 3y & + & 4z & = & 7 \end{array}$$

aus § 6. Die erweiterte Koeffizientenmatrix des ersten Systems wird durch die Schritte

$$\begin{pmatrix} 3 & 0 & 2 & 8 \\ -1 & 2 & 5 & -3 \\ 0 & 7 & -2 & -23 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -2 & -5 & 3 \\ 3 & 0 & 2 & 8 \\ 0 & 7 & -2 & -23 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -2 & -5 & 3 \\ 0 & 6 & 17 & -1 \\ 0 & 7 & -2 & -23 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -2 & -5 & 3 \\ 0 & 6 & 17 & -1 \\ 0 & 1 & -19 & -22 \end{pmatrix} \mapsto$$

$$\begin{pmatrix} 1 & -2 & -5 & 3 \\ 0 & 1 & -19 & -22 \\ 0 & 6 & 17 & -1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -2 & -5 & 3 \\ 0 & 1 & -19 & -22 \\ 0 & 0 & 131 & 131 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -2 & -5 & 3 \\ 0 & 1 & -19 & -22 \\ 0 & 0 & 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -2 & 0 & 8 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

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

auf normierte Zeilenstufenform gebracht. An der umgeformten Matrix kann die spezielle Lösung $(2,-3,1)$ abgelesen werden. Auch die linke 3×3-Teilmatrix befindet sich in normierter Zeilenstufenform, mit den Kennzahlen $r=3$, $j_1=1$, $j_2=2$, $j_3=3$. Mit der Notation von oben gilt $S=\varnothing$. Dies zeigt, dass $\mathscr{L}_{A,b}^{\text{hom}}=\{(0,0,0)\}$ gilt und somit die gesamte Lösungsmenge durch $\mathscr{L}_{A,b}=\{(2,-3,1)\}$ gegeben ist.

Beim zweiten System ergeben die Umformungsschritte

$$\begin{pmatrix} 3 & 5 & -3 & -4 \\ 2 & -8 & 7 & 11 \\ 5 & -3 & 4 & 7 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 13 & -10 & -15 \\ 2 & -8 & 7 & 11 \\ 5 & -3 & 4 & 7 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 13 & -10 & -15 \\ 0 & -34 & 27 & 41 \\ 0 & -68 & 54 & 82 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 13 & -10 & -15 \\ 0 & 1 & -\frac{27}{34} & -\frac{41}{34} \\ 0 & -68 & 54 & 82 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 13 & -10 & -15 \\ 0 & 1 & -\frac{27}{34} & -\frac{41}{34} \\ 0 & 0 & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 13 & -10 & -15 \\ 0 & 1 & -\frac{27}{34} & -\frac{41}{34} \\ 0 & 0 & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & \frac{11}{34} & \frac{23}{34} \\ 0 & 1 & -\frac{27}{34} & -\frac{41}{34} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Hier lesen wir mit dem Verfahren von oben die spezielle Lösung $(\frac{23}{34},-\frac{41}{34},0)$ ab. Die Kennzahlen der normierten ZSF in der linken 3×3-Teilmatrix lauten $r=2$, $j_1=1$, $j_2=2$. Es gilt also $S=\{3\}$, und an der Teilmatrix kann der Basisvektor $v_3=(-\frac{11}{34},\frac{27}{34},1)$ des Lösungsraums $\mathscr{L}_{A,b}^{\text{hom}}$ abgelesen werden. Insgesamt erhalten wir die Lösungsmenge

$$\mathscr{L}_{A,b} = \left\{ \begin{pmatrix} \frac{23}{34} \\ -\frac{41}{34} \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} -\frac{11}{34} \\ \frac{27}{34} \\ 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix} + \lambda \begin{pmatrix} -\frac{11}{34} \\ \frac{27}{34} \\ 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix} + \lambda \begin{pmatrix} -11 \\ 27 \\ 34 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}$$

Hier haben die Darstellung der Lösungsmenge in den beiden folgenden Schritten etwas optimiert: Im ersten Schritt haben wir verwendet, dass neben $(\frac{23}{34},-\frac{41}{34},0)$ auch $(1,-2,-1)$ eine spezielle Lösung des Systems ist, wie man durch Setzen von $\lambda=-1$ sieht. Offenbar ändert sich die Lösungsmenge auch nicht, wenn man den Basisvektor v_3 mit einem beliebigen skalaren Vielfachen multipliziert. In diesem Fall haben wir durch Multiplikation mit 34 die Bruchzahlen in v_3 beseitigt.

Wir beschäftigen uns nun noch mit der Frage, wie man die Invertierbarkeit von Matrizen nachweist, und wie gegebenenfalls die inverse Matrix berechnet werden kann.

(7.13) Satz Lässt sich eine Matrix $A \in \mathscr{M}_{n,K}$ durch endliche viele elementare Zeilenumformungen in eine Matrix A' in normierter ZSF mit Zeilenrang $r = n$ umwandeln, so ist A invertierbar.

Beweis: Bereits oben haben wir bemerkt, dass eine Matrix A' in normierter ZSF mit Zeilenrang $r = n$ zwangsläufig mit der Einheitsmatrix $E^{(n)}$ übereinstimmt. Weil A durch elementare Zeilenumformungen in $A' = E^{(n)}$ überführt werden kann, gibt es eine Matrix $T \in \mathscr{E}_n(K) \subseteq \mathrm{GL}_n(K)$ mit $TA = E^{(n)}$. Es folgt $A = E^{(n)}A = (T^{-1}T)A = T^{-1}(TA) = T^{-1}E^{(n)} = T^{-1}$. Damit ist die Invertierbarkeit von A bewiesen. □

Die Beweisidee in Satz (7.13) kann genutzt werden, um die zu A inverse Matrix auszurechnen. Wendet man die Zeilenumformungen im Beweis statt auf A auf die Blockmatrix $(A \;\; E^{(n)})$ an, so erhält man die Matrix

$$T(A \;\; E^{(n)}) \qu= \quad (TA \;\; TE^{(n)}) \quad = \quad (E^{(n)} \;\; T).$$

Aus der rechten Hälfte der umgeformten Matrix kann die Inverse von A abgelesen werden, denn es gilt die Äquivalenz $A = T^{-1} \Leftrightarrow A^{-1} = T$. Wir demonstrieren dieses Berechnungsverfahren, indem wir A^{-1} für die Matrix

$$A \quad = \quad \begin{pmatrix} 3 & 0 & 2 \\ -1 & 1 & -1 \\ 7 & 0 & 5 \end{pmatrix}$$

bestimmen. Dazu schreiben wir die Einheitsmatrix $E^{(3)}$ neben unsere Matrix A und formen auf normierte ZSF um.

$$\left(\begin{array}{ccc|ccc} 3 & 0 & 2 & 1 & 0 & 0 \\ -1 & 1 & -1 & 0 & 1 & 0 \\ 7 & 0 & 5 & 0 & 0 & 1 \end{array}\right) \;\mapsto\; \left(\begin{array}{ccc|ccc} -1 & 1 & -1 & 0 & 1 & 0 \\ 3 & 0 & 2 & 1 & 0 & 0 \\ 7 & 0 & 5 & 0 & 0 & 1 \end{array}\right) \;\mapsto$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 1 & 0 & -1 & 0 \\ 3 & 0 & 2 & 1 & 0 & 0 \\ 7 & 0 & 5 & 0 & 0 & 1 \end{array}\right) \;\mapsto\; \left(\begin{array}{ccc|ccc} 1 & -1 & 1 & 0 & -1 & 0 \\ 0 & 3 & -1 & 1 & 3 & 0 \\ 0 & 7 & -2 & 0 & 7 & 1 \end{array}\right) \;\mapsto$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 1 & 0 & -1 & 0 \\ 0 & 1 & -\frac{1}{3} & \frac{1}{3} & 1 & 0 \\ 0 & 7 & -2 & 0 & 7 & 1 \end{array}\right) \;\mapsto\; \left(\begin{array}{ccc|ccc} 1 & -1 & 1 & 0 & -1 & 0 \\ 0 & 1 & -\frac{1}{3} & \frac{1}{3} & 1 & 0 \\ 0 & 0 & \frac{1}{3} & -\frac{7}{3} & 0 & 1 \end{array}\right) \;\mapsto$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 1 & 0 & -1 & 0 \\ 0 & 1 & -\frac{1}{3} & \frac{1}{3} & 1 & 0 \\ 0 & 0 & 1 & -7 & 0 & 3 \end{array}\right) \;\mapsto\; \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & 7 & -1 & -3 \\ 0 & 1 & 0 & -2 & 1 & 1 \\ 0 & 0 & 1 & -7 & 0 & 3 \end{array}\right) \;\mapsto\; \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 5 & 0 & -2 \\ 0 & 1 & 0 & -2 & 1 & 1 \\ 0 & 0 & 1 & -7 & 0 & 3 \end{array}\right)$$

Als Ergebnis erhalten wir also

$$A^{-1} \quad = \quad \begin{pmatrix} 3 & 0 & 2 \\ -1 & 1 & -1 \\ 7 & 0 & 5 \end{pmatrix}^{-1} \quad = \quad \begin{pmatrix} 5 & 0 & -2 \\ -2 & 1 & 1 \\ -7 & 0 & 3 \end{pmatrix}.$$

Offen bleibt hierbei die Frage, wie es zu interpretieren ist, wenn die Matrix A zwar auf normierte ZSF, aber mit Zeilenrang $r < n$, gebracht werden kann. Dafür ist es notwendig, dass wir uns neben den Zeilen- auch mit ***Spaltenumformungen*** einer Matrix befassen. Unter einer ***elementaren*** Spaltenumformungen verstehen wir, dass die zu den Zeilenumformungen analogen Operationen auf die Spalten einer Matrix $A \in \mathscr{M}_{m\times n,K}$ angewendet werden, also im einzelnen

(i) die Multiplikation der k-ten Spalten einer Matrix mit einem Wert λ, wobei $\lambda \in K^\times$ und $k \in \{1,...,n\}$ ist
(ii) die Addition des λ-fachen der k-ten Spalte zur ℓ-ten, mit $\lambda \in K$ und $k, \ell \in \{1,...,n\}$, $k \neq \ell$.

(7.14) Lemma Die Multiplikationen einer Matrix $A \in \mathscr{M}_{m\times n,K}$ mit den Transponierten von Elementarmatrizen von rechts bewirken elementare Spaltenumformungen. Genauer gilt:

(i) Die Matrix $A\,{}^{\mathrm{t}}\mathrm{M}_{k,\lambda}$ entsteht aus der Matrix A durch Multiplikation der k-ten Spalte mit λ.

(ii) Die Matrix $A\,{}^{\mathrm{t}}\mathrm{A}_{k,\ell,\lambda}$ entsteht aus der Matrix A durch Addition des λ-fachen der k-ten Spalte zur ℓ-ten Spalte.

Beweis: Wir beschränken uns auf den Beweis der Aussage (i). Nach der Rechenregel (iv) in Proposition (5.15) gilt $A\,{}^{\mathrm{t}}\mathrm{M}_{k,\lambda} = {}^{\mathrm{t}}({}^{\mathrm{t}}A)\,{}^{\mathrm{t}}\mathrm{M}_{k,\lambda} = {}^{\mathrm{t}}(\mathrm{M}_{k,\lambda}\,{}^{\mathrm{t}}A)$. Der Übergang ${}^{\mathrm{t}}A \mapsto \mathrm{M}_{k,\lambda}\,{}^{\mathrm{t}}A$ bewirkt nach Proposition (7.10) die Multiplikation der k-ten Zeile von ${}^{\mathrm{t}}A$ mit dem Wert λ. Für jedes ℓ ist die ℓ-te Spalte von A gleich der ℓ-ten Zeile von ${}^{\mathrm{t}}A$, und entsprechend ist die ℓ-te Spalte von $A\,{}^{\mathrm{t}}\mathrm{M}_{k,\lambda} = {}^{\mathrm{t}}(\mathrm{M}_{k,\lambda}\,{}^{\mathrm{t}}A)$ gleich der ℓ-ten Zeile von $\mathrm{M}_{k,\lambda}\,{}^{\mathrm{t}}A$. Also stimmt die ℓ-te Spalte von A mit der ℓ-ten Spalte von $A\,{}^{\mathrm{t}}\mathrm{M}_{k,\lambda}$ für $\ell \neq k$ überein. Für $\ell = k$ unterscheiden sie sich um den Faktor λ. □

Wir bemerken noch, dass mit jeder Matrix $A \in \mathrm{GL}_n(K)$ auch die Transponierte ${}^{\mathrm{t}}A$ invertierbar ist, mit $({}^{\mathrm{t}}A)^{-1} = {}^{\mathrm{t}}(A^{-1})$. Dies folgt direkt aus der Rechnung

$$ {}^{\mathrm{t}}A\,{}^{\mathrm{t}}(A^{-1}) \quad = \quad {}^{\mathrm{t}}(A^{-1}A) \quad = \quad {}^{\mathrm{t}}E^{(n)} \quad = \quad E^{(n)} $$

und einer analogen Rechnung, die ${}^{\mathrm{t}}(A^{-1})\,{}^{\mathrm{t}}A = E^{(n)}$ liefert.

(7.15) Satz Für jede Matrix $A \in \mathscr{M}_{m\times n,K}$ gibt es invertierbare Matrizen $T \in \mathrm{GL}_m(K)$ und $U \in \mathrm{GL}_n(K)$ und ein $r \in \{1,...,n\}$, so dass die Matrix TAU die Blockgestalt

$$ \begin{pmatrix} E^{(r)} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \qquad \text{besitzt.} $$

Beweis: Wir wissen bereits, dass eine Matrix $T \in \mathrm{GL}_m(K)$ existiert, so dass $B = TA$ in normierter ZSF vorliegt, mit gewissen Kennzahlen $r, j_1, ..., j_r$. Nach Lemma (7.14) genügt es nun zu zeigen, dass B durch elementare Spaltenumformungen auf die angegebene Blockgestalt gebracht werden kann. Nach Definition der normierten ZSF befindet sich für $1 \leq k \leq r$ in der j_k-ten Spalten von B jeweils der k-te Einheitsvektor $e_k \in K^m$. Nun führt man nacheinander für $1 \leq k \leq r$ die folgende Operation aus:

$$ \text{Addition des } (-a_{k\ell})\text{-fachen der } j_k\text{-ten Spalte zur } \ell\text{-ten, für } j_k < \ell \leq n $$

Durch diese Operation werden die Einträge rechts von der Position (k, j_k) zu Null, während alle übrigen Einträge der Matrix unverändert bleiben.

Nach Durchführung dieser Schritte enthält die modifizierte Matrix B' in den Spalten $j_1, ..., j_r$ die Einheitsvektoren $e_1, ..., e_r$, alle übrigen Spalten sind Null. Nun vertauscht man die Spalten noch so, dass sich die Einheitsvektoren in den ersten r Spalten befinden. Dann hat die Matrix die gewünschte Form. □

Auch hier lassen sich die Matrizen T und U, die die angegebene Blockgestalt erzeugen, explizit berechnen. Zunächst wendet man die erforderlichen Zeilenumformungen statt auf A auf die Blockmatrix $(A \;\; E^{(m)})$ an und erhält so eine Matrix der Form $(B \;\; T)$ mit $T \in \mathrm{GL}_m(K)$, wobei $B = TA$ sich in normierter ZSF befindet. Anschließend wendet man auf die linke Teilmatrix von $(B \;\; E^{(n)})$ Spaltenumformungen an, die B auf die Blockgestalt bringen, und ***dieselben*** Spaltenumformungen auch auf die rechte Teilmatrix. Man erhält damit eine Matrix der Form $(C \;\; U)$ mit $U \in \mathrm{GL}_m(K)$, wobei $C = BU$ die angegebene Blockgestalt hat. Die Matrizen T und U haben die gewünschte Umformungeigenschaft.

Durch dieses Rechenverfahren haben wir nun auch ein negatives Kriterium für Invertierbarkeit.

(7.16) Satz Sei $A \in \mathscr{M}_{n,K}$ eine Matrix, die durch elementare Zeilenumformungen auf normierte ZSF mit Zeilenrang $r < n$ gebracht werden kann. Dann ist A *nicht* invertierbar.

Beweis: Nehmen wir an, dass die Voraussetzung erfüllt ist, die Matrix A aber dennoch in $\mathrm{GL}_n(K)$ liegt. Nach Satz (7.15) gibt es Matrizen $T, U \in \mathrm{GL}_n(K)$ mit

$$TAU \quad = \quad \begin{pmatrix} E^{(r)} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

Mit A wäre dann auch TAU invertierbar. Aber eine Matrix mit Nullzeilen kann nicht invertierbar sein, denn für beliebiges $B \in \mathscr{M}_{r\times n,K}$ und $V \in \mathrm{GL}_n(K)$ gilt

$$\begin{pmatrix} B \\ \mathbf{0} \end{pmatrix} V \quad = \quad \begin{pmatrix} BV \\ \mathbf{0V} \end{pmatrix} \quad = \quad \begin{pmatrix} BV \\ \mathbf{0} \end{pmatrix} \quad ,$$

wobei die letzte Matrix offensichtlich *nicht* mit der Einheitsmatrix übereinstimmt. Der Widerspruch zeigt, dass die Annahme falsch war. □

Unser Rechenverfahren zur Bestimmung der Inversen einer Matrix A liefert also zugleich ein Entscheidungskriterium für die Invertierbarkeit: Kommt bei der Rechnung eine normierte ZSF mit Zeilenrang $r < n$ heraus, dann existiert die Inverse von A nicht.

§ 8. *Linearkombinationen und lineare Unabhängigkeit*

Inhaltsübersicht

Sei K ein Körper und V ein K-Vektorraum. Ist (v, w) ein Paar bestehend aus Vektoren $v, w \in V$, dann wird jeder Vektor der Form $\lambda v + \mu w$ mit $\lambda, \mu \in K$ eine *Linearkombination* von v und w genannt. Folgt für alle $\lambda, \mu \in K$ aus $\lambda v + \mu w = 0_V$ jeweils $\lambda = \mu = 0_K$, dann bezeichnet man das Paar (v, w) als *linear unabhängig*. Beide Begriffe lassen sich auf beliebig lange Tupel von Vektoren aus V verallgemeinern.
Sei nun $S \subseteq V$ eine beliebige, möglicherweise auch unendlich große, Teilmenge von V. Dann bilden die Linearkombinationen, die mit Vektoren aus der Menge S gebildet werden können, ihrerseits einen Untervektorraum von V, den wir mit $\langle V \rangle_K$ bezeichnen und den *von S erzeugten* Untervektorraum nennen. Es handelt sich um den kleinsten Untervektorraum U von V, der S als Teilmenge enthält. Man bezeichnet die Menge S als *linear unabhängig*, wenn jede Linearkombination eines Tupels von lauter verschiedenen Vektoren aus S linear unabhängig ist. Beide Begriffe werden im folgenden Kapitel bei der Definition des Dimenionsbegriffs eine wichtige Rolle spielen.

Wichtige Begriffe und Sätze

- Linearkombination eines Tupels von Vektoren
- von einer Menge S erzeugter Untervektorraum $\langle S \rangle_K$, Erzeugendensystem eines Untervektorraums
- lineare Unabhängigkeit eines Tupels von Vektoren
- lineare Unabhängigkeit einer Teilmenge S
- Polynomring $R[x]$ über einem Ring R

Im Verlauf dieses Kapitels werden wir es häufig mit Tupeln $(v_1, ..., v_r)$ bestehend Vektoren, also Elementen eines K-Vektorraus, zu tun haben. Dabei ist es praktisch, auch den Fall $r = 0$ zuzulassen. Das leere Tupel bestehend aus null Vektoren bezeichnen wir mit ().

(8.1) Definition Sei V ein K-Vektorraum, $r \in \mathbb{N}_0$ und $(v_1, ..., v_r)$ ein Tupel von Elementen aus V. Wir bezeichnen einen Vektor $w \in V$ als ***Linearkombination*** des Tupels, wenn ein Tupel $(\lambda_1, ..., \lambda_r) \in K^r$ existiert, so dass

$$w = \sum_{i=1}^{r} \lambda_i v_i \qquad \text{erfüllt ist.}$$

Ist (v,w) ein Paar von Vektoren, dann sind die Linearkombinationen von (v,w) genau die Vektoren der Form $\lambda v+\mu w$ mit $\lambda,\mu\in K$. Beispielsweise kann jeder Vektor $v=(a,b)\in\mathbb{R}^2$ als Linearkombination der Einheitsvektoren $e_1=(1,0)$ und $e_2=(0,1)$ dargestellt werden, denn es ist

$$v \quad = \quad \begin{pmatrix} a \\ b \end{pmatrix} \quad = \quad a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad = \quad ae_1 + be_2.$$

Besteht unser Tupel (v) nur aus einem einzigen Vektor, dann sind die Linearkombinationen dieses Tupels genau die Vektoren der Form λv mit $\lambda\in K$, also genau die skalaren Vielfachen von v. Die einzige Linearkombination des leeren Tupels $()$ ist der Nullvektor 0_V, denn jede Summe bestehend aus null Summanden ist definitionsgemäß gleich null.

(8.2) Definition Sei V ein K-Vektorraum und $S\subseteq V$ eine beliebige Teilmenge. Dann bezeichnen wir mit

$$\langle S\rangle_K \quad = \quad \left\{ \sum_{k=1}^{r} \lambda_k v_k \;\middle|\; r\in\mathbb{N}_0, \lambda_1,\ldots,\lambda_r\in K, v_1,\ldots,v_r\in S \right\}$$

die Menge aller Linearkombinationen von Tupeln bestehend aus Vektoren der Menge S. Man nennt $\langle S\rangle_K$ den von S ***erzeugten*** oder ***aufgespannten*** Untervektorraum.

Die Rechtfertigung für diese Bezeichnung wird durch folgenden Satz geliefert.

(8.3) Satz Sei V ein K-Vektorraum und $S\subseteq V$ eine Teilmenge. Dann gilt

(i) Die Menge $\langle S\rangle_K$ bildet einen Untervektorraum von V mit $\langle S\rangle_K\supseteq S$.

(ii) Ist U ein weiterer Untervektorraum von V mit $U\supseteq S$, dann gilt $U\supseteq\langle S\rangle_K$.

Es handelt sich also bei $\langle S\rangle_K$ um den *kleinsten* Untervektorraum von V, der S als Teilmenge enthält.

Beweis: zu (i) Zunächst beweisen wir, dass $\langle S\rangle_K$ ein Untervektorraum von V ist. Der Nullvektor 0_V ist eine Linearkombination des leeren Tupels $()$ und somit in $\langle S\rangle_K$ enthalten. Seien nun $v,w\in\langle S\rangle_K$ und $\lambda\in K$ vorgegeben. Zu zeigen ist $v+w\in\langle S\rangle_K$ und $\lambda v\in\langle S\rangle_K$. Wegen $v\in\langle S\rangle_K$ gibt es ein $r\in\mathbb{N}_0$ und ein Tupel $(v_1,\ldots,v_r)$, so dass v Linearkombination dieses Tupels ist. Es existiert also ein Tupel $(\lambda_1,\ldots,\lambda_r)\in K^r$ mit $v=\sum_{i=1}^r\lambda_i v_i$. Genauso folgt aus $w\in\langle S\rangle_K$ die Existenz eines $s\in\mathbb{N}_0$ und von $w_1,\ldots,w_s\in S$ und $\mu_1,\ldots,\mu_s\in K$ mit $w=\sum_{j=1}^s\mu_j w_j$. Die Gleichung

$$v+w \quad = \quad \sum_{i=1}^{r}\lambda_i v_i + \sum_{j=1}^{s}\mu_j w_j$$

zeigt, dass $v+w$ eine Linearkombination des Tupels $(v_1,\ldots,v_r,w_1,\ldots,w_s)$ ist und somit in $\langle S\rangle_K$ liegt. Ebenso folgt aus $\lambda v=\sum_{i=1}^r(\lambda\lambda_i)v_i$, dass λv eine Linearkombination von $(v_1,\ldots,v_r)$ ist und λv somit ebenfalls in $\langle S\rangle_K$ enthalten ist.

Der Nachweis der Untervektorraum-Eigenschaft von $\langle S\rangle_K$ ist damit abgeschlossen. Es gilt $S \subseteq \langle S\rangle_K$, denn jedes $v \in S$ ist wegen $v = 1_K \cdot v$ jeweils Linearkombination des einelementigen Tupels (v) und somit nach Definition in $\langle S\rangle_K$ enthalten.

zu (ii) Sei U ein beliebiger Untervektorraum von V mit $U \supseteq S$. Wir zeigen durch vollständige Induktion über $r \in \mathbb{N}_0$, dass jede Linearkombination jedes r-elementigen Tupels $(v_1, ..., v_r)$ mit $v_k \in S$ für $1 \leq k \leq r$ in U enthalten ist. Daraus folgt dann unmittelbar $\langle S\rangle_K \subseteq U$. Für $r = 0$ ist die Aussage klar, denn die einzige Linearkombination des leeren Tupels $()$ ist der Nullvektor 0_V, und es gilt $0_V \in U$, weil U ein Untervektorraum von V ist.

Sei nun $r \in \mathbb{N}_0$, und setzen wir die Aussage für dieses r voraus. Sei $(v_1, ..., v_{r+1})$ ein Tupel mit $v_k \in S$ für $1 \leq k \leq r+1$, und sei w eine Linearkombination dieses Tupels. Es gibt dann also $\lambda_1, ..., \lambda_{r+1} \in K$ mit $w = \sum_{k=1}^{r+1} \lambda_k v_k$. Der Vektor $w' = \sum_{k=1}^{n} \lambda_k v_k$ ist eine Linearkombination des r-elementigen Tupels $(v_1, ..., v_r)$ und somit nach Induktionsvoraussetzung in U enthalten. Weiter gilt $v_{r+1} \in U$ wegen $S \subseteq U$ und weiter $\lambda_{r+1} v_{r+1} \in U$ und $w = w' + \lambda_{r+1} v_{r+1} \in U$, da U ein Untervektorraum von V ist. Damit ist der Induktionsbeweis abgeschlossen. □

Ist umgekehrt ein Untervektorraum U eines K-Vektorraums V vorgegeben, dann kann man danach fragen, für welche Teilmengen $S \subseteq V$ jeweils $U = \langle S\rangle_K$ erfüllt ist.

(8.4) Definition Ist V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum, dann wird jede Teilmenge $S \subseteq V$ mit der Eigenschaft $U = \langle S\rangle_K$ ein ***Erzeugendensystem*** von U genannt.

Wegen Satz (8.3) erfüllt jedes Erzeugendensystem S von U notwendigerweise die Bedingung $S \subseteq U$, und insbesondere gilt $\langle U\rangle_K = U$. In der Regel ist die Teilmenge S im Vergleich zu U eine sehr kleine Menge und besteht häufig nur aus endlich vielen Elementen.

Im nächsten Kapitel werden wir uns oft auch für Erzeugendensysteme des gesamten Vektorraums V, also Teilmengen $S \subseteq V$ mit $\langle S\rangle_K = V$, interessieren. Für die Vektorräume K^n und $\mathscr{M}_{m\times n,K}$ existieren endliche Erzeugendensysteme, nämlich im ersten Fall die Menge $\{e_1, ..., e_n\}$ der Einheitsvektoren und im zweiten die Menge $\{B_{k\ell} \mid 1 \leq k \leq m, 1 \leq \ell \leq n\}$ der Basismatrizen. Es gibt aber auch Vektorräume, die durch keine endliche Teilmenge ihrer Vektoren aufgespannt werden können. Um zumindest ein konkretes Beispiel für eine solche Situation vor Augen zu haben, und weil wir ihn auch in den späteren Kapiteln noch brauchen werden, führen wir den Polynomring über einem Ring R ein.

(8.5) Satz *(ohne Beweis)*

Für jeden Ring R gibt es einen Erweiterungsring $R[x] \supseteq R$ mit einem ausgezeichneten Element $x \notin R$, so dass für jedes $f \in R[x]$ folgende Bedingung erfüllt ist. *Entweder* ist $f = 0_R$, *oder* es gibt ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte Elemente $a_0, ..., a_n \in R$ mit

$$f \quad = \quad \sum_{k=0}^{n} a_k x^k \quad \text{und} \quad a_n \neq 0_R.$$

Man nennt $R[x]$ den ***Polynomring*** über dem Körper R, seine Elemente bezeichnet man als *Polynome*. Im Fall $f \neq 0_R$ bezeichnet man n als den ***Grad*** des Polynoms.

Jedem Element $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ kann eine Abbildung $R \to R$ zugeordnet werden, die ein Element $c \in R$ jeweils auf

$$f(c) \quad = \quad \sum_{k=0}^{n} a_k c^k$$

abbildet. Man nennt diese Abbildung die dem Polynom f zugeordnete ***Polynomfunktion***. Ein häufiger Fehler besteht darin, ein Polynom f mit seiner Polynomfunktion gleichzusetzen. Diese Gleichsetzung ist aber unzulässig und kann zu Widersprüchen führen. Der Grund dafür ist, dass bei einem endlichen Ring R verschiedene Polynome dieselbe Polynomfunktion liefern können. Ist beispielsweise $R = \mathbb{F}_2 = \{\bar{0}, \bar{1}\}$, der Körper mit zwei Elementen, dann haben die Polynome $x \in \mathbb{F}_2[x]$ und $x^2 \in \mathbb{F}_2[x]$ dieselbe zugeordnete Polynomfunktion, gegeben durch $\bar{0} \mapsto \bar{0}$ und $\bar{1} \mapsto \bar{1}$.

In diesem Zusammenhang sei auch darauf hingewiesen, dass das Element x des Polynomrings $R[x]$ kein Element des Rings R ist! Statt einer Funktion $R \to R$ sollte man sich unter einem Polynom in $R[x]$ deshalb eher einen rein „formalen Ausdruck“, gebildet mit Elementen des Rings R und der Variablen x des Polynomrings, vorstellen.

Nach diesem kurzen Exkurs kehren wir nun zur Linearen Algebra zurück. Ist K ein Körper, dann kann man $K[x]$ als K-Vektorraum betrachten, in dem man die Vektoraddition mit der gewöhnlichen Addition im Ring $K[x]$ gleichsetzt und die skalare Multiplikation $K \times K[x] \to K[x]$ durch Einschränkung der Multiplikationsabbildung

$$K[x] \times K[x] \longrightarrow K[x] \quad , \quad (f, g) \mapsto f\,g$$

definiert. In diesem Fall ist dann $S = \{x^n \mid n \in \mathbb{N}_0\}$ ein (unendliches) Erzeugendensystem von $K[x]$ als K-Vektorraum, wobei $x^0 = 1_K$ gesetzt wird. Jedes Polynom ist Linearkombination von S. Beispielsweise ist das Polynom $f = x^7 - 4x^3 + 5$ eine Linearkombination des Tupels $(1, x^3, x^7)$, und ebenso eine Linearkombination von $(1, x, x^2, ..., x^7)$.

Man kann sich aber leicht überzeugen, dass keine *endliche* Teilmenge $T \subseteq K[x]$ mit der Eigenschaft $\langle T \rangle_K = K[x]$ existiert. Denn in T gibt es ein Polynom mit maximalem Grad n, und folglich kann keine Linearkombination von T einen Grad größer als n haben. Dies bedeutet, dass zum Beispiel x^{n+1} nicht in $\langle T \rangle_K$ enthalten ist.

Kommen wir nun zur zweiten wichtigen Definition dieses Kapitels.

(8.6) Definition Sei V ein K-Vektorraum. Wir bezeichnen ein Tupel $(v_1, ..., v_r)$ mit $r \in \mathbb{N}_0$, bestehend aus Vektoren $v_k \in V$, als ***linear unabhängig***, wenn für jedes Tupel $(\lambda_1, ..., \lambda_r) \in K^r$ die Implikation

$$\sum_{k=1}^{r} \lambda_k v_k = 0_V \quad \Rightarrow \quad \lambda_1 = ... = \lambda_r = 0_K \qquad \text{erfüllt ist.}$$

erfüllt ist. Ein Tupel, das nicht linear unabhängig ist, wird ***linear abhängig*** genannt.

Das leere Tupel () ist nach Definition linear unabhängig. Ein Tupel (v) bestehend aus einem einzelnen Vektor v ist genau dann linear unabhängig, wenn $v \neq 0_V$ ist. Ein Paar (v, w) bestehend aus zwei Vektoren ist genau dann linear unabhängig, wenn $v \neq 0_V$ und w kein skalares Vielfaches von v ist, also $w \neq \lambda v$ für alle $\lambda \in K$ gilt.

Für jedes $n \in \mathbb{N}$ ist im K-Vektorraum K^n das Tupel $(e_1, ..., e_n)$ bestehend aus den Einheitsvektoren linear unabhängig. Sei nämlich $(\lambda_1, ..., \lambda_n) \in K^n$ ein Tupel mit $\sum_{k=1}^{n} \lambda_k v_k = 0_{K^n}$. Für $1 \leq i \leq n$ ist die i-te Komponente von $\sum_{k=1}^{n} \lambda_k e_k$ jeweils gleich $\sum_{k=1}^{n} \lambda_k \delta_{ki} = \lambda_i$. Aus $\sum_{k=1}^{n} \lambda_k v_k = 0_{K^n}$ folgt also $\lambda_i = 0_K$ für $1 \leq u \leq n$. Also ist $(e_1, ..., e_n)$ linear unabhängig.

Auch für den Begriff der linearen Unabhängigkeit gibt es eine Variante, die sich auf Mengen bezieht.

(8.7) Definition Sei V ein K-Vektorraum. Eine Teilmenge $S \subseteq V$ bezeichnen wir als ***linear unabhängig***, wenn jedes Tupel $(v_1, ..., v_r)$ bestehend aus lauter verschiedenen Elementen v_k der Menge S linear unabhängig ist.

Die Einschränkung in der Definition ist sinnvoll, denn ein Tupel, indem derselbe Vektor mehrfach vorkommt, ist automatisch linear abhängig. Sei nämlich $r \in \mathbb{N}$, $r \geq 2$ und $(v_1, ..., v_r)$ ein Tupel bestehend aus Elementen von V. Nehmen wir weiter an, dass es natürliche Zahlen i, j mit $1 \leq i < j \leq r$ und $v_i = v_j$ gibt. Definieren wir dann $\lambda_i = 1_K$, $\lambda_j = -1_K$ und $\lambda_k = 0_K$ für alle $k \in \{1, ..., r\} \setminus \{i, j\}$, dann gilt $\sum_{k=1}^{r} \lambda_k v_k = 0_V$, ohne dann die Koeffizienten $\lambda_1, ..., \lambda_r$ alle gleich null sind.

Wir notieren einige elementare Beobachtungen, die sich direkt aus der Definition ergeben.

(8.8) Lemma Sei V ein K-Vektorraum.

(i) Ist $S \subseteq V$ linear unabhängig, dann gibt dasselbe für jede Teilmenge $T \subseteq S$. Insbesondere ist die leere Menge $\emptyset$ stets linear unabhängig.

(ii) Jede Teilmenge $S \subseteq V$ mit $0_V \in S$ ist linear abhängig.

(iii) Ist $r \in \mathbb{N}_0$ und sind $v_1, ..., v_r \in V$ mit $v_i \neq v_j$ für $i \neq j$, so ist r-elementige Menge $\{v_1, ..., v_r\}$ genau dann linear unabhängig, wenn das Tupel $(v_1, ..., v_r)$ linear unabhängig ist.

Betrachten wir noch einige konkrete Beispiele.

(i) Die Menge $\{e_1, ..., e_n\}$ der Einheitsvektoren ist eine n-elementige linear unabhängige Teilmenge des K-Vektorraums K^n. Dies ergibt sich aus Teil (iii) des soeben formulierten Lemmas in Verbindung mit der Feststellung von oben, dass das n-Tupel $(e_1, ..., e_n)$ linear unabhängig ist.

(ii) Auf ähnliche Weise kann man zeigen, dass die Menge $\{ B_{k\ell}^{(m\times n)} \mid 1 \leq k \leq m, 1 \leq \ell \leq n \}$ der Basismatrizen im K-Vektorraum $\mathcal{M}_{m\times n,K}$ der $m \times n$-Matrizen linear unabhängig ist.

(iii) In einigen Vektorräumen existieren auch unendliche linear unabhängige Mengen. Beispielsweise ist im Polynomring $K[x]$, aufgefasst als K-Vektorraum, die Teilmenge $\{x^n \mid n \in \mathbb{N}_0\}$ bestehend aus den sog. *Monomen*, linear unabhängig.

(8.9) Proposition Sei V ein K-Vektorraum und $S \subseteq V$ eine beliebige Teilmenge.

(i) Genau dann ist S linear abhängig, wenn ein $v \in S$ mit $v \in \langle S \setminus \{v\}\rangle_K$ existiert.

(ii) Sie ist genau dann linear unabhängig, wenn $v \notin \langle S \setminus \{v\}\rangle_K$ für alle $v \in S$ erfüllt ist.

(iii) Ist S linear unabhängig und $v \in V \setminus \langle S\rangle_K$, dann ist auch $S \cup \{v\}$ linear unabhängig.

Beweis: zu (i) „⇐“ Angenommen, es gibt ein $v \in S$ mit $v \in \langle S \setminus \{v\}\rangle_K$. Dann gibt es ein $r \in \mathbb{N}_0$ und ein Tupel $(v_1, ..., v_r)$ von Vektoren aus $S \setminus \{v\}$ mit der Eigenschaft, dass v eine Linearkombination dieses Tupels ist. Es gibt also ein Tupel $(\lambda_1, ..., \lambda_r) \in K^r$ mit $v = \sum_{k=1}^{r} \lambda_k v_k$. Dabei dürfen wir davon ausgehen, dass die Vektoren $v_1, ..., v_r$ alle verschieden sind. Kommt nämlich einer der Vektoren v_i mehrfach im Tupel vor, gilt also $v_j = v_i$ für ein $j \neq i$, dann können wir die Summe $\lambda_i v_i + \lambda_j v_j$ durch $(\lambda_i + \lambda_j)v_i$ ersetzen. Dies zeigt, dass wir v_j aus dem Tupel streichen können, ohne dass die Eigenschaft von v, eine Linearkombination des Tupels zu sein, verloren geht. Die Gleichung

$$v = \sum_{k=1}^{r} \lambda_k v_k \quad \Leftrightarrow \quad (-1_K)v + \sum_{i=1}^{r} \lambda_i v_i = 0_V$$

zeigt nun, dass das Tupel $(v, v_1, ..., v_r)$ linear abhängig ist. Weil das Tupel aus lauter verschiedenen Elementen der Menge S besteht, folgt daraus, dass S linear abhängig ist.

„⇒“ Ist S linear abhängig, dann gibt es ein $r \in \mathbb{N}$ und ein linear abhängiges Tupel $(v_1, ..., v_r)$ bestehend aus lauter verschiedenen Vektoren der Menge S. Die lineare Abhängigkeit bedeutet, dass $\lambda_1, ..., \lambda_r \in K$ existieren, nicht alle gleich Null, mit $\sum_{k=1}^{r} \lambda_k v_k = 0_V$. Nehmen wir an, dass $i \in \{1, ..., r\}$ ein Index mit $\lambda_i \neq 0$ ist. Dann kann die Gleichung umgestellt werden zu

$$v_i \quad = \quad \sum_{j \neq i} \left(-\frac{\lambda_j}{\lambda_i}\right) v_j.$$

Dies zeigt, dass v_i in $\langle S \setminus \{v_i\}\rangle_K$ enthalten ist.

Die Aussage (ii) folgt rein logisch aus Teil (i) durch Negation auf beiden Seiten der Äquivalenz.

zu (iii) Nehmen wir an, dass S linear unabhängig ist, dass $v \notin \langle S\rangle_K$ gilt, und dass $S \cup \{v\}$ dennoch linear abhängig ist. Dann gibt es ein $r \in \mathbb{N}$ und ein linear abhängiges Tupel $(v_1, ..., v_r)$ bestehend aus lauter verschiedenen Elementen der Menge $S \cup \{v\}$. Einer dieser Vektoren v_i muss mit v übereinstimmen, denn ansonsten wäre $(v_1, ..., v_r)$ ein linear abhängiges Tupel bestehend aus Elementen der Menge S, und S somit linear abhängig, im Widerspruch zur Voraussetzung.

Sei $i \in \{1, ..., r\}$ der Index mit $v_i = v$. Auf Grund der linearen Abhängigkeit gibt es Koeffizienten $\lambda_1, ..., \lambda_r \in K$, nicht alle gleich Null, mit $\sum_{k=1}^{r} \lambda_k v_k = 0_V$. Dabei muss $\lambda_i \neq 0_K$ gelten, denn andernfalls wäre das Tupel ohne den Vektor v_i ebenfalls linear abhängig, was erneut im Widerspruch zur linearen Unabhängigkeit von S stehen würde. So aber können wir die Gleichung wieder zu

$$v \quad = \quad v_i \quad = \quad \sum_{j \neq i} \left(-\frac{\lambda_j}{\lambda_i}\right) v_j$$

umstellen. Aber dies steht im Widerspruch zur Voraussetzung $v \notin \langle S\rangle_K$. □

Am Ende dieses Kapitels sehen wir uns an, wie sich lineare Unabhängigkeit und die Existenz von Linearkombinationen rechnerisch nachweisen lässt. Sei $V = \mathbb{R}^3$ und (v_1, v_2, v_3) das Tupel bestehend aus den drei Vektoren

$$v_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad , \quad v_2 = \begin{pmatrix} 2 \\ 6 \\ 7 \end{pmatrix} \quad , \quad v_3 = \begin{pmatrix} 0 \\ 8 \\ 7 \end{pmatrix}.$$

Sei außerdem $v = (1, 0, 1)$ und $w = (3, 5, 7)$. Unser Ziel ist es zu überprüfen, ob v bzw. w Linearkombinationen des Tupels (v_1, v_2, v_3) sind. Dass es sich bei v um eine Linearkombination des Tupels handelt, ist äquivalent zur Existenz von Koeffizienten $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ mit

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = v \quad \Leftrightarrow \quad \lambda_1 \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 6 \\ 7 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 \\ 8 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \Leftrightarrow$$

$$\begin{pmatrix} \lambda_1 + 2\lambda_2 \\ -\lambda_1 + 6\lambda_2 + 8\lambda_3 \\ 7\lambda_2 + 7\lambda_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$$\Leftrightarrow \quad (\lambda_1, \lambda_2, \lambda_3) \text{ ist Lösungsmenge des LGS } x_1 + 2x_2 = 1 \ , \ -x_1 + 6x_2 + 8x_3 = 0 \ , \ 7x_2 + 7x_3 = 1.$$

Um zu sehen, ob das LGS eine Lösung hat, stellen wir die erweiterte Koeffizientenmatrix auf und bringen sie auf normierte Zeilenstufenform.

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ -1 & 6 & 8 & 0 \\ 0 & 7 & 7 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 8 & 8 & 1 \\ 0 & 7 & 7 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 7 & 7 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & -2 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Die dritte Zeile in der letzten Matrix entspricht der Gleichung $0 = 1$. Das LGS ist also *unlösbar*. Auf Grund der oben formulierten Äquivalenz folgt daraus, dass v *keine* Linearkombination des Tupels (v_1, v_2, v_3) ist.

Betrachten wir nun an Stelle von v den Vektor w. Hier führt die Gleichung $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = w$ nach dem gleichen Schema auf das LGS

$$x_1 + 2x_2 = 3 \ , \ -x_1 + 6x_2 + 8x_3 = 5 \ , \ 7x_1 + 7_x 3 = 7.$$

Wieder stellen wir die erweiterte Koeffizientenmatrix auf und formen auf normierte ZSF um.

$$\begin{pmatrix} 1 & 2 & 0 & 3 \\ -1 & 6 & 8 & 5 \\ 0 & 7 & 7 & 7 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 8 & 8 & 8 \\ 0 & 7 & 7 & 7 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & -2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Die Gleichungen in der letzten Matrix lauten $x_1 - 2x_3 = 1$ und $x_2 + x_3 = 1$, was zu $x_1 = 1 + 2x_3$ und $x_2 = 1 - x_3$ umgeformt werden kann. Die Lösungsmenge $\mathscr{L}$ des ursprünglichen LGS ist also gegeben durch

$$\mathscr{L} \quad = \quad \left\{ \begin{pmatrix} 1 + 2x_3 \\ 1 - x_3 \\ x_3 \end{pmatrix} \;\middle|\; x_3 \in \mathbb{R} \right\} \quad = \quad \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}.$$

Jedes Element der Lösungsmenge liefert eine Darstellung von w als Linearkombination des Tupels (v_1, v_2, v_3). Setzt man $\lambda = 0$, so erhält man zum Beispiel das Element $(1,1,0) \in \mathscr{L}$, und $\lambda = 1$ entspricht $(3,0,1) \in \mathscr{L}$. Tatsächlich gilt sowohl

$$1 \cdot \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 2 \\ 6 \\ 7 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 8 \\ 7 \end{pmatrix} \quad = \quad \begin{pmatrix} 3 \\ 5 \\ 7 \end{pmatrix} \qquad \text{als auch} \qquad 3 \cdot \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 2 \\ 6 \\ 7 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 8 \\ 7 \end{pmatrix} \quad = \quad \begin{pmatrix} 3 \\ 5 \\ 7 \end{pmatrix}.$$

Nach einem ähnlichen Schema lässt sich auch die lineare Unabhängigkeit behandeln. Diesmal betrachten wir in $V = \mathbb{R}^3$ das Tupel (v_1, v_2, v_3) bestehend aus den Vektoren

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \quad , \quad v_2 = \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix} \quad , \quad v_3 = \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix}.$$

Diesmal besteht unser Ziel darin, die lineare Unabhängigkeit von (v_1, v_2, v_3) nachzuweisen. Für jedes Tripel $(\lambda_1, \lambda_2, \lambda_3)$ in $\mathbb{R}^3$ gilt die Äquivalenz

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0_{\mathbb{R}^3} \quad \Leftrightarrow \quad \lambda_1 \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix} + \lambda_3 \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad \begin{pmatrix} \lambda_1 + 3\lambda_3 \\ 2\lambda_1 + 2\lambda_2 + 3\lambda_3 \\ -\lambda_2 + 3\lambda_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Leftrightarrow \quad (\lambda_1, \lambda_2, \lambda_3) \text{ ist Lösung des LGS } x_1 + 3x_3 = 0 \ , \ 2x_1 + 2x_2 + 3x_3 = 0 \ , \ -x_2 + 3x_3 = 0.$$

Diesmal handelt es sich um ein *homogenes* LGS. Es genügt also, die nicht-erweiterte Koeffizientenmatrix aufzustellen und auf normierte ZSF zu bringen.

$$\begin{pmatrix} 1 & 0 & 3 \\ 2 & 2 & 3 \\ 0 & -1 & 3 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & -3 \\ 0 & 1 & -3 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -3 \\ 0 & 2 & -3 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\mapsto \quad \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Die letzte Matrix entspricht dem System $x_1 = 0 \ , \ x_2 = 0 \ , \ x_3 = 0$, die Lösungsmenge $\mathscr{L}$ des Systems ist also gleich $\{(0,0,0)\}$. Daraus ergibt sich insgesamt die Äquivalenz

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0_{\mathbb{R}^3} \quad \Leftrightarrow \quad (\lambda_1, \lambda_2, \lambda_3) = (0,0,0) \quad \Leftrightarrow \quad \lambda_1 = \lambda_2 = \lambda_3 = 0.$$

Dies zeigt, dass das Tupel (v_1, v_2, v_3) tatsächlich linear unabhängig ist; dafür ist bereits die Gültigkeit der Implikation „⇒“ hinreichend. Das Beispiel zeigt, auf welche Weise die lineare Unabhängigkeit eines Tupels von Vektoren im K^m allgemein überprüft werden kann.

(8.10) Proposition Seien $m, n \in \mathbb{N}$, und sei $(v_1, ..., v_n)$ ein Tupel bestehend aus Vektoren $v_k \in K^m$. Sei $A \in \mathscr{M}_{m\times n,K}$ die Matrix mit der Eigenschaft, dass v_k jeweils der k-te Spaltenvektor $a_{\bullet k}$ von A ist, für $1 \leq k \leq n$. Genau dann ist Tupel linear unabhängig, wenn die einzige Lösung des homogenen linearen Gleichungssystems $Ax = 0_{K^m}$ der Nullvektor 0_{K^n} ist.

Beweis: Für beliebige $\lambda_1, ..., \lambda_n \in K$ ist der Vektor $\sum_{k=1}^{n} \lambda_k v_k \in K^m$ gleich dem Matrix-Vektor-Produkt Aw, mit $w = (\lambda_1, ..., \lambda_n)$, denn für $1 \leq i \leq m$ ist der i-te Eintrag von Aw nach Definition des Matrix-Vektor-Produkts gleich $\sum_{k=1}^{n} a_{ik}\lambda_k$, und wegen $v_k = a_{\bullet k} = (a_{1k}, ..., a_{mk})$ für $1 \leq k \leq n$ ist dies zugleich der i-te Eintrag des Vektors $\sum_{k=1}^{n} \lambda_k v_k$.

Das Tupel $(v_1, ..., v_n)$ ist nach Definition genau dann linear unahängig, wenn das einzige Tupel $(\lambda_1, ..., \lambda_n)$ mit der Eigenschaft $\sum_{k=1}^{n} \lambda_k v_k = 0_{K^m}$ der Nullvektor 0_{K^n} ist. Dies wiederum ist auf Grund unserer Vorüberlegung genau dann der Fall, wenn die Gleichung $Aw = 0_{K^m}$ nur von $w = 0_{K^n}$ erfüllt ist, also genau dann, wenn 0_{K^n} die einzige Lösung des linearen Gleichungssystems $Ax = 0_{K^m}$ ist. □

§ 9. *Basen eines Vektorraums, Dimensionsbegriff*

Inhaltsübersicht

Eine Teilmenge eines K-Vektorraums V wird *Basis* genannt, wenn sie zugleich linear unabhängig und ein Erzeugendensystem von V ist. Das wichtigste Ergebnis dieses Abschnitts lautet, dass je zwei Basen eines endlich erzeugten K-Vektorraums dieselbe Elementezahl besitzen; diese wird dann die *Dimension* von V genannt.

Wir bestimmen Basen für eine Reihe konkreter K-Vektorräume (der K^n, Matrizen, Polynome). Außerdem leiten wir einige fundamentale Aussagen über K-Vektorräume her. Als wichtigste sind hier der *Basisauswahlsatz* und der *Basisergänzungssatz* zu nennen: Aus jedem Erzeugendensystem eines K-Vektorraums kann eine Basis ausgewählt werden, und jede linear unabhängige Teilmenge kann zu einer Basis ergänzt werden.

Wichtige Begriffe und Sätze

- Austauschsatz
- Je zwei Basen eines endlich erzeugten K-Vektorraums haben gleich viele Elemente.
- Basisauswahlsatz
- Basisergänzungssatz

(9.1) Definition Sei V ein K-Vektorraum. Eine Teilmenge $B \subseteq V$ heißt ***Basis*** von V, wenn sie linear unabhängig und ein Erzeugendensystem von V ist. Ein Tupel $(v_1, ..., v_n)$ mit $n \in \mathbb{N}_0$, bestehend aus Vektoren $v_i \in V$, wird ***geordnete Basis*** genannt, wenn $\{v_1, ..., v_n\}$ aus n verschiedenen Elementen besteht und eine Basis von V bildet.

Im letzten Kapitel haben wir mehrere Beispiele für Teilmengen eines Vektorraums V gesehen, die einerseits den Vektorraum V erzeugen und andererseits auch linear unabhängig sind. Beispielsweise ist durch die Menge $\{e_1, ..., e_n\}$ der Einheitsvektoren eine Basis des K^n gegeben. Die Menge $\{B_{k\ell}^{(m\times n)} \mid 1 \leq k \leq m, 1 \leq \ell \leq n\}$ der Basismatrizen bildet eine Basis des Vektorraums $\mathscr{M}_{m\times n,K}$ (daher der Name). Die Menge $\{x^n \mid n \in \mathbb{N}_0\}$ bildet eine (unendliche) Basis des K-Vektorraums $K[x]$.

(9.2) Satz Sei V ein K-Vektorraum. Für eine Teilmenge $B \subseteq V$ sind die folgenden Aussagen äquivalent.

(i) Sie ist eine Basis von V.
(ii) Sie ist ein minimales Erzeugendensystem von V.
(iii) Sie ist eine maximale linear unabhängige Teilmenge von V.

Beweis: „(i) ⇒ (ii)“ Nehmen wir an, dass B kein minimales Erzeugendensystem von V ist. Dann gibt es eine Teilmenge $S \subsetneq B$ mit $V = \langle S \rangle_K$. Wählen wir $v \in B \setminus S$ beliebig, dann gilt $v \in \langle S \rangle_K$. Nach Prop. (8.9) (i) ist $S \cup \{v\}$ also linear abhängig. Wegen $B \supseteq S \cup \{v\}$ ist dann auch B linear abhängig, im Widerspruch zur Voraussetzung.

„(ii) ⇒ (iii)“ Gehen wir zunächst davon aus, dass B linear abhängig ist. Dann gibt es nach Prop. (8.9) (i) ein $v \in B$ mit $v \in \langle B \setminus \{v\} \rangle_K$. Aus $B \setminus \{v\} \subseteq \langle B \setminus \{v\} \rangle_K$ und $v \in \langle B \setminus \{v\} \rangle_K$ folgt $B \subseteq \langle B \setminus \{v\} \rangle_K$. Mit Satz (8.3) folgt $V = \langle B \rangle_K \subseteq \langle B \setminus \{v\} \rangle_K$, weil $\langle B \setminus \{v\} \rangle_K$ ein Untervektorraum von V ist, und damit $V = \langle B \setminus \{v\} \rangle_K$ Aber dies steht im Widerspruch zu der Vorausetzung, dass B ein *minimales* Erzeugendensystem von V ist.

Nehmen wir nun an, B ist zwar linear unabhängig, aber als linear unabhängige Teilmenge nicht maximal. Dann gibt es eine linear unabhängige Teilmenge S von V mit $S \supsetneq B$. Sei nun v ein beliebiges Element in $S \setminus B$. Wegen $V = \langle B \rangle_K$ gilt $v \in \langle B \rangle_K$ und wegen $B \subseteq S \setminus \{v\}$ damit erst recht $v \in \langle S \setminus \{v\} \rangle_K$. Nach Prop. (8.9) (i) bedeutet dies, dass S linear abhängig ist. Unsere Annahme hat also erneut zu einem Widerspruch geführt.

„(iii) ⇒ (i)“ Nehmen wir an, dass B kein Erzeugendensystem von V ist. Dann existiert ein $v \in V \setminus \langle B \rangle_K$. Nach Prop. (8.9) (ii) ist deshalb mit B auch $B \cup \{v\}$ linear unabhängig. Aber dies widerspricht der Voraussetzung, dass B maximal als linear unabhängige Teilmenge von V ist. Also ist B sowohl linear unabhängig als auch ein Erzeugendensystem von V, insgesamt eine Basis. □

(9.3) Proposition Sei V ein K-Vektorraum, E ein Erzeugendensystem von V und $B \subseteq E$ eine maximale linear unabhängige Teilmenge von E. Dann ist B eine Basis von V.

Beweis: Nach Voraussetzung ist $B \cup \{v\}$ für jedes $v \in E \setminus B$ linear abhängig. Nach Prop. (8.9) (i) folgt daraus jeweils $v \in \langle B \rangle_K$, es gilt also $E \setminus B \subseteq \langle B \rangle_K$. Zusammen mit $B \subseteq \langle B \rangle_K$ erhalten wir $E \subseteq \langle B \rangle_K$. Weil $\langle B \rangle_K$ ein Untervektorraum von V ist, folgt $V = \langle E \rangle_K \subseteq \langle B \rangle_K$ nach Satz (8.3). Es gilt somit $V = \langle B \rangle_K$, und B ist linear unabhängig. Also ist B insgesamt eine Basis von V. □

(9.4) Lemma *(Austauschlemma)*
Sei V ein K-Vektorraum, $S \subseteq V$ eine linear unabhängige Teilmenge und $E \subseteq V$ ein Erzeugendensystem von V. Dann gibt es für jeden Vektor $v \in S \setminus E$ ein $w \in E \setminus S$, so dass auch $(S \setminus \{v\}) \cup \{w\}$ eine linear unabhängige Teilmenge von V ist.

Beweis: Sei $v \in S \setminus E$ und $S' = S \setminus \{v\}$. Nehmen wir an, dass kein w mit der angegebenen Eigenschaft existiert. Dann ist $(S \setminus \{v\}) \cup \{w\}$ für alle $w \in E \setminus S$ linear abhängig. Nach Prop. (8.9) (ii) folgt daraus $w \in \langle S' \rangle_K$ für alle $w \in E \setminus S$, also $E \setminus S \subseteq \langle S' \rangle_K$. Da auch $S' \subseteq \langle S' \rangle_K$ gilt, ist insgesamt $S' \cup (E \setminus S) = E \setminus \{v\}$ eine Teilmenge von $\langle S' \rangle_K$. Wegen $v \notin E$ gilt außerdem $E \setminus \{v\} = E$. Aus $E \subseteq \langle S' \rangle_K$ folgt nach Satz (8.3), dass $V = \langle E \rangle_K$ in $\langle S' \rangle_K$ enthalten ist. Es gilt also $V = \langle S' \rangle_K$, und insbesondere $v \in \langle S' \rangle_K$. Aber nach Prop. (8.9) (i) ist dann $S = S' \cup \{v\}$ linear abhängig, im Widerspruch zur Voraussetzung. □

(9.5) Satz *(Austauschsatz)*
Sei V ein K-Vektorraum, $S \subseteq V$ eine linear unabhängige Teilmenge und $E \subseteq V$ ein Erzeugendensystem. Dann gibt es für jede endliche Teilmenge $T \subseteq S$ eine Teilmenge $F \subseteq E$ mit der Eigenschaft, dass $|F| = |T|$ gilt und auch $(S \setminus T) \cup F$ linear unabhängig ist.

Beweis: Der Hauptteil des Beweises besteht im Nachweis der folgenden Hilfsaussage: Für jede endliche Teilmenge $T \subseteq S \setminus E$ gibt es eine Teilmenge $F \subseteq E \setminus S$, so dass $|F| = |T|$ gilt und $(S \setminus T) \cup F$ linear unabhängig ist. Wir beweisen diese Aussage durch vollständige Induktion über $n = |T|$. Ist $n = 0$, dann folgt $T = \emptyset$. Setzen wir $F = \emptyset$, dann gilt $|F| = 0 = |T|$. Außerdem gilt $(S \setminus T) \cup F = S$, also ist diese Menge linear unabhängig.

Sei nun $n \in \mathbb{N}_0$, und setzen wir die Aussage für n voraus. Sei $T \subseteq S \setminus E$ eine $(n+1)$-elementige Teilmenge und $v \in T$ ein beliebiges Element. Wir setzen $T' = T \setminus \{v\}$. Wegen $|T'| = n$ und $T' \subseteq S \setminus E$ dürfen wir die Induktionsvoraussetzung anwenden und erhalten eine Teilmenge $F' \subseteq E \setminus S$ mit $|F'| = n$ und der Eigenschaft, dass die Menge

$$S' \quad = \quad (S \setminus T') \cup F'$$

linear unabhängig ist. Nun wenden wir das Austauschlemma, Lemma (9.4), auf die linear unabhängige Menge S', das Erzeugendensystem E und den Vektor v an. Es gilt $v \in S' \setminus E$ (wird noch überprüft, siehe unten); deshalb ist die Anwendung des Austauschlemmas zulässig, und wir erhalten ein $w \in E \setminus S'$ derart, dass $(S' \setminus \{v\}) \cup \{w\}$ linear unabhängig ist.

Wir überprüfen nun, dass die Menge $F = F' \cup \{w\}$ alle gewünschten Eigenschaften hat. Wegen $w \notin F'$ (s.u.) gilt $|F| = n + 1$. Aus $F' \subseteq E \setminus S$ und $w \in E \setminus S$ (s.u.) folgt $F \subseteq E \setminus S$. Darüber hinaus gilt

$$(S' \setminus \{v\}) \cup \{w\} \quad = \quad (((S \setminus T') \cup F') \setminus \{v\}) \cup \{w\} \quad = \quad ((S \setminus T') \setminus \{v\}) \cup F' \cup \{w\} \quad = \quad (S \setminus T) \cup F \quad ,$$

wobei die zweite Gleichung dadurch zu Stande kommt, dass $v \notin F'$ gilt (s.u.) und es deshalb gleichgültig ist, ob wir erst F' hinzunehmen und dann v aus der Menge entfernen, oder umgekehrt. Um den Beweis der Hilfsaussage abzuschließen, müssen wir nur noch überprüfen, dass tatsächlich

$$\text{(i) } v \in S' \setminus E \qquad \text{(ii) } w \in E \setminus S \qquad \text{(iii) } v \notin F' \qquad \text{(iv) } w \notin F' \qquad \text{erfüllt ist.}$$

zu (i) Wegen $v \in S \setminus T'$ gilt $v \in S'$, und aus $v \in T$ und $T \subseteq S \setminus E$ folgt $v \notin E$.

zu (ii) Aus $w \in E \setminus S'$ folgt $w \in E$. Angenommen, es gilt auch $w \in S$. Weil aus $w \notin S'$ insbesondere $w \notin S \setminus T'$ folgt, ist dies nur möglich, wenn w in T' liegt. Aber dies ist wegen $w \in E$ und $T' \subseteq T \subseteq S \setminus E$ nicht der Fall.

zu (iii) Wegen $F' \subseteq E$, $v \in T$ und $T \subseteq S \setminus E$ ist $v \in F'$ ausgeschlossen.

zu (iv) Aus $w \in F'$ würde $w \in S'$ folgen, im Widerspruch zu $w \in E \setminus S'$.

Um nun die eigentliche Aussage des Austauschsatzes zu beweisen, sei $T \subseteq S$ eine endliche Teilmenge. Definieren wir $T' = T \setminus E$, dann besitzt T die disjunkte Zerlegung $T = T' \cup (T \cap E)$, und außerdem gilt $T' \subseteq S \setminus E$. Auf Grund der Hilfsaussage existiert eine Teilmenge $F' \subseteq E \setminus S$ mit $|F'| = |T'|$ und der Eigenschaft, dass $(S \setminus T') \cup F'$ linear unabhängig ist. Sei nun $F = F' \cup (T \cap E)$. Wegen $T \subseteq S$ und $F' \cap S = \emptyset$ ist auch dies eine disjunkte Zerlegung, und folglich gilt $|F| = |F'| + |T \cap E| = |T'| + |T \cap E| = |T|$. Außerdem gilt

$$(S \setminus T) \cup F \quad = \quad ((S \setminus T') \setminus (T \cap E)) \cup F \quad = \quad (S \setminus T') \setminus (T \cap E)) \cup (T \cap E) \cup F' \quad = \quad (S \setminus T') \cup F' \quad ,$$

also ist diese Menge linear unabhängig. □

Ein K-Vektorraum V wird ***endlich erzeugt*** genannt, wenn eine endliche Teilmenge $E \subseteq V$ mit $V = \langle E \rangle_K$ existiert.

(9.6) Satz Sei V ein endlich erzeugter K-Vektorraum.

(i) In V existiert eine endliche Basis B.

(ii) Für jede Basis B' von V gilt $|B'| = |B|$, insbesondere ist jede Basis endlich.

(iii) Ist $S \subseteq V$ linear unabhängig und $E \supseteq S$ ein Erzeugendensystem von V, dann gibt es eine Basis B' von V mit $S \subseteq B' \subseteq E$.

Beweis: zu (i) Nach Voraussetzung existiert eine endliche Teilmenge $E_0 \subseteq V$ mit $V = \langle E_0 \rangle_K$. Weil E_0 endlich ist, existiert in E_0 eine maximale linear unabhängige Teilmenge B, die natürlich ebenfalls endlich ist. Nach Prop. (9.3) ist B also eine endliche Basis von V.

zu (ii) Sei B' eine weitere Basis von V. Zunächst zeigen wir, dass $|B'| \geq |B|$ gilt. Dazu wenden wir den Austauschsatz (9.5) auf $S = T = B$ und $E = B'$ an. Demzufolge existiert eine Teilmenge $F \subseteq B'$ mit $|F| = |B|$. Insbesondere gilt also die Ungleichung $|B'| \geq |F| = |B|$.

Um die Endlichkeit von B' zu beweisen, wählen wir in B' eine beliebige Teilmenge T' mit $|T'| = |B|$, was wegen $|B'| \geq |B|$ möglich ist. Der Austauschsatz liefert uns eine Teilmenge $F' \subseteq B$ mit der Eigenschaft, dass $|F'| = |T'| = |B|$ gilt und $(B' \setminus T') \cup F'$ linear unabhängig ist. Wegen $F' \subseteq B$ und $|F'| = |B|$ gilt $F' = B$. Folglich ist die Menge $(B' \setminus T') \cup B$ linear unabhängig. Weil aber B als Basis nach Satz (9.2) eine *maximale* linear unabhängige Teilmenge von V ist, muss $B' \setminus T' \subseteq B$ gelten. Es folgt $|B'| \leq |B' \setminus T'| + |T'| = |B' \setminus T'| + |B| \leq |B| + |B| = 2|B|$, insbesondere ist B' endlich.

Dasselbe Argument, dass oben die Ungleichung $|B| \leq |B'|$ gezeigt hat, kann nun auch auf B' an Stelle von B angewendet werden, und ergibt damit die Abschätzung $|B'| \leq |B|$. Insgesamt ist damit $|B'| = |B|$ gezeigt.

zu (iii) Sei $n = |B|$; wir zeigen zunächst, dass $|T| \leq n$ für jede linear unabhängige Menge mit $S \subseteq T \subseteq E$ gelten muss. Wenden wir den Austauschsatz auf T, eine beliebige *endliche* Teilmenge $T' \subseteq T$ und das Erzeugendensystem B an, so erhalten wir eine Teilmenge $F \subseteq B$ mit $|F| = |T'|$. Daraus folgt $n = |B| \geq |F| = |T'|$. Jede endliche Teilmenge von T hat also eine Mächtigkeit $\leq n$; dies ist nur möglich, wenn T endlich ist und $|T| \leq n$ gilt. Auf Grund der soeben bewiesenen Ungleichung gibt es in E eine *maximale* linear unabhängige (und endliche) Teilmenge B' mit $B' \supseteq S$. Aus Prop. (9.3) folgt, dass diese Teilmenge B' eine Basis von V ist. □

Aus Teil (iii) von Satz (9.6) ergibt sich unmittelbar

(9.7) Folgerung Sei V ein endlich erzeugter K-Vektorraum.

(i) *(Basisergänzungssatz)*
Jede linear unabhängige Teilmenge $S \subseteq V$ kann zu einer Basis von V ergänzt werden.

(ii) *(Basisauswahlsatz)*
Aus jedem Erzeugendensystem E von V kann man eine Basis von V auswählen.

Beweis: Für Aussage (i) genügt es, Satz (9.6) (iii) auf S und $E = V$ anzuwenden. Für Aussage (ii) wendet man den Satz auf $S = \varnothing$ und E an. □

(9.8) Definition Sei V ein K-Vektorraum. Dann ist die ***Dimension*** von V definiert durch

$$\dim V \quad = \quad \begin{cases} |B| & \text{falls } B \text{ eine endliche Basis von } V \text{ ist,} \\ \infty & \text{falls } V \text{ nicht endlich erzeugt ist.} \end{cases}$$

Man überprüfe anhand der bisherigen Resultate, dass die Dimension eines beliebigen K-Vektorraums damit wohldefiniert ist: Nach Satz (9.6) hat V entweder eine endliche Basis, oder V ist nicht endlich erzeugt. Im ersten Fall gilt außerdem für beliebig gewählte endliche Basen B, B' von V jeweils $|B| = |B'|$; es ist somit gleichgültig, welche Basis man für die Definition der Dimension heranzieht.

Wir bestimmen nun die Dimensionen der meisten uns bereits bekannten Vektorräume.

(i) Ist K ein Körper und $n \in \mathbb{N}$, dann gilt $\dim K^n = n$. Denn wie wir bereits festgestellt haben, bilden die Einheitsvektoren $e_1, \ldots, e_n$ in K^n eine n-elementige Basis.

(ii) Seien K ein Körper und $m, n \in \mathbb{N}$. Dann gilt $\dim \mathscr{M}_{m\times n,K} = mn$, weil die Basismatrizen $B_{k\ell}^{(m\times n)}$ mit $1 \leq k \leq m$ und $1 \leq \ell \leq n$ eine mn-elementige Basis von $\mathscr{M}_{m\times n,K}$ bilden.

(iii) Wir wissen bereits, dass $\mathbb{C}$ auf natürliche Weise als $\mathbb{R}$-Vektorraum angesehen werden kann. Eine Basis dieses Vektorraums ist durch $\{1, i\}$ gegeben. Denn einerseits kann jedes $z \in \mathbb{C}$ auf Grund der Zerlegung in Real- und Imaginärteil in der Form $z = a \cdot 1 + b \cdot i$ mit $a, b \in \mathbb{R}$ dargestellt werden. Dies zeigt, dass $\{1, i\}$ ein Erzeugendensystem ist. Andererseits ist diese Darstellung auch eindeutig, denn aus $z = a \cdot 1 + b \cdot i$ mit $a, b \in \mathbb{R}$ folgt $a = \mathrm{Re}(z)$ und $b = \mathrm{Im}(z)$. Deshalb ist $\{1, i\}$ auch linear unabhängig. Für $\mathbb{C}$ als $\mathbb{R}$-Vektorraum gilt also $\dim \mathbb{C} = 2$; um zu verdeutlichen, dass $\mathbb{C}$ als $\mathbb{R}$-Vektorraum betrachtet wird, schreibt man $\dim_{\mathbb{R}} \mathbb{C} = 2$.

(iv) Fassen wir $\mathbb{C}$ dagegen als $\mathbb{C}$-Vektorraum auf, dann ist $\{1\}$ eine Basis, und es gilt $\dim \mathbb{C} = \dim_{\mathbb{C}} \mathbb{C} = 1$. Allgemein ist es nicht schwer zu zeigen, dass $\dim_{\mathbb{C}} \mathbb{C}^n = n$ und $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$ für alle $n \in \mathbb{N}$ gilt; eventuell erledigen wir das in den Übungen.

(v) Ist K ein Körper und V ein K-Vektorraum mit $V = \{0_V\}$, dann gilt $\dim V = 0$, denn in diesem Fall ist die leere Menge $\varnothing$ eine nullelementige Basis von V. Tatsächlich ist $\varnothing$ linear unabhängig, und die einzige Linearkombination von $\varnothing$ ist der Nullvektor; es gilt also $\langle \varnothing \rangle_K = \{0_V\}$. Man kann sich leicht überlegen, dass umgekehrt aus $\dim V = 0$ jeweils $V = \{0_V\}$ folgt.

(vi) Für jeden Körper K gilt $\dim K[x] = \infty$. Denn wie wir in § 6 festgestellt haben, besitzt $K[x]$ als K-Vektorraum kein endliches Erzeugendensystem.

Als weitere Konsequenz aus Satz (9.6) notieren wir noch

(9.9) Folgerung Sei V ein endlich erzeugter K-Vektorraum und $n = \dim V$.

(i) Für jede linear unabhängige Teilmenge $S \subseteq V$ gilt $|S| \leq n$ mit Gleichheit genau dann, wenn S eine Basis von V ist.

(ii) Für jedes Erzeugendensystem E von V gilt $|E| \geq n$ mit Gleichheit genau dann, wenn E eine Basis von V ist.

Beweis: zu (i) Sei $S \subseteq V$ linear unabhängig. Nach dem Basisergänzungssatz gibt es eine Basis B von V mit $B \supseteq S$. Daraus folgt $|S| \leq |B| = \dim V = n$. Beweisen wir nun die Äquivalenz. Gilt $|S| = n$, dann folgt aus $S \subseteq B$ und $|S| = n = |B|$ die Gleichheit $S = B$. In diesem Fall ist S also selbst eine Basis. Setzen wir umgekehrt voraus, dass S eine Basis von V ist, dann muss $|S| = \dim V = n$ gelten, denn die Dimension von V kann mit jeder beliebigen Basis bestimmt werden.

zu (ii) Sei $E \subseteq V$ ein Erzeugendensystem. Nach dem Basisauwahlsatz gibt es eine Basis $B \subseteq E$ von V. Daraus folgt $n = \dim V = |B| \leq |E|$. Gilt $|E| = n$ dann folgt aus $|E| = n = |B|$ und $B \subseteq E$ die Gleichheit $E = B$. Also ist E in diesem Fall selbst eine Basis. Setzen wir andererseits voraus, dass E eine Basis von V ist, dann muss $|E| = \dim V = n$ gelten, mit demselben Argument wie in Teil (i). □

Die soeben bewiesene Aussage kann folgendermaßen praktisch genutzt werden: Wenn man von einem endlich erzeugten K-Vektorraum V die (endliche) Dimension n bereits kennt und $T \subseteq V$ eine n-elementige Teilmenge ist, dann folgt aus der linearen Unabhängigkeit bereits die Basiseigenschaft von T. Ebenso folgt aus $V = \langle T \rangle_K$ bereits die Basiseigenschaft.

Beispielsweise ist wegen $\dim \mathbb{R}^3 = 3$ jede dreielementige linear unabhängige Teilmenge des $\mathbb{R}^3$ bereits eine Basis von $\mathbb{R}^3$, und ebenso ist jedes dreielementige Erzeugendensystem eine Basis. Andererseits zeigt die Folgerung auch, dass es in $\mathbb{R}^3$ kein zweielementiges Erzeugendensystem und keine vierelementige linear unabhängige Teilmenge geben kann.

(9.10) Folgerung Sei V ein endlich erzeugter K-Vektorraum, $n = \dim V$ und U ein Untervektorraum von V. Dann gilt $\dim U \leq n$ mit Gleichheit genau dann, wenn $U = V$ gilt.

Beweis: Sei B eine Basis von U. Dann ist B insbesondere eine linear unabhängige Teilmenge von V, und aus Folgerung (9.9) (i) erhalten wir $\dim U = |B| \leq n$. Setzen wir $U = V$ voraus, dann folgt offenbar $\dim U = \dim V = n$. Sei nun umgekehrt $\dim U = n = \dim V$ vorausgesetzt. Dann ist B wegen $|B| = \dim U$ eine n-elementige linear unabhängige Teilmenge von V. Aus Folgerung (9.9) (i) ergibt sich, dass B eine Basis von V ist. Somit gilt $U = \langle B \rangle_K = V$. □

Zum Abschluss des Kapitels soll eine praktische Umsetzung von Basisauswahlsatz und Basisergänzungssatz diskutiert werden. Konkret beantworten wir die folgenden beiden Fragen. Sei V ein endlich-dimensionaler K-Vektorraum.

- Wenn $E = \{v_1, ..., v_r\}$ ein Erzeugendensystem von V ist, wie findet man eine in E enthaltene Basis?
- Wenn $S = \{v_1, ..., v_r\}$ eine r-elementige linear unabhängige Teilmenge von V ist, wie lässt sich die Menge S zu einer Basis von V ergänzen?

Der folgende Satz liefert eine Antwort auf die erste Frage im Spezialfall $V = K^m$. Wir werden später sehen, dass jeder endlich-dimensionale K-Vektoraum $V \neq \{0_V\}$ isomorph zu K^m für ein $m \in \mathbb{N}$ ist. Das Problem der Basisauswahl lässt sich dann leicht auf solche Vektorräume übertragen.

(9.11) Satz Seien $m, n \in \mathbb{N}$, und sei $S = \{v_1, ..., v_n\}$ eine n-elementige Teilmenge von K^m. Sei $A \in \mathcal{M}_{m\times n,K}$ die Matrix, deren Spalten genau die Vektoren $v_1, ..., v_n$ sind, und sei A' die Matrix in normierter ZSF, die man durch Anwendung des Gauß-Verfahrens auf A erhält. Seien $r, j_1, ..., j_r$ die Kennzahlen der ZSF. Dann ist $\{v_{j_1}, ..., v_{j_r}\}$ eine Basis von $\langle S\rangle_K$.

Beweis: Die gemeinsame Lösungsmenge $\mathcal{L} \subseteq K^n$ der homogenen linearen Gleichungssysteme mit den Koeffizientenmatrizen A und A' sind genau die Tupel $(\lambda_1, ..., \lambda_n)$ mit der Eigenschaft $\lambda_1 v_1 + ... + \lambda_n v_n = 0_{K^m}$. Sei $S = \{1, ..., n\} \setminus \{j_1, ..., j_r\}$. Wir betrachten nun das LGS zur Matrix A'. Bilden wir für ein beliebiges $\ell \in S$ den Lösungsvektor b_ℓ wie es im Kapitel zur Lösung von LGS beschrieben, dann enthält dieser an der ℓ-ten Position den Wert 1, und die übrigen Einträge ungleich null müssen sich auf die Positionen $j_1, ..., j_r$ verteilen. Dies zeigt, dass der Vektor v_ℓ eine Linearkombination von $T = \{v_{j_1}, ..., v_{j_r}\}$ ist. Insgesamt zeigt dies, dass die Vektoren $v_1, ..., v_n$ alle in $\langle T\rangle_K$ enthalten und T folglich ein Erzeugendensystem von $\langle S\rangle_K$ ist.

Wäre T keine Basis von $\langle S\rangle_K$, also linear abhängig, dann müsste es nach Prop. (8.9) (i) möglich sein, ein Element v_{j_k} als Linearkombination der Vektoren v_{j_s} mit $s \neq k$ darzustellen. Es gäbe dann in $\mathcal{L}$ ein Element der Form $(\lambda_1, ..., \lambda_n)$ mit $\lambda_{j_k} = 1$ und $\lambda_\ell = 0$ für alle $\ell \in S$. Setzt man diese Werte aber in die der k-ten Zeile von A' entsprechenden Gleichung ein, in der (nach Definition der normierten ZSF) alle Koeffizienten der Variablen x_{j_s} mit $s \neq k$ gleich null sind, so erhält man die falsche Gleichung $1 = 0$. Der Widerspruch zeigt, dass es in $\mathcal{L}$ kein derartiges Element und somit auch keine Darstellung von v_{j_k} als Linearkombination der Vektoren v_{j_s} mit $s \neq k$ existiert. □

Wir demonstrieren die Anwendung des Satzes an einem konkreten Beispiel. Unser Ziel ist es, aus der Teilmenge $S = \{v_1, v_2, v_3\}$ des $\mathbb{R}^3$ gegeben durch

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad , \quad v_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{und} \quad v_3 = \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$$

eine Basis des Vektorraums $V = \langle S \rangle_K$ auszuwählen. Dazu tragen wir die Vektoren als Spalten in eine Matrix ein und formen auf normierte ZSF um.

$$\begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 3 \\ 3 & 1 & 4 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 1 & 2 \\ 0 & -1 & -1 \\ 0 & -2 & -2 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & -2 & -2 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Die normierte ZSF am Ende hat die Kennzahlen $r = 2$, $j_1 = 1$ und $j_2 = 2$. Nach Satz (9.11) ist somit $\{v_1, v_2\}$ eine Basis von $\langle S \rangle_K$. Anhand der Lösungsmenge des zur Matrix gehörenden homogenen LGS lässt sich auch leicht erkennen, dass der Vektor v_3 als Linearkombination von $\{v_1, v_2\}$ dargestellt werden kann und somit für eine Basis von $\langle S \rangle_K$ nicht benötigt wird. Die Matrix in normierter ZSF entspricht dem LGS bestehend aus den Gleichungen $x_1 + x_3 = 0$, $x_2 + x_3 = 0$. Die Lösungsmenge ist somit gegeben durch

$$\mathscr{L} \quad = \quad \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \;\middle|\; x_1 = -x_3 \;,\; x_2 = -x_3 \right\} \quad = \quad \left\{ \begin{pmatrix} -x_3 \\ -x_3 \\ x_3 \end{pmatrix} \;\middle|\; x_3 \in \mathbb{R} \right\} \quad = \quad \left\{ x_3 \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \;\middle|\; x_3 \in \mathbb{R} \right\}.$$

Der Lösungsvektor $(-1,-1,1) \in \mathscr{L}$ liefert die Gleichung $(-1)v_1 + (-1)v_2 + v_3 = 0_{\mathbb{R}^3}$, was zu $v_3 = v_1 + v_2$ äquivalent ist.

Kommen wir nun zu unserer zweiten Frage. Gegeben sei eine linear unabhängige Teilmenge $S = \{v_1, ..., v_n\}$ im K^m, die zu einer Basis von K^m ergänzt werden soll. Wir wissen bereits, dass die Menge $\{e_1, ..., e_m\}$ der Einheitsvektoren eine Basis und damit erst recht ein Erzeugendensystem des K^m bildet. Also ist auch die Menge $T = \{v_1, ..., v_n, e_1, ..., e_m\}$ ein Erzeugendensystem des K^m. Mit dem in Satz (9.11) formulierten Kriterium kann aus T eine Basis ausgewählt werden. Dabei ist nur zu beachten, dass die Vektoren $v_1, ..., v_n, e_1, ..., e_m$ tatsächlich in dieser Reihenfolge als Spalten in die Matrix A eingetragen werden.

Für $1 \leq \ell \leq n+m$ wird der ℓ-te Vektor der Menge T vom Algorithmus genau dann aus dem Erzeugensystem entfernt, wenn ℓ in der Menge S liegt, also nicht unter den Kennzahlen $j_1, ..., j_r$ der normierten ZSF vorkommt. Der zugehörige Lösungsvektor b_ℓ besitzt Einträge ungleich null nur an den Stellen j_k mit $k < \ell$ (denn nach Definition der normierten ZSF kann der Eintrag $a'_{k\ell}$ der ℓ-ten Spalte nur dann ungleich null sein, wenn $j_k < \ell$ ist). Dies bedeutet, dass der Vektor v_ℓ eine Linearkombination der Vektoren v_{j_k} mit $j_k < \ell$ ist. Weil die Menge $S = \{v_1, ..., v_n\}$ linear unabhängig ist, ist kein v_k mit $k \in \{1, ..., n\}$ als Linearkombination von $v_1, ..., v_{k-1}$ darstellbar. Dies bedeutet, dass keiner der Vektoren v_k aus dem Erzeugendensystem entfernt wird. Somit ist gewährleistet, dass wir tatsächlich eine Basis von K^m erhalten, die S als Teilmenge enthält.

Auch die Basisergänzung demonstrieren wir an einem konkreten Beispiel. Wie man mit Proposition (8.9) (i) leicht überprüft, ist die Menge $S = \{v_1, v_2\}$ bestehend aus den Vektoren

$$v_1 = \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} \qquad \text{und} \qquad v_2 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

linear unabhängig. Unser Ziel besteht darin, S zu einer Basis von $\mathbb{R}^3$ zu ergänzen. Dazu schreiben wir die Vektoren v_1, v_2, e_1, e_2, e_3 als Spalten in eine Matrix und formen diese auf normierte ZSF um.

$$\begin{pmatrix} 2 & 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 \\ 3 & 3 & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 \\ 3 & 3 & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & \frac{3}{2} & -\frac{3}{2} & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -\frac{3}{2} & 1 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 & -\frac{2}{3} \end{pmatrix} \mapsto \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -1 & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & -\frac{2}{3} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 1 & 0 & -\frac{1}{3} \\ 0 & 1 & -1 & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & -\frac{2}{3} \end{pmatrix}$$

Die normierte ZSF hat die Kennzahlen $r = 3$, $j_1 = 1$, $j_2 = 2$, $j_3 = 4$. Mit Satz (9.11) folgt daraus, dass $B = \{v_1, v_2, e_2\}$ eine Basis von $\mathbb{R}^3$ ist, die zudem S als Teilmenge enthält.

Ähnlich wie im vorherigen Beispiel findet man durch Bestimmung der Lösungsmenge $\mathscr{L} \subseteq \mathbb{R}^5$ des homogenen LGS zur umgeformten Matrix konkrete Darstellungen von e_1 und e_3 als Linearkombinationen der Basis B; es gilt

$$1 \cdot \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

und

$$(-\tfrac{1}{3}) \cdot \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} + \tfrac{2}{3} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + (-\tfrac{2}{3}) \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

§ 10. Dimensionssätze

Inhaltsübersicht

In diesem Abschnitt beweisen wir zwei wichtige Sätze über die Dimension von Vektorräumen. Der Schnittdimensionssatz stellt einen Zusammenhang her zwischen den Dimensionen von $W \cap W'$ und $W + W'$, falls W und W' Untervektorräume eines K-Vektorraums V sind. Der Dimensionssatz für eine lineare Abbildung $\phi : V \to W$ besagt, dass sich die Dimension des Kerns und die Dimension des Bildes von ϕ immer zur Dimension von V addieren. Dieser Satz lässt sich auch für Matrizen formulieren und liefert auf diese Weise wichtige Aussagen über die Lösungsmengen linearer Gleichungssysteme.

Wichtige Begriffe und Sätze

- (direkte) Summe von Untervektorräumen
- Zeilen- und Spaltenraum, Zeilen- und Spaltenrang einer Matrix
- Dimensionssatz für lineare Abbildungen
- Schnittdimensionssatz
- Dimensionssatz für lineare Abbildungen
- Rangsatz

(10.1) Proposition Sei V ein K-Vektorraum, und seien U, U' Untervektorräume von V. Dann sind auch die Mengen

$$U \cap U' \qquad \text{und} \qquad U + U' = \{u + u' \mid u \in U, u' \in U'\} \qquad \text{Untervektorräume von } V.$$

Man bezeichnet $U + U'$ als die ***Summe*** von U und U'.

Beweis: Zunächst beweisen wir die Untervektorraum-Eigenschaft von $U \cap U'$. Weil U, U' nach Voraussetzung Untervektorräume sind, gilt $0_V \in U$ und $0_V \in U'$. Es folgt $0_V \in U \cap U'$. Seien nun Elemente $v_1, v_2 \in U \cap U'$ und $\lambda \in K$ beliebig vorgegeben. Dann gilt insbesondere $v_1, v_2 \in U$. Weil U ein Untervektorraum ist, folgt $v_1 + v_2 \in U$ und $\lambda v_1 \in U$, und ebenso gilt $v_1 + v_2 \in U'$ und $\lambda v_1 \in U'$, weil U' ein Untervektorraum ist. Aus $v_1 + v_2 \in U$ und $v_1 + v_2 \in U'$ folgt $v_1 + v_2 \in U \cap U'$, ebenso erhalten wir $\lambda v_1 \in U \cap U'$. Damit sind die Untervektorraum-Eigenschaften für die Menge $U \cap U'$ nachgewiesen.

Nun zeigen wir, dass auch die Menge $U + U'$ ein Untervektorraum von V ist. Wegen $0_V \in U$ und $0_V \in U'$ gilt zunächst $0_V = 0_V + 0_V \in U + U'$. Seien nun $v_1, v_2 \in U + U'$ und $\lambda \in K$ vorgegeben. Dann gibt es $u_1, u_2 \in U$ und $u_1', u_2' \in U'$ mit $v_1 = u_1 + u_1'$ und $v_2 = u_2 + u_2'$. Weil U ein Untervektorraum ist, gilt $u_1 + u_2 \in U$, ebenso gilt $u_1' + u_2' \in U'$. Es folgt $v_1 + v_2 = (u_1 + u_1') + (u_2 + u_2') = (u_1 + u_2) + (u_1' + u_2') \in U + U'$. Aus der Untervektorraum-Eigenschaft von U und U' folgt auch, dass $\lambda u_1 \in U$ und $\lambda u_1' \in U'$ gilt. Wir erhalten $\lambda v_1 = \lambda(u_1 + u_1') = \lambda u_1 + \lambda u_1' \in U + U'$. Damit haben wir auch die Untervektorraum-Eigenschaften von $U + U'$ nachgerechnet. □

Auch aus mehr als zwei Untervektorräumen kann eine Summe gebildet werden. Sei V ein K-Vektorraum, und sei $U_1, U_2, U_3, \ldots$ eine beliebige Anzahl von Untervektorräumen von V. Man definiert

$$\sum_{k=1}^{1} U_k = U_1 \qquad \text{und} \qquad \sum_{k=1}^{r+1} U_k = \left(\sum_{k=1}^{r} U_k\right) + U_{r+1} \quad \text{für} \quad r \geq 1.$$

Der Nachweis, dass es sich bei $\sum_{k=1}^{r} U_k$ für jedes $r \in \mathbb{N}$ um einen Untervektorraum von V handelt, erfolgt durch vollständige Induktion über r, was hier aus Zeitgründen aber nicht ausgeführt wird. Ebenso zeigt man durch vollständige Induktion, dass

$$\sum_{k=1}^{r} U_k \quad = \quad \left\{ \sum_{k=1}^{r} u_k \;\middle|\; u_k \in U_k \text{ für } 1 \leq k \leq r \right\} \qquad \text{gilt.}$$

(10.2) Definition Ein K-Vektorraum V wird ***direkte Summe*** der Untervektorräume $U, U' \subseteq V$ genannt, wenn die Bedingungen

$$V = U + U' \quad \text{und} \quad U \cap U' = \{0_V\} \qquad \text{erfüllt sind.}$$

Die direkte Summe zweier Untervektorräume U, U' wird mit $U \oplus U'$ bezeichnet.

(10.3) Lemma Sei V ein K-Vektorraum mit Untervektorräumen $U, U' \subseteq V$. Dann sind die folgenden Bedingungen äquivalent:

(i) $V = U \oplus U'$

(ii) Für jedes $v \in V$ gibt es eindeutig bestimmte Vektoren $u \in U$ und $u' \in U'$ mit $v = u + u'$.

Beweis: „(i) ⇒ (ii) “ Wegen $V = U + U'$ gibt es für jeden Vektor $v \in V$ Elemente $u \in U$ und $u' \in U'$ mit $v = u + u'$. Wir beweisen nun die Eindeutigkeit. Sei $v \in V$, und seien $u_1, u_2 \in U$ und $u_1', u_2' \in U'$ mit $v = u_1 + u_1' = u_2 + u_2'$. Dann gilt $u_1 - u_2 = u_2' - u_1' \in U \cap U'$. Wegen $U \cap U' = \{0_V\}$ folgt $u_1 - u_2 = u_2' - u_1' = 0_V$, also $u_1 = u_2$ und $u_1' = u_2'$.

„(ii) ⇒ (i)“ Weil jeder Vektor $v \in V$ in der Form $v = u + u'$ mit $u \in U$ und $u \in U'$ geschrieben werden kann, gilt $V = U + U'$. Wir zeigen nun, dass auch $U \cap U' = \{0_V\}$ erfüllt ist. Die Inklusion „$\supseteq$“ ist offensichtlich, da U und U' Untervektorräume sind und somit 0_V in U und U' enthalten ist. Sei nun $v \in U \cap U'$ vorgegeben. Nach Voraussetzung gibt es eindeutig bestimmte $u \in U$, $u' \in U'$ mit $v = u + u'$. Aus $v = 0_V + v$ mit $0_V \in U$ und $v \in U'$ folgt auf Grund der Eindeutigkeit $u = 0_V$. Ebenso können wir v auch in der Form $v = v + 0_V$ mit $v \in U$ und $0_V \in U'$ schreiben. Diesmal liefert die Eindeutigkeit die Gleichung $u' = 0_V$. Insgesamt erhalten wir $v = u + u' = 0_V + 0_V = 0_V$. □

Auch die direkte Summe von mehreren Untervektorräumen lässt sich rekursiv definieren. Sei V ein K-Vektorraum, und seien $U_1, U_2, U_3, \ldots$ Untervektorräume von V. Dann setzt man

$$\bigoplus_{k=1}^{1} U_k = U_1 \qquad \text{und} \qquad \bigoplus_{k=1}^{r+1} U_k = \left(\bigoplus_{k=1}^{r} U_k\right) \oplus U_{r+1} \quad \text{für} \quad r \geq 1.$$

Damit die direkte Summe $\bigoplus_{k=1}^{r+1} U_k$ gebildet werden kann, dürfen sich $\bigoplus_{k=1}^{r} U_k$ und U_{r+1} jeweils nur in $\{0_V\}$ schneiden.

(10.4) Satz Sei V ein Vektorraum, $r \in \mathbb{N}$, und seien $U_1, ..., U_r$ Untervektorräume von V. Dann sind die folgenden Aussagen äquivalent.

(i) Es gilt $V = \bigoplus_{k=1}^{r} U_k$.

(ii) Jeder Vektor $v \in V$ kann auf eindeutige Weise als Summe $v = \sum_{k=1}^{r} u_k$ dargestellt werden, mit $u_k \in U_k$ für $1 \leq k \leq r$.

(iii) Für $1 \leq k \leq r$ gilt $V = \sum_{j=1}^{r} U_j$ und $U_k \cap \left(\sum_{j \neq k} U_j \right) = \{0_V\}$.

Beweis: Wir beweisen die Äquivalenz der drei Aussagen durch vollständige Induktion über r. Im Fall $r = 1$ besteht (i) nur in der Aussage $V = U_1$. Aussage (ii) besagt, dass für jedes $v \in V$ ein eindeutig bestimmter Vektor $u_1 \in U_1$ mit $v = u_1$ existiert, was offenbar zu (i) äquivalent ist. Die Aussage (iii) besteht aus den Gleichungen $V = U_1$ und $U_1 \cap \{0_V\} = \{0_V\}$, und wiederum ist „(i) $\Leftrightarrow$ (iii)“ offensichtlich.

Sei nun $r \in \mathbb{N}$ vorgegeben, und setzen wir die Äquivalenz von (i), (ii) und (iii) für dieses r voraus. Seien $U_1, ..., U_{r+1}$ beliebige Untervektorräume von V. Wir beginnen mit dem Beweis der Implikation „(i) $\Rightarrow$ (ii)“. Hier lautet die Voraussetzung

$$V \quad = \quad \bigoplus_{k=1}^{r+1} U_k \quad = \quad \left(\bigoplus_{k=1}^{r} U_k \right) \oplus U_{r+1}.$$

Insbesondere gilt $V = \sum_{k=1}^{r+1} U_k$; dies bedeutet, dass jedes $v \in V$ jedenfalls als Summe $v = u_1 + ... + u_{r+1}$ dargestellt werden kann, mit $u_k \in U_k$ für $1 \leq k \leq r+1$. Nehmen wir nun an, dass $v = u_1' + ... + u_{r+1}'$ eine weitere solche Darstellung ist. Weil V nach Voraussetzung die direkte Summe von $\bigoplus_{k=1}^{r} U_k$ und U_{r+1} ist, folgt $u_1 + ... + u_r = u_1' + ... + u_r'$ und $u_{r+1} = u_{r+1}'$ nach Lemma (10.3). Nach Induktionsvoraussetzung besitzt jedes Element in $\bigoplus_{k=1}^{r} U_k$ eine eindeutige Darstellung als Summe von Elementen in $U_1, ..., U_k$. Aus $u_1 + ... + u_r = u_1' + ... + u_r'$ folgt also $u_k = u_k'$ für $1 \leq k \leq r$.

Beweisen wir nun die Implikation „(ii) $\Rightarrow$ (iii)“ und setzen dazu (ii) voraus. Zunächst zeigen wir die Gleichung $V = \sum_{k=1}^{r+1} U_k$. Die Inklusion „$\supseteq$“ ist nach Definition der Summe offensichtlich. Andererseits hat auf Grund unserer Voraussetzung jedes Element $v \in V$ eine Darstellung $v = u_1 + ... + u_{r+1}$ mit $u_k \in U_k$ für $1 \leq k \leq r+1$. Also gilt auch „$\subseteq$“. Sei nun $k \in \{1, ..., r+1\}$ vorgegeben. Zu zeigen ist die Gleichung

$$U_k \cap \left(\sum_{j \neq k} U_j \right) \quad = \quad \{0_V\}.$$

Hier ist „$\supseteq$“ offensichtlich erfüllt. Zum Beweis von „$\subseteq$“ nehmen wir an, dass ein Vektor $v \neq 0_V$ im Durchschnitt existiert. Dann liegt v einerseits in U_k, andererseits gilt $v = \sum_{j \neq k} u_j$ für gewisse Elemente u_j mit $u_j \in U_j$ für $1 \leq j \leq r+1$ und $j \neq k$. Setzen wir $u_k = -v$, dann gilt $\sum_{j=1}^{r+1} u_j = 0_V$. Weil aber der Nullvektor auch in der Form $0_V + ... + 0_V$ mit $0_V \in U_j$ für $1 \leq j \leq r+1$ dargestellt werden kann, und weil diese Darstellung nach (ii) eindeutig ist, folgt $u_j = 0_V$ für $1 \leq j \leq r+1$ mit $j \neq k$ und auch $v = -u_k = 0_V$, im Widerspruch zur Annahme.

Zeigen wir nun noch die Implikation „(iii) ⇒ (i)“ und setzen dazu (iii) voraus. Zu zeigen ist

$$V \quad = \quad \bigoplus_{k=1}^{r+1} U_k \quad = \quad \left(\bigoplus_{k=1}^{r} U_k\right) \oplus U_{r+1}.$$

Wir betrachten den Untervektorraum $U = \sum_{k=1}^{r} U_k$. Nach Voraussetzung gilt $U_k \cap (\sum_{j\neq k} U_j) = \{0_V\}$ für $1 \leq k \leq r+1$. Damit ist für $1 \leq k \leq r$ jeweils erst recht der Durchschnitt von U_k mit $\sum_{j\neq k,r+1} U_j$ gleich $\{0_V\}$. Also ist die Bedingung (iii) für den K-Vektorraum U und die Untervektorräume $U_1, ..., U_r$ von U erfüllt. Die Induktionsvoraussetzung liefert uns damit $U = \bigoplus_{k=1}^{r} U_k$. Weiter gilt nach Voraussetzung $V = U + V_{r+1}$, außerdem $U \cap V_{r+1} = \{0_V\}$. Somit folgt schließlich die Gleichung $V = U \oplus V_{r+1} = \bigoplus_{k=1}^{r+1} U_k$. □

(10.5) Satz *(Schnittdimensionssatz)*

Sei V ein endlich erzeugter K-Vektorraum, und seien W, W' Untervektorräume von V. Dann gilt

$$\dim(W + W') \quad = \quad \dim(W) + \dim(W') - \dim(W \cap W').$$

Beweis: Sei $n = \dim(W \cap W')$ und $\{v_1, ..., v_n\}$ eine Basis von $W \cap W'$. Weil $W \cap W'$ ein Untervektorraum sowohl von W als auch von W' ist, gilt $\dim(W \cap W') \leq \dim W$ und $\dim(W \cap W') \leq \dim W'$ nach Folgerung (9.10). Es gibt also $k, \ell \in \mathbb{N}_0$ mit $\dim W = n + k$ und $\dim W' = n + \ell$.

Weil $\{v_1, ..., v_n\}$ eine linear unabhängige Menge in W ist, existieren nach dem Basisergänzungssatz Vektoren $w_1, ..., w_k$, so dass $B = \{v_1, ..., v_n, w_1, ..., w_k\}$ eine Basis von W ist. Ebenso finden wir Elemente $w'_1, ..., w'_\ell$ mit der Eigenschaft, dass die Familie $B' = \{v_1, ..., v_n, w'_1, ..., w'_\ell\}$ eine Basis von W' ist. Der Satz ist bewiesen, wenn wir zeigen können, dass es sich bei

$$B_0 \quad = \quad B \cup B' \quad = \quad \{v_1, ..., v_n, w_1, ..., w_k, w'_1, ..., w'_\ell\}$$

um eine $n + k + \ell$-elementige Basis von $W + W'$ handelt, denn dann gilt

$$\dim(W + W') \quad = \quad n + k + \ell \quad = \quad (n + k) + (n + \ell) - n \quad = \\ \dim(W) + \dim(W') - \dim(W \cap W').$$

Zunächst zeigen wir, dass B_0 ein Erzeugendensystem von $W + W'$ ist. Jedes $v \in W + W'$ lässt sich in der Form $v = w + w'$ mit $w \in W$ und $w' \in W'$ schreiben. Da $\{v_1, ..., v_n, w_1, ..., w_k\}$ eine Basis von W ist, finden wir Koeffizienten $\mu_i, \lambda_i \in K$ mit $w = \sum_{i=1}^{n} \mu_i v_i + \sum_{i=1}^{k} \lambda_i w_i$. Ebenso gibt es $\mu'_i, \lambda'_i \in K$ mit $w' = \sum_{i=1}^{n} \mu'_i v_i + \sum_{i=1}^{\ell} \lambda'_i w'_i$. Insgesamt erhalten wir

$$v \quad = \quad w + w' \quad = \quad \sum_{i=1}^{n} (\mu_i + \mu'_i) v_i + \sum_{i=1}^{k} \lambda_i w_i + \sum_{i=1}^{\ell} \lambda'_i w'_i \quad ,$$

also kann jedes $v \in W + W'$ tatsächlich als Linearkombination von B_0 dargestellt werden.

Als nächstes überprüfen wir, dass B_0 tatsächlich aus $n + k + \ell$ verschiedenen Elementen besteht. Besteht die Menge aus weniger Elementen, dann muss $w_i = w'_j$ für gewissen i, j mit $1 \leq i \leq k$ und $1 \leq j \leq \ell$ gelten. Dies würde bedeuteten,

dass w_i in $W \cap W'$ enthalten ist. Damit wäre w_i also in $\langle v_1, ..., v_n \rangle_K$ enthalten und die Menge B damit linear abhängig, im Widerspruch zur Basis-Eigenschaft von B. Also ist $|B_0| = n + k + \ell$ erfüllt.

Nun beweisen wir die lineare Unabhängigkeit. Seien $\mu_i, \lambda_i, \lambda'_i \in K$ Koeffizienten mit

$$\sum_{i=1}^{n} \mu_i v_i + \sum_{i=1}^{k} \lambda_i w_i + \sum_{i=1}^{\ell} \lambda'_i w'_i \quad = \quad 0.$$

Sei $v = \sum_{i=1}^{n} \mu_i v_i + \sum_{i=1}^{k} \lambda_i w_i \in W$. Wegen $v = -\sum_{i=1}^{\ell} \lambda'_i w'_i$ liegt v in $W \cap W'$. Weil $\{v_1, .., v_n\}$ eine Basis von $W \cap W'$ ist, gibt es auch $\alpha_1, ..., \alpha_n \in K$ mit $v = \sum_{i=1}^{n} \alpha_i v_i$. Es folgt

$$\sum_{i=1}^{n} (\mu_i - \alpha_i) v_i + \sum_{i=1}^{k} \lambda_i w_i \quad = \quad \left(\sum_{i=1}^{n} \mu_i v_i + \sum_{i=1}^{k} \lambda_i w_i \right) - \sum_{i=1}^{n} \alpha_i v_i \quad = \quad v - v \quad = \quad 0.$$

Auf Grund der linearen Unabhängigkeit von B erhalten wir $\mu_i = \alpha_i$ für $1 \leq i \leq n$ und $\lambda_i = 0$ für $1 \leq i \leq k$. Setzen wir dies oben ein, so erhalten wir $\sum_{i=1}^{n} \mu_i v_i + \sum_{i=1}^{\ell} \lambda'_i w'_i = 0$. Wegen der linearen Unabhängigkeit von B' folgt daraus wiederum $\lambda'_i = 0$ für $1 \leq i \leq \ell$ und $\mu_i = 0$ für $1 \leq i \leq n$. □

(10.6) Folgerung Sei V ein endlich-dimensionaler K-Vektorraum, und seien W, W' Untervektorräume von V, so dass $V = W \oplus W'$ erfüllt ist. Sei B eine Basis von W und B' eine Basis von W'. Dann gilt

(i) $\dim V = \dim W + \dim W'$

(ii) Die Mengen B und B' sind disjunkt.

(iii) Die Vereinigung $B \cup B'$ ist eine Basis von V.

Beweis: Sei $m = \dim W$ und $m' = \dim W'$. Nach Voraussetzung gilt $W \cap W' = \{0_V\}$, also $\dim(W \cap W') = 0$. Aus dem Schnittdimensionssatz folgt

$$\dim V \quad = \quad \dim W + \dim W' - \dim(W \cap W') \quad = \quad m + m' - 0 \quad = \quad m + m'.$$

Sei $B = \{w_1, ..., w_m\}$ eine Basis von W und $B' = \{w'_1, ..., w'_{m'}\}$ eine Basis von W'. Wir zeigen, dass $E = B \cup B'$ ein Erzeugendensystem von V ist. Sei $v \in V$ vorgegeben. Wegen $V = W + W'$ gibt es $w \in W$ und $w' \in W'$ mit $v = w + w'$. Weil B eine Basis von W und B' eine Basis von W' ist, gibt es $\lambda_1, ..., \lambda_m \in K$ und $\mu_1, ..., \mu_{m'} \in K$ mit

$$w = \sum_{k=1}^{m} \lambda_k w_k \qquad \text{und} \qquad w' = \sum_{k=1}^{m'} \mu_k w'_k.$$

Es folgt

$$v \quad = \quad w + w' \quad = \quad \sum_{k=1}^{m} \lambda_k w_k + \sum_{k=1}^{m'} \mu_k w'_k.$$

Dies zeigt, dass E tatsächlich ein Erzeugendensystem von V ist. Wegen $\dim V = m + m'$ besteht jedes Erzeugendensystem von V aus mindestens $m+m'$ Elementen. Die Mengen B und B' sind also disjunkt, da ansonsten $|E| < m+m'$ gelten würde. Als $(m+m')$-elementiges Erzeugendensystem ist E wegen $\dim V = m+m'$ eine Basis von V. □

Durch vollständige Induktion über r erhält man

(10.7) Folgerung Sei V ein K-Vektorraum, und seien $W_1, ..., W_r$ Untervektorräume von V mit $V = \bigoplus_{k=1}^{r} W_k$. Dann gilt $\dim V = \sum_{k=1}^{r} \dim W_k$. Ist B_k eine Basis von W_k für $1 \le k \le r$, dann ist $B = \bigcup_{k=1}^{r} B_k$ eine Basis von V, und es gilt $B_k \cap B_\ell = \varnothing$ für $k \neq \ell$.

Als nächstes untersuchen wir die Vektorraum-Dimension im Zusammenhang mit linearen Abbildungen.

(10.8) Satz Seien V, W endlich-dimensionale Vektorräume über einem Körper K, und sei $\phi : V \to W$ eine lineare Abbildung. Dann gilt

$$\dim V \quad = \quad \dim \ker(\phi) + \dim \operatorname{im}(\phi).$$

Beweis: Sei $\{u_1, ..., u_m\}$ eine Basis von $\ker(\phi)$ und $\{w_1, ..., w_n\}$ eine Basis von $\operatorname{im}(\phi)$. Wir wählen für jedes w_i einen Vektor $v_i \in V$ mit $\phi(v_i) = w_i$ und zeigen, dass durch

$$B \quad = \quad \{u_1, ..., u_m, v_1, ..., v_n\}$$

eine $(m+n)$-elementige Basis von V gegeben ist. Haben wir dies gezeigt, dann ist damit $\dim V = m+n = \dim \ker(\phi) + \dim \operatorname{im}(\phi)$ bewiesen. Dass B aus weniger als $m+n$ Elementen besteht ist nur möglich, wenn $u_i = v_j$ für gewisse i, j mit $1 \le i \le m$ und $1 \le j \le n$ gilt. Aber dann wäre $w_j = \phi(v_j) = \phi(u_i) = 0_W$ im Widerspruch dazu, dass w_j in einer Basis von W liegt und somit ungleich Null sein muss.

Zunächst weisen wir nun nach, dass es sich bei B um ein Erzeugendensystem von V handelt. Sei dazu $v \in V$ vorgegeben. Da $\{w_1, ..., w_n\}$ eine Basis von $\operatorname{im}(\phi)$ ist, finden wir $\lambda_1, ..., \lambda_n \in K$ mit

$$\phi(v) \quad = \quad \sum_{i=1}^{n} \lambda_i w_i.$$

Aus der Linearität der Abbildung ϕ folgt $\phi(v) = \sum_{i=1}^{n} \lambda_i \phi(v_i) = \phi(v')$ mit $v' = \sum_{i=1}^{n} \lambda_i v_i$. Wegen $\phi(v) - \phi(v') = \phi(v - v') = 0_W$ liegt dann der Vektor $v - v'$ in $\ker(\phi)$. Da $\{u_1, ..., u_m\}$ eine Basis dieses Untervektorraums ist, existieren $\mu_1, ..., \mu_m \in K$ mit

$$v - v' = \sum_{j=1}^{m} \mu_j u_j \qquad \Leftrightarrow \qquad v = \sum_{j=1}^{m} \mu_j u_j + v' = \sum_{j=1}^{m} \mu_j u_j + \sum_{i=1}^{n} \lambda_i v_i.$$

Damit haben wir gezeigt, dass B ein Erzeugendensystem von V ist. Nun beweisen wir die lineare Unabhängigkeit. Seien $\mu_i, \lambda_j \in K$ mit

$$\sum_{i=1}^{m} \mu_i u_i + \sum_{j=1}^{n} \lambda_j v_j \quad = \quad 0_V$$

vorgegeben. Wenden wir die lineare Abbildung ϕ auf beide Seiten der Gleichung an, dann folgt

$$0_W \quad = \quad \phi(0_V) \quad = \quad \phi\left(\sum_{i=1}^{m}\mu_i u_i + \sum_{j=1}^{n}\lambda_j v_j\right) \quad = \quad 0_W + \sum_{j=1}^{n}\lambda_j \phi(v_j) \quad = \quad \sum_{j=1}^{n}\lambda_j w_j.$$

Dabei haben wir verwendet, dass die Summe $\sum_{i=1}^{m}\mu_i u_i$ in $\ker(\phi)$ enthalten ist. Weil die Menge $\{w_1, ..., w_n\}$ linear unabhängig ist, bedeutet dies $\lambda_1 = ... = \lambda_n = 0$. Setzen wir dies in die Ausgangsgleichung ein, dann erhält man $\sum_{i=1}^{m}\mu_i u_i = 0_V$. Da $\{u_1, ..., u_m\}$ nach Voraussetzung einer Basis von $\ker(\phi)$ und insbesondere linear unabhängig ist, hat dies wiederum $\mu_1 = ... = \mu_m = 0$ zur Folge. Also B tatsächlich linear unabhängig. □

(10.9) Folgerung Für isomorphe Vektorräume V, W gilt $\dim V = \dim W$.

Beweis: Wir beschränken uns auf den Fall, dass V und W endlich erzeugt sind. Sei $\phi : V \to W$ ein Isomorphismus. Dann ist $\ker(\phi) = \{0_V\}$ und $\mathrm{im}(\phi) = W$. Also folgt die Aussage aus dem Dimensionssatz (10.8) für lineare Abbildungen. □

Wir werden den Dimensionssatz für lineare Abbildungen nun verwenden, um die Struktur von Matrizen genauer zu untersuchen.

(10.10) Proposition Sei $A = (a_{ij})$ eine $(m \times n)$-Matrix über K und $\phi_A : K^n \to K^m$ die lineare Abbildung gegeben durch $v \mapsto Av$. Dann gilt

(i) Für $1 \leq k \leq n$ gilt $\phi_A(e_k) = a_{\bullet k}$. Die Bilder der Einheitsvektoren sind also genau die Spalten der Matrix.

(ii) Es gilt $\mathrm{im}(\phi_A) = \langle a_{\bullet 1}, ..., a_{\bullet n}\rangle_K$.

Beweis: zu (i) Sei $k \in \{1, ..., n\}$ vorgegeben. Nach Definition des Matrix-Vektor-Produkts erhält man für jedes $i \in \{1, ..., m\}$ den i-ten Eintrag von $\phi_A(e_k)$ durch die Formel

$$\sum_{j=1}^{n} a_{ij}\delta_{jk} \quad = \quad a_{ik}\delta_{kk} \quad = \quad a_{ik}.$$

Dies ist genau der i-te Eintrag des k-ten Spaltenvektors $a_{\bullet k}$ der Matrix.

zu (ii) Sei $v \in K^n$ beliebig vorgegeben, $v = (\lambda_1, ..., \lambda_n)$. Da ϕ_A eine lineare Abbildung ist, gilt

$$\phi_A\left(\sum_{k=1}^{n}\lambda_k e_k\right) \quad = \quad \sum_{k=1}^{n}\lambda_k \phi_A(e_k) \quad = \quad \sum_{k=1}^{n}\lambda_k a_{\bullet k}.$$

Damit ist $\mathrm{im}(\phi_A) \subseteq \langle a_{\bullet 1}, ..., a_{\bullet n}\rangle_K$ nachgewiesen. Andererseits ist $\mathrm{im}(\phi_A)$ ein Untervektorraum von K^m, der nach Teil (i) die Menge $\{a_{\bullet 1}, ..., a_{\bullet n}\}$ der Spaltenvektoren enthält. Nach Satz (8.3) (ii) folgt $\langle a_{\bullet 1}, ..., a_{\bullet n}\rangle_K \subseteq \mathrm{im}(\phi_A)$. □

(10.11) Definition Sei A eine $(m \times n)$-Matrix über K.

(i) Der Untervektorraum $\mathrm{im}(\phi_A) = \langle a_{\bullet 1}, \ldots, a_{\bullet n} \rangle_K$ von K^m wird der ***Spaltenraum*** der Matrix A genannt und von uns mit $\mathrm{SR}(A)$ bezeichnet. Die Dimension $\mathrm{sr}(A) = \dim \mathrm{SR}(A)$ nennt man den ***Spaltenrang*** von A.

(ii) Ebenso nennt man den Untervektorraum von K^n gegeben durch $\langle a_{1\bullet}, \ldots, a_{m\bullet} \rangle_K$ den ***Zeilenraum*** von A und bezeichnet ihn mit $\mathrm{ZR}(A)$. Die Dimension $\mathrm{zr}(A) = \dim \mathrm{ZR}(A)$ wird ***Zeilenrang*** von A genannt.

Zur Illustration dieser neuen Begriffe betrachten wir die Matrix

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

Der Zeilenraum von A wird aufgespannt von den Zeilenvektoren der Matrix A, es gilt also

$$\mathrm{ZR}(A) \quad = \quad \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\rangle_{\mathbb{R}}.$$

Die Menge $\{(1,2,3),(4,5,6)\}$ ist linear unabhängig, da $(1,2,3)$ nicht der Nullvektor und $(4,5,6)$ kein Vielfaches von $(1,2,3)$ ist. Somit ist diese Menge eine Basis des Zeilenraums von A, und es folgt $\mathrm{zr}(A) = \dim \mathrm{ZR}(A) = 2$. Der Spaltenraum von A wird von den Spalten der Matrix aufgespannt, es gilt also

$$\mathrm{ZR}(A) \quad = \quad \left\langle \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix} \right\rangle_{\mathbb{R}}.$$

Die Menge $\{(1,4),(2,5),(3,6)\}$ ist linear abhängig, denn es gilt

$$\begin{pmatrix} 3 \\ 6 \end{pmatrix} \quad = \quad (-1) \cdot \begin{pmatrix} 1 \\ 4 \end{pmatrix} + 2 \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

während $\{(1,4),(2,5)\}$ offenbar linear unabhängig ist. Dies zeigt, dass $\{(1,4),(2,5)\}$ eine Basis des Spaltenraums $\mathrm{SR}(A)$ ist, und es folgt $\mathrm{sr}(A) = \dim \mathrm{SR}(A) = 2$. Zeilen- und Spaltenraum haben also die gleiche Dimension, obwohl sie in unterschiedlichen Vektorräumen enthalten sind; nach Definition ist $\mathrm{ZR}(A) \subseteq \mathbb{R}^3$ und $\mathrm{SR}(A) \subseteq \mathbb{R}^2$. Die weiteren Ausführungen werden zeigen, dass diese Übereinstimmung kein Zufall ist.

Für Matrizen in normierter ZSF hatten wir den Zeilenrang schon im letzten Semester definiert; es handelt sich um die Kennzahl r der ZSF. Wir zeigen, dass in diesem Spezialfall die neu eingeführte Definition des Zeilenrangs mit der alten Definition übereinstimmt.

(10.12) Proposition Sei $A \in \mathscr{M}_{m\times n,K}$ eine Matrix in normierter Zeilenstufenform, mit r und $j_1, \ldots, j_r$ als Kennzahlen. Dann ist r der Zeilenrang von A im Sinne von Definition (10.11).

Beweis: Wir zeigen, dass in der Matrix A die Zeilenvektoren $a_{1\bullet}, ..., a_{r\bullet} \in K^n$ ungleich Null linear unabhängig sind und somit eine Basis des Zeilenraums $\mathrm{ZR}(A)$ bilden. Seien $\lambda_1, ..., \lambda_r \in K$ vorgegeben, mit

$$\sum_{i=1}^{r} \lambda_i a_{i\bullet} \quad = \quad 0_{K^n}. \tag{10.13}$$

Nach Definition der normierten ZSF ist in der j_k-ten Spalte der Eintrag $a_{kj_k} = 1_K$ der einzige Eintrag ungleich Null. Insgesamt sind die Einträge der j_k-ten Spalte also gegeben durch $a_{ij_k} = \delta_{ik}$ für $1 \leq i \leq m$. Betrachtet man in der Gleichung (10.13) also jeweils die j_k-te Komponenten für $k = 1, ..., r$, so erhält man die Gleichungen

$$\sum_{i=1}^{r} \lambda_i a_{ij_k} = 0_K \quad \Leftrightarrow \quad \sum_{i=1}^{r} \lambda_i \delta_{ik} = 0_K \quad \Leftrightarrow \quad \lambda_k = 0_K.$$

Damit ist die lineare Unabhängigkeit nachgewiesen. Nach Definition bilden die Zeilen von A ein Erzeugendensystem von $\mathrm{ZR}(A)$, und dasselbe gilt auch für die Zeilen ungleich Null. Somit besitzt der Zeilenraum $\mathrm{ZR}(A)$ eine r-elementige Basis, und es folgt $\mathrm{zr}(A) = \dim \mathrm{ZR}(A) = r$. □

(10.14) Proposition Sei $A \in \mathscr{M}_{m\times n,K}$ und $i \in \{1, ..., m\}$ eine Zeilennummer mit der Eigenschaft, dass die i-te Zeile von A eine Linearkombination der übrigen $m-1$ Zeilen ist. Entsteht nun die Matrix $\bar{A} \in \mathscr{M}((m-1)\times n, K)$ aus A durch Streichung der i-ten Zeile, dann gilt $\mathrm{ZR}(\bar{A}) = \mathrm{ZR}(A)$ (also insbesondere $\mathrm{zr}(\bar{A}) = \mathrm{zr}(A)$) und ebenso $\mathrm{sr}(\bar{A}) = \mathrm{sr}(A)$.

Beweis: Nach Definition der Untervektorräume $\mathrm{ZR}(A)$ und $\mathrm{ZR}(\bar{A})$ gilt

$$\mathrm{ZR}(A) = \langle a_{1\bullet}, ..., a_{m\bullet} \rangle_K \qquad \text{und} \qquad \mathrm{ZR}(\bar{A}) = \langle a_{1\bullet}, ..., a_{i-1\bullet}, a_{i+1\bullet}, ..., a_{m\bullet} \rangle_K.$$

Nach Voraussetzung enthält $\mathrm{ZR}(\bar{A})$ neben den Vektoren $a_{k\bullet}$ mit $k \neq i$ auch den i-ten Zeilenvektor $a_{i\bullet}$. Aus der Inklusion $\{a_{1\bullet}, ..., a_{m\bullet}\} \subseteq \mathrm{ZR}(\bar{A})$ und der Untervektorraum-Eigenschaft von $\mathrm{ZR}(\bar{A})$ folgt $\mathrm{ZR}(A) \subseteq \mathrm{ZR}(\bar{A})$. Die umgekehrte Inklusion $\mathrm{ZR}(\bar{A}) \subseteq \mathrm{ZR}(A)$ ist offensichtlich.

Wir betrachten nun die Abbildung $\pi : K^m \to K^{m-1}$, die aus jedem Vektor $c \in K^m$ die i-te Komponente entfernt, also $\pi(c) = (c_1, ..., c_{i-1}, c_{i+1}, ..., c_m)$ für $c = (c_1, ..., c_m) \in K^m$. Man überprüft unmittelbar, dass π eine lineare Abbildung ist. Die Spalten der Matrix A werden von π auf die Spalten von $\bar{A}$ abgebildet. Durch Übergang zur eingeschränkten Abbildung $\phi = \pi|_{SR(A)}$ erhalten wir also eine surjektive lineare Abbildung $\phi : \mathrm{SR}(A) \to \mathrm{SR}(\bar{A})$.

Nun zeigen wir, dass $\ker(\phi) = \{0_{K^m}\}$ gilt. Weil die i-te Zeile von A eine Linearkombination der übrigen Zeilen ist, gibt es Koeffizienten $\mu_j \in K$ mit

$$a_{i\bullet} \quad = \quad \sum_{k=1}^{i-1} \mu_k a_{k\bullet} + \sum_{k=i+1}^{m} \mu_k a_{k\bullet}.$$

Die Einträge der Matrix erfüllen also die Gleichungen $a_{ij} = \sum_{k=1}^{i-1} \mu_k a_{kj} + \sum_{k=i+1}^{m} \mu_k a_{kj}$ für $1 \leq j \leq n$. Die Spalten $w_1, ..., w_n$ von A sind damit im Untervektorraum

$$W \quad = \quad \left\{ c \in K^m \;\middle|\; c_i = \sum_{k=1}^{i-1} \mu_k c_k + \sum_{k=i+1}^{m} \mu_k c_k \right\}$$

von K^m enthalten, es gilt also $\mathrm{SR}(A) \subseteq W$. Sei nun $c \in \ker(\phi)$ vorgegeben. Es gilt $(c_1, ..., c_{i-1}, c_{i+1}, ..., c_m) = \phi(c) = (0, ..., 0)$, also $c_j = 0$ für $j \neq i$. Wegen $c \in W$ ist damit auch

$$c_i \quad = \quad \sum_{k=1}^{i-1} \mu_k c_k + \sum_{k=i+1}^{m} \mu_k c_k \quad = \quad \sum_{k=1}^{i-1} \mu_k \cdot 0 + \sum_{k=i+1}^{m} \mu_k \cdot 0 \quad = \quad 0 \quad , \quad \text{also} \quad c = 0_{K^m}.$$

Damit ist $\ker(\phi) = \{0_{K^m}\}$ bewiesen. Durch Anwendung des Dimensionssatzes für lineare Abbildungen, Satz (10.8), auf die Abbildung ϕ erhalten wir $\mathrm{sr}(A) = \dim \mathrm{SR}(A) = \dim \ker(\phi) + \dim \mathrm{im}(\phi) = 0 + \dim SR(\bar{A}) = \mathrm{sr}(\bar{A})$. □

(10.15) Satz *(Rangsatz)*

Für jede Matrix $A \in \mathscr{M}_{m\times n,K}$ gilt $\mathrm{zr}(A) = \mathrm{sr}(A)$. Wir bezeichnen die Zahl $\mathrm{zr}(A)$ deshalb einfach als den ***Rang*** $\mathrm{rg}(A)$ der Matrix.

Beweis: Sei $r = \mathrm{zr}(A)$. Nach dem Basisauswahlsatz können wir so lange Zeilen aus A streichen, bis die verbleibenden r Zeilen der Restmatrix $A' \in \mathscr{M}(r \times n, K)$ eine Basis von $\mathrm{ZR}(A)$ bilden. Durch wiederholte Anwendung von Prop. (10.14) erhalten wir $\mathrm{zr}(A) = \mathrm{zr}(A') = r$ und $\mathrm{sr}(A) = \mathrm{sr}(A')$. Wegen $\mathrm{SR}(A') \subseteq K^r$ und $\dim K^r = r$ gibt es in $\mathrm{SR}(A')$ keine linear unabhängige Teilmenge mit mehr als r Elementen; es gilt also $\mathrm{sr}(A) = \mathrm{sr}(A') \leq r = \mathrm{zr}(A)$. Anwendung derselben Abschätzung auf die transponierte Matrix ${}^tA$ liefert $\mathrm{zr}(A) = \mathrm{sr}({}^tA) \leq \mathrm{zr}({}^tA) = \mathrm{sr}(A)$, denn die Zeilen von A sind die Spalten von ${}^tA$ und umgekehrt. Insgesamt gilt also $\mathrm{zr}(A) = \mathrm{sr}(A)$. □

Wie man sich leicht überzeugt, ändert sich der Zeilenrang einer Matrix durch elementare Zeilenumformungen nicht. Denn jede Zeile in der Matrix *nach* einer solchen Umformung ist Linearkombination der Zeilen in der Matrix *vor* der Umformung. Der Zeilenrang kann also durch eine elementare Zeilenumformung nicht größer werden. Weil andererseits jede solche Umformung durch eine weitere elementare Zeilenumformung rückgängig gemacht werden kann, ist es ebenso unmöglich, dass der Zeilenrang kleiner wird.

Der Rang einer Matrix A lässt sich leicht berechnen: Wie wir in § 3 gezeigt haben, lässt sich A durch endlich viele Zeilenumformungen in eine Matrix A' in normierter ZSF überführen. Seien r und $j_1, ..., j_r$ die Kennzahlen dieser ZSF. Nach Prop. (10.12) ist r der Zeilenrang von A'. Weil sich der Zeilenrang durch elementare Zeilenumformungen nicht ändert, ist r auch der Zeilenrang und somit der Rang der Matrix A.

Den Kern der linearen Abbildung $\phi_A : K^n \to K^m$, $v \mapsto Av$ nennt man auch den ***Kern der Matrix*** A und bezeichnet ihn mit $\ker(A)$. Aus dem Rangsatz und dem Dimensionssatz für lineare Abbildungen ergibt sich die folgende Formel für die Dimension von Lösungsmengen linearer Gleichungssysteme.

(10.16) Satz Sei $A \in \mathscr{M}_{m\times n,K}$ und $\mathscr{L} \subseteq K^n$ die Lösungsmenge des linearen Gleichungssystems

$$Ax \quad = \quad 0_{K^m}.$$

Dann gilt $\dim \mathscr{L} = n - \mathrm{rg}(A)$.

Beweis: Wie oben sei $\phi_A : K^n \to K^m$ gegeben durch $\phi_A(v) = Av$. Nach Definition ist der Lösungsraum $\mathscr{L}$ gegeben durch $\mathscr{L} = \{x \in K^n \mid Ax = 0_{K^m}\} = \ker(\phi_A)$. Der Dimensionssatz (10.8) liefert $\dim\ker(\phi_A) + \dim\operatorname{im}(\phi_A) = \dim K^n = n$. Wie wir oben bereits festgestellt haben, ist $\operatorname{im}(\phi_A)$ genau der Spaltenraum $\mathrm{SR}(A)$ von A. Folglich gilt $\dim\operatorname{im}(\phi_A) = \dim\mathrm{SR}(A) = \mathrm{sr}(A)$ und somit $\dim\ker(\phi_A) + \mathrm{sr}(A) = n$. Auf Grund des Rangsatzes (10.15) dürfen wir den Spaltenrang $\mathrm{sr}(A)$ durch den Rang $\mathrm{rg}(A)$ ersetzen und erhalten somit insgesamt $\dim\mathscr{L} = \dim\ker(\phi_A) = n - \mathrm{sr}(A) = n - \mathrm{rg}(A)$. □

Damit ist nun auch klar, wie man eine Basis des Lösungsraums $\mathscr{L}$ von $Ax = 0_{K^m}$ erhält: Sei A' die umgeformte Matrix in normierter ZSF mit Kennzahlen r und $j_1, ..., j_r$, und sei $S = \{1, ..., n\} \setminus \{j_1, ..., j_r\}$. Im Kapitel über lineare Gleichungssysteme wurde beschrieben, wie man mit Hilfe der Matrix A' jedem $\ell \in S$ einen Vektor $b_\ell \in K^n$ zuordnet, so dass jeder Vektor $v \in \mathscr{L}$ dann als Linearkombination der Vektoren b_ℓ darstellbar ist. Damit ist $E = \{b_\ell \mid \ell \in S\}$ ein Erzeugendensystem von $\mathscr{L}$. Weil $\dim\mathscr{L} = n - \mathrm{rg}(A) = n - r = |S|$ mit de Anzahl der Elemente von E übereinstimmt, muss E nach Folgerung (9.9) (ii) eine Basis von $\mathscr{L}$ sein.

Als weitere Anwendung des Dimensionssatzes zeigen wir noch

(10.17) Satz Sei $n \in \mathbb{N}$, und sei $\phi : V \to W$ eine lineare Abbildung zwischen Vektorräumen V, W derselben Dimension n. Dann sind äquivalent

(i) Die Abbildung ϕ ist injektiv.
(ii) Sie ist surjektiv.
(iii) Sie ist bijektiv.

Beweis: „(i) ⇒ (ii)“ Ist ϕ injektiv, dann gilt $\ker(\phi) = \{0_V\}$. Es folgt $\dim\ker(\phi) = 0$, und der Dimensionssatz für lineare Abbildungen liefert $\dim\operatorname{im}(\phi) = \dim V - \dim\ker(\phi) = n - 0 = n$. Sei B eine Basis von $\operatorname{im}(\phi)$. Dann ist B eine n-elementige linear unabhängige Teilmenge von W und wegen $\dim W = n$ nach Folgerung (9.9) (i) eine Basis von W. Es folgt $\operatorname{im}(\phi) = \langle B\rangle_K = W$ und damit die Surjektivität von ϕ.

„(ii) ⇒ (iii)“ Ist ϕ surjektiv, dann gilt $\operatorname{im}(\phi) = W$ und somit $\dim\operatorname{im}(\phi) = \dim W = n$. Der Dimensionssatz für lineare Abbildungen liefert $\dim\ker(\phi) = \dim V - \dim\operatorname{im}(\phi) = n - n = 0$. Es folgt $\ker(\phi) = \{0_V\}$, also ist ϕ injektiv und damit insgesamt bijektiv.

„(iii) ⇒ (i)“ Als bijektive Abbildung ist ϕ insbesondere injektiv. □

Kehren wir noch einmal zum Schnittdimensionssatz zurück, den wir zu Beginn des Kapitels behandelt haben. Auch hier stellt sich wieder die Frage nach einer konkreten Berechnungsmethode. Genauer: Ist V ein endlich-dimensionaler K-Vektorraum und sind U und W Untervektorräume gegeben jeweils durch eine Basis, wie findet man Basen der Untervektorräume $U+W$ und $U \cap W$? Bei der Summe $U+W$ ist die Sache einfach: Wie man leicht sieht, bilden die Basen von U und W bilden zusammengenommen ein Erzeugendensystem von $U+W$, und mit dem Basisauswahlverfahren aus § 9 kommt man zu einer Basis von $U+W$. Beim Durchschnitt erhält man ein Rechenverfahren mit Hilfe der folgenden Aussage.

(10.18) Proposition Sei V ein endlich-dimensionaler K-Vektorraum und seien U und W Untervektorräume mit $r = \dim U$ und $s = \dim W$. Es sei $\{u_1, ..., u_r\}$ eine Basis von U und $\{w_1, ..., w_s\}$ eine Basis von W. Weiter definieren wir die Teilmenge $\mathscr{L} \subseteq K^{r+s}$ durch

$$\mathscr{L} \quad = \quad \left\{ (\lambda_1, ..., \lambda_r, \mu_1, ..., \mu_s) \,\middle|\, \sum_{i=1}^{r} \lambda_i u_i + \sum_{j=1}^{s} \mu_j w_j = 0_V \right\}.$$

Dann gilt $U \cap W = \left\{ \sum_{i=1}^{r} \lambda_i u_i \;\middle|\; \lambda_1, ..., \lambda_r \in K \text{ , } \exists\, \mu_1, ..., \mu_s \text{ mit } (\lambda_1, ..., \lambda_r, \mu_1, ..., \mu_s) \in \mathscr{L} \right\}$.

Beweis: „$\subseteq$“ Ist $v \in U \cap W$, dann existieren Koeffizienten $\lambda_1, ..., \lambda_r$ und $\mu'_1, ..., \mu'_s$ in K mit

$$\sum_{i=1}^{r} \lambda_i u_i \quad = \quad v \quad = \quad \sum_{j=1}^{r} \mu'_j w_j.$$

Setzen wir $\mu_j = -\mu'_j$ für $1 \leq j \leq s$, dann folgt $\sum_{i=1}^{r} \lambda_i u_i + \sum_{j=1}^{r} \mu_j w_j = 0_V$. Also ist $v = \sum_{i=1}^{r} \lambda_i u_i$ ein Element der Menge auf der rechten Seite der Gleichung. „$\supseteq$“ Sei $v = \sum_{i=1}^{r} \lambda_i u_i$ ein Element der Menge rechts. Dann gibt es nach Definition Koeffizienten $\mu_1, ..., \mu_s \in K$, so dass $(\lambda_1, ..., \lambda_r, \mu_1, ..., \mu_s)$ in $\mathscr{L}$ liegt. Daraus wiederum folgt $\sum_{i=1}^{r} \lambda_i u_i + \sum_{j=1}^{s} \mu_j w_j = 0_V$ und somit $\sum_{i=1}^{r} \lambda_i u_i = -\sum_{j=1}^{s} \mu_j w_j \in U \cap W$. □

Mit Hilfe der Proposition erhält man das folgende Berechnungsverfahren für den Durchschnitt. Sei $V = K^m$, und seien U, W, r, s sowie die Vektoren u_i und w_j wie in der Proposition definiert.

- Trage die Vektoren $u_1, ..., u_r, w_1, ..., w_s$ als Spalten in eine Matrix $A \in \mathscr{M}_{m\times(r+s),K}$ ein.
- Wende das Gaußsche Eliminationsverfahren an, um A in eine Matrix $A' = (a'_{ij}) \in \mathscr{M}_{m\times(r+s),K}$ in normierter Zeilenstufenform umzuwandeln.
- Seien $b_1, ..., b_\ell \in K^{r+s}$ die Basisvektoren von $\mathscr{L}$, wie sie im Kapitel über lineare Gleichungssysteme definiert wurden. Setze $v_k = \sum_{i=1}^{r} b_{ki} u_i$ für $1 \leq k \leq \ell$. Dann ist $\{v_1, ..., v_\ell\}$ eine Basis von $U \cap W$.

Wir überprüfen die Korrektheit des Verfahrens. Die Matrix A, die im ersten Schritt definiert wurde, entspricht einem linearen Gleichungssystem bestehend aus n Gleichungen in $r + s$ Unbekannten, dessen Lösungsmenge genau mit der Menge $\mathscr{L}$ aus Prop. (10.18) übereinstimmt. In der Tat, ein Tupel $(\lambda_1, ..., \lambda_r, \mu_1, ..., \mu_s) \in K^{r+s}$ ist genau dann ein Element der Lösungsmenge, dann gilt $\sum_{i=1}^{r} \lambda_i u_{ik} + \sum_{j=1}^{s} \mu_j w_{jk} = 0$ für $1 \leq k \leq m$. Dabei ist die k-te Gleichung jeweils äquivalent dazu, dass die k-te Komponenten des Vektors $\sum_{i=1}^{r} \lambda_i u_i + \sum_{j=1}^{s} \mu_j w_j$ gleich Null ist. Alle Gleichungen zusammen sind also äquivalent zu $\sum_{i=1}^{r} \lambda_i u_i + \sum_{j=1}^{s} \mu_j w_j = 0_V$ und somit zu $(\lambda_1, ..., \lambda_r, \mu_1, ..., \mu_s) \in \mathscr{L}$. Weil die Spalten von A ein Erzeugendensystem von $U + W$ durchlaufen, gilt außerdem $\mathrm{rg}(A) = \dim(U + W)$.

Wegen $\mathrm{rg}(A) = \mathrm{rg}(A') = t$ gilt $\dim \mathscr{L} = r+s-t$ nach Satz (10.16). Aus Prop. (10.18) folgt, dass $U \cap W$ genau das Bild von $\pi(\mathscr{L})$ unter der Abbildung $\mathbb{R}^r \to \mathbb{R}^m$, $(\lambda_1, ..., \lambda_r) \mapsto \sum_{i=1}^{R} \lambda_i u_i$ ist. Daraus, dass die im letzten Schritt definierten Vektoren $v_1, ..., v_\ell$ den Untervektorraum $U \cap W$ aufspannen. Auf Grund des Schnittdimensionssatzes (10.5) gilt

$$\ell \quad = \quad \dim \mathscr{L} \quad = \quad r+s-t \quad = \quad r+s-\mathrm{rg}(A) \quad = \quad \dim U + \dim W - \dim(U+W) \quad = \quad \dim(U \cap W).$$

Deshalb bilden diese Vektoren sogar eine Basis von $U \cap W$.

Wir demonstrieren das Verfahren an einem konkreten Beispiel. Berechnet werden soll der Durchschnitt $U \cap W$ der Untervektorräume

$$U = \left\langle \begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 2 \\ -3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle_{\mathbb{R}} \qquad \text{und} \qquad W = \left\langle \begin{pmatrix} 1 \\ 2 \\ 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -1 \\ -1 \end{pmatrix} \right\rangle_{\mathbb{R}}$$

im $\mathbb{R}^4$. Wir setzen voraus, dass bereits überprüft wurde, dass es sich bei den angegebenen Erzeugendensystemen um Basen von U und W handelt. Der Anleitung von oben folgend, schreiben wir die Basisvektoren in eine Matrix und formen diese auf normierte ZSF um.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 2 & -1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 0 & -1 \\ 0 & -3 & 0 & 5 & -1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & -1 & -1 & 0 & -3 \\ 0 & 2 & 0 & -1 & -3 \\ 0 & -3 & 0 & 5 & -1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 2 & 0 & -1 & -3 \\ 0 & -3 & 0 & 5 & -1 \end{pmatrix} \mapsto$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & -2 & -1 & -9 \\ 0 & 0 & 3 & 5 & 8 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & \frac{1}{2} & \frac{9}{2} \\ 0 & 0 & 3 & 5 & 8 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & \frac{1}{2} & \frac{9}{2} \\ 0 & 0 & 0 & \frac{7}{2} & -\frac{11}{2} \end{pmatrix} \mapsto$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & \frac{1}{2} & \frac{9}{2} \\ 0 & 0 & 0 & 1 & -\frac{11}{7} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 1 & 0 & \frac{25}{7} \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 & \frac{37}{7} \\ 0 & 0 & 0 & 1 & -\frac{11}{7} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & -\frac{12}{7} \\ 0 & 1 & 0 & 0 & -\frac{16}{7} \\ 0 & 0 & 1 & 0 & \frac{37}{7} \\ 0 & 0 & 0 & 1 & -\frac{11}{7} \end{pmatrix}$$

An der Matrix in normierter ZSF kann abgelesen werden, dass der Lösungsraum des LGS durch

$$\mathscr{L} \quad = \quad \langle (\tfrac{12}{7}, \tfrac{16}{7}, -\tfrac{37}{7}, \tfrac{11}{7}, 1) \rangle_{\mathbb{R}} \quad = \quad \langle (12, 16, -37, 11, 7) \rangle_{\mathbb{R}}$$

gegeben ist. Laut Verfahren ist somit auch $U \cap W$ eindimensional, und es gilt $U \cap W = \langle v \rangle_{\mathbb{R}}$ mit dem Vektor

$$v \quad = \quad 12 \cdot \begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix} + 16 \cdot \begin{pmatrix} 0 \\ -1 \\ 2 \\ -3 \end{pmatrix} + (-37) \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \quad = \quad \begin{pmatrix} -25 \\ -29 \\ 7 \\ -48 \end{pmatrix}.$$

§ 11. Koordinatenabbildungen und Darstellungsmatrizen

Inhaltsübersicht

Das Rechnen in endlich-dimensionalen Vektorräumen wird durch die Einführung von Koordinatenabbildungen erheblich erleichtert, weil sich hierdurch jede Rechnung auf den einfach zu handhabenden Vektorraum K^n reduzieren lässt. Von großer praktischer Bedeutung ist die Umrechnung zwischen verschiedenen Koordinatensystemen; man denke zum Beispiel an die Verwendung unterschiedlicher Bezugssysteme in der Physik. Wir werden sehen, dass sich eine solche Umrechnung stets durch eine einfache Matrix-Vektor-Multiplikation bewerkstelligen lässt.

Genauso wie sich jedes Element eines endlich-dimensionalen Vektorraums V nach Wahl einer Basis durch ein Element des K^n beschreiben lässt, so kann eine lineare Abbildung zwischen zwei solchen Vektorräumen V, W durch eine Matrix angegeben werden. Zuvor müssen hierfür allerdings Basen auf V *und* W gewählt werden. Auch hier ist eine wichtige Frage, wie sich die Matrix ändert, wenn man auf V oder auf W zu einer anderen Basis übergeht.

Wichtige Begriffe und Sätze

- Koordinatenabbildung $\Phi_{\mathscr{B}}$ zu einer geordneten Basis
- lineare Abbildung $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)$ zu einer Matrix A
- Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$ einer linearen Abbildung ϕ
- Jeder n-dimensionale K-Vektorraum ist isomorph zum K^n.
- Existenz- und Eindeutigkeitssatz für lineare Abbildungen
- Rechenregeln für Darstellungsmatrizen, Transformationsformel

Alle Ergebnisse aus diesem Kapitel basieren auf der folgenden Feststellung.

(11.1) Lemma Sei V ein K-Vektorraum, $(v_1, ..., v_n)$ ein linear unabhängiges Tupel von Vektoren aus V und $U = \langle v_1, ..., v_n\rangle_K$. Dann besitzt jeder Vektor $v \in U$ genau eine Darstellung der Form $v = \sum_{j=1}^n \lambda_j v_j$ mit $\lambda_1, ..., \lambda_n \in K$.

Beweis: Sei $v \in V$. Die Existenz einer solchen Darstellung ergibt sich direkt aus der Definition von $\langle v_1, ..., v_n\rangle_K$ als Menge der Linearkombinationen von $\{v_1, ..., v_n\}$. Zum Nachweis der Eindeutigkeit seien $\lambda_1, ..., \lambda_n \in K$ und $\mu_1, ..., \mu_n \in K$ vorgegeben mit $v = \sum_{j=1}^n \lambda_n v_n = \sum_{j=1}^n \mu_n v_n$. Durch Umstellen erhalten wir die Gleichung

$$\sum_{j=1}^n (\lambda_j - \mu_j) v_j \quad = \quad \sum_{j=1}^n \lambda_j v_j - \sum_{j=1}^n \mu_j v_j \quad = \quad v - v \quad = \quad 0_V.$$

Weil das Tupel $(v_1, ...v_n)$ linear unabhängig ist, folgt $\lambda_j - \mu_j = 0_K$ und damit $\lambda_j = \mu_j$, für $1 \leq j \leq n$. □

(11.2) Satz *(Existenz und Eindeutigkeit linearer Abbildungen)*

Sei $n \in \mathbb{N}_0$, V ein endlich erzeugter und W ein beliebiger K-Vektorraum. Außerdem sei $(v_1, ..., v_n)$ ein Tupel von Vektoren aus V und $(w_1, ..., w_n)$ ein Tupel von Vektoren aus W.

(i) Ist $(v_1, ..., v_n)$ linear unabhängig, dann existiert eine lineare Abbildung $\phi : V \to W$ mit $\phi(v_j) = w_j$ für $1 \leq j \leq n$.

(ii) Gilt $V = \langle v_1, ..., v_n \rangle_K$, dann existiert höchstens eine lineare Abbildung $\phi : V \to W$ mit $\phi(v_j) = w_j$ für $1 \leq j \leq n$.

(iii) Ist $(v_1, ..., v_n)$ eine geordnete Basis von V, dann gibt es genau eine lineare Abbildung mit dieser Eigenschaft.

Beweis: Offenbar folgt die Aussage (iii) direkt aus (i) und (ii).

zu (i) Auf Grund des Basisergänzungssatzes (9.7) (i) können wir $v_1, ..., v_n$ durch weitere Vektoren $v_{n+1}, ..., v_m$ (mit $m \in \mathbb{N}_0$, $m \geq n$) zu einer Basis von V ergänzen. Nach Lemma (11.1) besitzt jeder Vektor $v \in V$ eine eindeutige Darstellung der Form $v = \sum_{j=1}^{m} \lambda_j v_j$. Wir definieren eine Abbildung $\phi : V \to W$, indem wir $\phi(v) = \sum_{j=1}^{n} \lambda_j w_j$ setzen, und überprüfen nun, dass diese Abbildung linear ist.

Seien $v, w \in V$ und $\alpha \in K$ vorgegeben. Zu zeigen ist $\phi(v + w) = \phi(v) + \phi(w)$ und $\phi(\lambda v) = \lambda \phi(v)$. Wiederum auf Grund von Lemma (11.1) existieren eindeutig bestimmte Tupel $(\lambda_1, ..., \lambda_m)$ und $(\mu_1, ..., \mu_m)$ in K^m mit $v = \sum_{j=1}^{m} \lambda_j v_j$ und $w = \sum_{j=1}^{m} \mu_j v_j$. Nach Definition ist $\phi(v) = \sum_{j=1}^{n} \lambda_j w_j$ und $\phi(w) = \sum_{j=1}^{n} \mu_j w_j$. Aus $v + w = \sum_{j=1}^{m} (\lambda_j + \mu_j) v_j$ und $\alpha v = \sum_{j=1}^{m} (\alpha \lambda_j) v_j$ folgt $\phi(v + w) = \sum_{j=1}^{n} (\lambda_j + \mu_j) w_j$ und $\phi(\alpha v) = \sum_{j=1}^{n} (\alpha \lambda_j) w_j$. Insgesamt erhalten wir

$$\phi(v + w) \quad = \quad \sum_{j=1}^{n} (\lambda_j + \mu_j) w_j \quad = \quad \sum_{j=1}^{n} \lambda_j w_j + \sum_{j=1}^{n} \mu_j w_j \quad = \quad \phi(v) + \phi(w)$$

und $\phi(\alpha v) = \sum_{j=1}^{n} (\alpha \lambda_j) w_j = \alpha \sum_{j=1}^{n} \lambda_j w_j = \alpha \phi(v)$, wie gewünscht.

zu (ii) Nehmen wir an, ϕ und ψ sind lineare Abbildung $V \to W$ mit $\phi(v_j) = w_j = \psi(v_j)$ für $1 \leq j \leq n$. Sei $v \in V$ vorgegeben; zu zeigen ist dann $\phi(v) = \psi(v)$. Wegen $V = \langle v_1, ..., v_n \rangle_K$ gibt es (nicht notwendigerweise eindeutig bestimmte) $\lambda_1, ..., \lambda_n \in K$ mit $v = \sum_{j=1}^{n} \lambda_j v_j$. Weil ϕ und ψ beide linear sind, erhalten wir

$$\phi(v) \quad = \quad \phi\left(\sum_{j=1}^{n} \lambda_j v_j \right) \quad = \quad \sum_{j=1}^{n} \lambda_j \phi(v_j) \quad = \quad \sum_{j=1}^{n} \lambda_j \psi(v_j) \quad = \quad \psi\left(\sum_{j=1}^{n} \lambda_j v_j \right) \quad = \quad \psi(v). \qquad \square$$

(11.3) Folgerung Sei $n \in \mathbb{N}_0$, V ein n-dimensionaler K-Vektorraum und $\mathcal{B} = (v_1, ..., v_n)$ eine geordnete Basis von V. Dann gibt es eine eindeutig bestimmte lineare Abbildung $\Phi_{\mathcal{B}} : V \to K^n$ mit $\Phi_{\mathcal{B}}(v_j) = e_j$ für $1 \leq j \leq n$ (wobei e_j jeweils den j-ten Einheitsvektor bezeichnet). Wir nennen sie die ***Koordinatenabbildung*** zur geordneten Basis $\mathcal{B}$. Es handelt sich dabei um einen Isomorphismus von K-Vektorräumen.

Beweis: Die Existenz und Eindeutigkeit folgt direkt aus Satz (11.2) (iii). Es bleibt zu zeigen, dass $\Phi_{\mathscr{B}}$ bijektiv ist. Wegen $\dim V = \dim K^n = n$ genügt es nach Satz (10.17), die Surjektivität zu überprüfen. Sei dazu $w \in K^n$ vorgegeben, $w = \sum_{j=1}^n \lambda_j e_j$ mit $\lambda_1, ..., \lambda_n \in K$. Setzen wir $v = \sum_{n=1}^n \lambda_j v_j$, dann erhalten wir

$$\phi(v) \quad = \quad \phi\left(\sum_{j=1}^n \lambda_j v_j\right) \quad = \quad \sum_{j=1}^n \lambda_j \phi(v_j) \quad = \quad \sum_{j=1}^n \lambda_j e_j \quad = \quad w.$$

Damit ist die Surjektivität nachgewiesen. □

Wir bemerken noch, dass nach Definition der Koordinatenabbildung das Bild $\Phi_{\mathscr{B}}(v_j)$ des j-ten Basisvektors gerade der j-te Einheitsvektor e_j ist. Es gilt nämlich $v_j = \sum_{k=1}^n \delta_{jk} v_k$, und die Koeffizienten δ_{jk} sind gerade die Komponenten des j-ten Einheitsvektors e_j.

Die folgende Aussage kann als Umkehrung von Satz (10.9) angesehen werden.

(11.4) Folgerung Zwischen zwei beliebigen K-Vektorräumen derselben endlichen Dimension existiert ein Isomorphismus.

Beweis: Seien V und W zwei n-dimensionale K-Vektorräume, und seien $\mathscr{B}$, $\mathscr{C}$ geordnete Basen von V bzw. W. Dann erhält man durch Komposition der Isomorphismen $\Phi_{\mathscr{B}} : V \to K^n$ und $\Phi_{\mathscr{C}}^{-1} : K^n \to W$ insgesamt einen Isomorphismus $\Phi_{\mathscr{C}}^{-1} \circ \Phi_{\mathscr{B}} : V \to W$ zwischen V und W. □

Für jedes $n \in \mathbb{N}$ sei $\mathscr{E}_n = (e_1, ..., e_n)$ die Basis des K^n bestehend aus den Einheitsvektoren. Man nennt $\mathscr{E}_n$ auch die ***kanonische Basis*** von K^n. Für jeden Vektor $v = (v_1, ..., v_n)$ gilt $\Phi_{\mathscr{E}_n}(v) = v$, also $\Phi_{\mathscr{E}_n} = \mathrm{id}_{K^n}$. Dies folgt unmittelbar aus der Gleichung $v = \sum_{k=1}^n v_k e_k$ und der Definition von $\Phi_{\mathscr{E}_n}(v)$.

Wir geben einige konkrete Beispiele für $\mathscr{B}$-Koordinaten an.

(i) Sei $K = \mathbb{R}$, $V = \mathbb{R}^3$ und $\mathscr{E}_3 = (e_1, e_2, e_3)$ die geordnete Basis bestehend aus den Einheitsvektoren. Gesucht werden die $\mathscr{E}_3$-Koordinaten des Vektors $v = (1, 3, 5)$. Es gilt

$$v \quad = \quad \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} \quad = \quad 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 5 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Also ist $\Phi_{\mathscr{E}_3}(v) = (1, 3, 5)$.

(ii) Wieder sei $K = \mathbb{R}$ und $V = \mathbb{R}^3$, aber diesmal suchen wir die $\mathscr{B}$-Koordinaten von $v = (1, 3, 5)$ bezüglich der Basis

$$\mathscr{B} \quad = \quad \left(\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \right).$$

Die Gleichung

$$v \quad = \quad \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} \quad = \quad 3 \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + (-5) \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \tfrac{5}{3} \cdot \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}$$

zeigt, dass diese Koordianten durch $\Phi_{\mathscr{B}}(v) = (3, -5, \frac{5}{3})$ gegeben sind.

In Beispiel (ii) war es nicht schwierig, die Koeffizienten 3, -5 und $\frac{5}{3}$ durch Vergleich der einzelnen Komponenten direkt zu finden. Im Allgemeinen bestimmt man die Koordinaten durch Lösen eines linearen Gleichungssystems. Dazu macht man in der vorliegenden Situation den Ansatz

$$\begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} \quad = \quad \lambda_1 \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \cdot \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}$$

mit $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$. Diese Gleichung ist äquivalent zu

$$\begin{pmatrix} 2\lambda_1 + \lambda_2 \\ \lambda_1 \\ 3\lambda_3 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}$$

und wird von genau den Tupeln $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$ erfüllt, die das inhomogene LGS bestehend aus den Gleichungen $2x_1 + x_2 = 1$, $x_1 = 3$, $3x_3 = 5$ lösen. Genauer gesagt besitzt dieses LGS genau *eine* Lösung, die wie immer auch mit dem Gauß-Algorithmus bestimmt werden kann.

Betrachten wir noch weitere Beispiele für $\mathscr{B}$-Koordinaten.

(iii) Sei $K = \mathbb{R}$ und V der $\mathbb{R}$-Vektorraum der Polynome in $\mathbb{R}[x]$ vom Grad ≤ 2. Dieser Raum besitzt $\mathscr{B} = (1, x, x^2)$ als geordnete Basis. Sei $f = x^2 - 2x + 1$. Es gilt

$$f \quad = \quad 1 \cdot 1 + (-2) \cdot x + 1 \cdot x^2$$

und somit $\Phi_{\mathscr{B}}(f) = (1, -2, 1)$.

(iv) Seien K, V und f wie im vorherigen Beispiel definiert; diesmal betrachten wir aber die geordnete Basis $\mathscr{C} = (1, x+1, x^2+x)$. Hier gilt nun

$$f \quad = \quad x^2 - 2x + 1 \quad = \quad 4 \cdot 1 + (-3) \cdot (x+1) + 1 \cdot (x^2 + x)$$

und somit $\Phi_{\mathscr{C}}(f) = (4, -3, 1)$.

(v) Sei $K = \mathbb{C}$, $V = \mathbb{C}^2$ und $v = (3+i, 2-6i)$. Sei $\mathscr{E}_2 = (e_1, e_2)$ die Basis der Einheitsvektoren. Die Gleichung

$$v \quad = \quad \begin{pmatrix} 3+i \\ 2-6i \end{pmatrix} \quad = \quad (3+i) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (2-6i) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

zeigt, dass $\Phi_{\mathscr{B}}(v) = (3+i, 2-6i)$ ist.

(vi) Diesmal betrachten wir $V = \mathbb{C}^2$ als $\mathbb{R}$-Vektorraum, es sei also $K = \mathbb{R}$. Dieser Vektorraum besitzt die geordnete Basis $\mathscr{B} = (e_1, ie_1, e_2, ie_2)$. Wieder sei $v = (3+i, 2-6i)$. Weil $\mathbb{C}^2$ als $\mathbb{R}$-Vektorraum vierdimensional ist, hat v diesmal vier Koordinaten, die aber in $\mathbb{R}$ liegen. Die Gleichung

$$v \quad = \quad \begin{pmatrix} 3+i \\ 2-6i \end{pmatrix} \quad = \quad 3 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} i \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + (-6) \cdot \begin{pmatrix} 0 \\ i \end{pmatrix}$$

zeigt, dass diese durch $\Phi_{\mathscr{B}}(v) = (3, 1, 2, -6)$ gegeben sind.

Als nächstes untersuchen wir nun den Zusammenhang zwischen Matrizen und linearen Abbildungen. Satz (11.2) kann verwendet werden, um jeder Matrix $A \in \mathscr{M}_{m\times n,K}$ eine lineare Abbildung zwischen Vektorräumen V, W der Dimension n und m zuzuordnen.

(11.5) Definition Seien V, W endlich-dimensionale K-Vektorräume und $\mathscr{A} = (v_1, ..., v_n)$, $\mathscr{B} = (w_1, ..., w_m)$ geordnete Basen von V bzw. W. Ferner sei $A = (a_{ij})$ eine Matrix aus $\mathscr{M}_{m\times n,K}$, mit $n = \dim V$ und $m = \dim W$. Dann gibt es nach Satz (11.2) eine eindeutig bestimmte lineare Abbildung

$$\phi : V \longrightarrow W \qquad \text{mit} \qquad \phi(v_j) = \sum_{i=1}^{m} a_{ij} w_i \quad \text{für} \quad 1 \le j \le n.$$

Wir bezeichnen diese Abbildung ϕ mit $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)$ und nennen sie die ***lineare Abbildung zur Matrix*** A bezüglich der Basen $\mathscr{A}$ und $\mathscr{B}$.

Auch diese Definition illustrieren wir durch zwei Beispiele.

(i) Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$, $W = \mathbb{R}^3$, $\mathscr{E}_2 = (e_1, e_2)$ und $\mathscr{E}_3 = (e_1, e_2, e_3)$. Wir suchen die lineare Abbildung $\phi = \mathscr{L}_{\mathscr{E}_3}^{\mathscr{E}_2}(A)$ zur Matrix

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

Nach Definition erfüllt ϕ die Gleichungen $\phi(e_1) = 1\cdot e_1 + 3\cdot e_2 + 5\cdot e_3 = (1, 3, 5)$ und $\phi(e_2) = 2\cdot e_1 + 4\cdot e_2 + 6\cdot e_3 = (2, 4, 6)$. Damit kann das Bild von ϕ auch für jeden beliebigen Vektor angegeben werden, denn auf Grund der Linearität von ϕ gilt

$$\phi \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \quad = \quad \phi \left(x_1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) \quad = \quad x_1 \cdot \phi \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \cdot \phi \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$= \quad x_1 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} \quad = \quad \begin{pmatrix} x_1 + 2x_2 \\ 3x_1 + 4x_2 \\ 5x_1 + 6x_2 \end{pmatrix}.$$

(ii) Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$, $W = \mathbb{R}^3$ und A wie in Beispiel (i) definiert. Diesmal aber betrachten wir die Basen $\mathscr{A} = (v_1, v_2)$ und $\mathscr{B} = (w_1, w_2, w_3)$ bestehend aus den Vektoren

$$v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ v_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix},\ w_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},\ w_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},\ w_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Sei $\psi = \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)$. Wieder können an den beiden Spalten von A die Bilder der Basisvektoren abgelesen werden: Nach Definition gilt

$$\psi(v_1) \quad = \quad 1 \cdot w_1 + 3 \cdot w_2 + 5 \cdot w_3 \quad = \quad 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 5 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 8 \\ 6 \\ 4 \end{pmatrix}$$

und

$$\psi(v_2) \quad = \quad 2 \cdot w_1 + 4 \cdot w_2 + 6 \cdot w_3 \quad = \quad 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 4 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + 6 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 10 \\ 8 \\ 6 \end{pmatrix}.$$

Mit diesen Informationen können wir auch die Bilder $\psi(e_1)$ und $\psi(e_2)$ der Einheitsvektoren ausrechnen. Aus $e_1 = \frac{1}{2}v_1 + \frac{1}{2}v_2$ folgt

$$\psi(e_1) \quad = \quad \psi(\tfrac{1}{2}v_1 + \tfrac{1}{2}v_2) \quad = \quad \tfrac{1}{2}\psi(v_1) + \tfrac{1}{2}\psi(v_2) \quad = \quad \tfrac{1}{2} \cdot \begin{pmatrix} 8 \\ 6 \\ 4 \end{pmatrix} + \tfrac{1}{2} \cdot \begin{pmatrix} 10 \\ 8 \\ 6 \end{pmatrix} \quad = \quad \begin{pmatrix} 9 \\ 7 \\ 5 \end{pmatrix},$$

und mit $e_2 = \frac{1}{2}v_1 + (-\frac{1}{2})v_2$ erhalten wir ebenso

$$\psi(e_2) \quad = \quad \psi(\tfrac{1}{2}v_1 + (-\tfrac{1}{2})v_2) \quad = \quad \tfrac{1}{2}\psi(v_1) + (-\tfrac{1}{2})\psi(v_2) \quad = \quad \tfrac{1}{2} \cdot \begin{pmatrix} 8 \\ 6 \\ 4 \end{pmatrix} + (-\tfrac{1}{2}) \cdot \begin{pmatrix} 10 \\ 8 \\ 6 \end{pmatrix} \quad = \quad \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}.$$

Damit können wir nun wieder das Bild jedes beliebigen Vektors angeben.

$$\begin{aligned} \psi\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \quad &= \quad \psi\left(x_1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \quad = \quad x_1 \cdot \psi\begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \cdot \psi\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \quad x_1 \cdot \begin{pmatrix} 9 \\ 7 \\ 5 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} \quad = \quad \begin{pmatrix} 9x_1 - x_2 \\ 7x_1 - x_2 \\ 5x_1 - x_2 \end{pmatrix}. \end{aligned}$$

Man sieht, dass $\phi \neq \psi$ ist, obwohl unter (i) und (ii) dieselbe Matrix A verwendet wurde.

Sind V und W endlich-dimensionale K-Vektorräume mit geordneten Basen $\mathscr{A}$ und $\mathscr{B}$, so kann jeder Matrix $A \in \mathscr{M}_{m\times n,K}$ also eine lineare Abbildung $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A) : V \to W$ zugeordnet werdne, sofern $n = \dim V$ und $m = \dim W$ ist. Nun sehen wir uns an, wie man umgekehrt jeder linearen Abbildung $V \to W$ eine Matrix zuordnet.

(11.6) Definition Seien V, W endlich-dimensionale K-Vektorräume und $\mathscr{A} = (v_1, ..., v_n)$, $\mathscr{B} = (w_1, ..., w_m)$ geordnete Basen von V bzw. W. Sei $\phi : V \to W$ eine lineare Abbildung. Für jedes $j \in \{1, ..., n\}$ stellen wir $\phi(v_j)$ als Linearkombination von $\mathscr{B}$ dar; es gilt

$$\phi(v_j) \quad = \quad \sum_{i=1}^{m} a_{ij} w_i \qquad 1 \leq j \leq n$$

mit eindeutig bestimmten Koeffizienten $a_{ij} \in K$. Wir nennen $A = (a_{ij}) \in \mathscr{M}_{m\times n,K}$ die ***Darstellungsmatrix*** von ϕ bezüglich der Basen $\mathscr{A}, \mathscr{B}$ und bezeichnen sie mit $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$.

Die Darstellungsmatrix $\mathscr{M}_{m\times n,K}$ kann ausgerechnet werden, indem man für jeden Basisvektor v_j aus $\mathscr{A}$ das Bild $\phi(v_j)$ als Linearkombination von $\mathscr{B}$ schreibt und die entsprechenden Koeffizienten als Spalten in die Darstellungsmatrix einträgt. Wieder betrachten wir zwei konkrete Beispiele.

(i) Es seien $K = \mathbb{R}$ und $V = W = \mathscr{M}_{2,\mathbb{R}}$, der $\mathbb{R}$-Vektorraum der reellen 2×2-Matrizen. Wir betrachten die geordneten Basen $\mathscr{A} = \mathscr{B} = (B_{11}, B_{12}, B_{21}, B_{22})$ bestehend aus den Basismatrizen und die Abbildung $\phi : V \to W$ gegeben durch

$$X \mapsto \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} X \qquad \text{für} \quad X \in \mathscr{M}_{2,\mathbb{R}}.$$

Es ist leicht zu überprüfen, dass ϕ eine lineare Abbildung ist. Die Bilder der Elemente von $\mathscr{A}$ sind nun gegeben durch

$$\begin{aligned}
\phi(B_{11}) &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 0 \end{pmatrix} = 1 \cdot B_{11} + 0 \cdot B_{12} + 3 \cdot B_{21} + 0 \cdot B_{22} \\
\phi(B_{12}) &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix} = 0 \cdot B_{11} + 1 \cdot B_{12} + 0 \cdot B_{21} + 3 \cdot B_{22} \\
\phi(B_{21}) &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix} = 2 \cdot B_{11} + 0 \cdot B_{12} + 4 \cdot B_{21} + 0 \cdot B_{22} \\
\phi(B_{22}) &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 4 \end{pmatrix} = 0 \cdot B_{11} + 2 \cdot B_{12} + 0 \cdot B_{21} + 4 \cdot B_{22}.
\end{aligned}$$

Jede Rechnung liefert eine Spalte der Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$. Insgesamt ist die gesuchte Matrix gegeben durch

$$\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi) \quad = \quad \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 0 & 4 & 0 \\ 0 & 3 & 0 & 4 \end{pmatrix}.$$

(ii) Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$, $W = \mathbb{R}^3$ und $\phi_A : V \to W$, $v \mapsto Av$ die Matrix-Vektor-Multiplikation mit der Matrix

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

Unser Ziel ist die Bestimmung der Darstellungsmatrix $\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$ bezüglich der geordneten Basen

$$\mathcal{A} = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) \qquad \text{und} \qquad \mathcal{B} = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right).$$

Wir rechnen die Bilder der Elemente von $\mathcal{A}$ aus und stellen sie als Linearkombination von $\mathcal{B}$ dar.

$$\phi_A\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) \quad = \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 3 \\ 7 \\ 11 \end{pmatrix} \quad = \quad (-4) \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + (-4) \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 11 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\phi_A\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) \quad = \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad = \quad \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} \quad = \quad 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Wieder liefert jede Rechnung eine Spalte von $\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$. Insgesamt ist die gesuchte Matrix gegeben durch

$$\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi) \quad = \quad \begin{pmatrix} -4 & 0 \\ -4 & 0 \\ 11 & -1 \end{pmatrix}.$$

Der folgende Satz zeigt, dass man mit Hilfe der Darstellungsmatrix $\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$ und den $\mathcal{A}$-Koordinaten eines Vektors $v \in V$ die $\mathcal{B}$-Koordinaten des Bildvektors $\phi(v) \in W$ ausrechnen kann.

(11.7) Satz Seien die Bezeichungen wie in der Definition gewählt. Dann gilt

$$\Phi_{\mathcal{B}}(\phi(v)) \quad = \quad \mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi) \Phi_{\mathcal{A}}(v) \qquad \text{für alle} \quad v \in V.$$

Beweis: Sei $A = \mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$ und $\phi_A : K^n \to K^m$ die Abbildung $v \mapsto Av$ gegeben durch das Matrix-Vektor-Produkt. Zum Beweis der Gleichung $\Phi_{\mathcal{B}} \circ \phi = \phi_A \circ \Phi_{\mathcal{A}}$ genügt es auf Grund des Existenz- und Eindeutigkeitssatzes zu zeigen, dass

$$(\Phi_{\mathcal{B}} \circ \phi)(v_j) \quad = \quad (\phi_A \circ \Phi_{\mathcal{A}})(v_j) \qquad \text{für} \quad 1 \leq j \leq n$$

erfüllt ist. Für die linke Seite der Gleichung gilt nach Definition

$$(\Phi_{\mathcal{B}} \circ \phi)(v_j) \quad = \quad \Phi_{\mathcal{B}}\left(\sum_{i=1}^{m} a_{ij} w_i \right) \quad = \quad \sum_{i=1}^{m} a_{ij} \Phi_{\mathcal{B}}(w_i) \quad = \quad \sum_{i=1}^{m} a_{ij} e_i \quad = \quad (a_{1j}, \ldots, a_{mj}).$$

Für die rechte Seite erhalten wir

$$(\phi_A \circ \Phi_{\mathscr{A}})(v_j) \quad = \quad \phi_A(e_j) \quad = \quad (a_{1j}, ..., a_{mj}) \quad ,$$

denn nach Propostion (10.10) sind die Bilder der Einheitsvektoren unter ϕ_A genau die Spalten der Matrix A. Damit ist gezeigt, dass die beiden Abbildungen übereinstimmen. □

Auch diesen Satz illustrieren wir durch eine kurze Rechnung. Wieder seien $V = \mathbb{R}^2$, $W = \mathbb{R}^3$ mit den geordneten Basen $\mathscr{A}$ und $\mathscr{B}$ aus dem letzten Beispiel vorgegeben, und wir betrachten dieselbe lineare Abbildung $\phi_A : V \to W$. Wir berechnen das Bild des Vektors $v = (5,3)$ auf zwei verschiedene Arten: einerseits durch direktes Einsetzen in die Definition, andererseits mit über den Koordinatenvektor $\Phi_{\mathscr{A}}(v)$ und die Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi_A)$. Das direkte Einsetzen ergibt

$$\phi_A(v) \quad = \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \quad = \quad \begin{pmatrix} 11 \\ 27 \\ 43 \end{pmatrix}.$$

Der Koordinatenvektor von v bezüglich $\mathscr{A}$ ist gegeben durch $\Phi_{\mathscr{A}} = (4,1)$, denn es gilt $(5,3) = 4 \cdot (1,1) + 1 \cdot (1,-1)$. Mit Satz (11.7) erhalten wir

$$\Phi_{\mathscr{B}}(\phi_A(v)) \quad = \quad \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi_A)\Phi_{\mathscr{A}}(v) \quad = \quad \begin{pmatrix} -4 & 0 \\ -4 & 0 \\ 11 & -1 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \end{pmatrix} \quad = \quad \begin{pmatrix} -16 \\ -16 \\ 43 \end{pmatrix}.$$

Aus den $\mathscr{B}$-Koordinaten von $\phi_A(v)$ können wir den Vektor $\phi_A(v)$ zurückgewinnen: Es ist

$$\phi_A(v) \quad = \quad (-16) \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + (-16) \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 43 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 11 \\ 27 \\ 43 \end{pmatrix}$$

Beide Rechenwege führen also zum gleichen Ergebnis.

(11.8) Proposition Seien $m, n \in \mathbb{N}$, $A \in \mathscr{M}_{m \times n, K}$ und $\phi_A : K^n \to K^m$ die lineare Abbildung gegeben durch $\phi_A(v) = Av$ für alle $v \in K^n$. Dann gilt

$$\mathscr{M}_{\mathscr{E}_m}^{\mathscr{E}_n}(\phi_A) \quad = \quad A.$$

Beweis: Für $1 \leq j \leq n$ gilt nach Satz (11.7) jeweils

$$\mathscr{M}_{\mathscr{E}_m}^{\mathscr{E}_n}(\phi_A)e_j \quad = \quad \mathscr{M}_{\mathscr{E}_m}^{\mathscr{E}_n}(\phi_A)\Phi_{\mathscr{E}_n}(e_j) \quad = \quad \Phi_{\mathscr{E}_m}(\phi_A(e_j)) \quad = \quad \phi_A(e_j) \quad = \quad Ae_j.$$

Dies zeigt, dass die j-te Spalte von $\mathscr{M}_{\mathscr{E}_m}^{\mathscr{E}_n}(\phi_A)$ mit der j-ten Spalte von A übereinstimmt, für $1 \leq j \leq n$. □

Durch den folgenden Satz wird nun der entscheidende Zusammenhang zwischen Matrizen und linearen Abbildungen hergestellt.

(11.9) Satz Seien V, W endlich-dimensionale K-Vektorräume und $\mathscr{A}, \mathscr{B}$ geordnete Basen von V bzw. W. Dann sind durch die beiden Abbildungen

$$\mathscr{M}_{m \times n, K} \to \mathrm{Hom}_K(V, W) \, , \, A \mapsto \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A) \qquad , \qquad \mathrm{Hom}_K(V, W) \to \mathscr{M}_{m \times n, K} \, , \, \phi \mapsto \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$$

zueinander inverse Isomorphismen von K-Vektorräumen definiert.

Beweis: Sei $\mathscr{A} = (v_1, ..., v_n)$ und $\mathscr{B} = (w_1, ..., w_m)$. Zunächst beweisen wir, dass $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}$ eine lineare Abbildung ist. Seien dazu $A, B \in \mathscr{M}_{m\times n,K}$ und $\lambda \in K$ beliebig vorgegeben, $A = (a_{ij})$, $B = (b_{ij})$. Für $1 \leq j \leq n$ gilt

$$\begin{aligned}\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A+B)(v_j) &= \sum_{i=1}^{m}(a_{ij}+b_{ij})w_i = \sum_{i=1}^{m}a_{ij}w_i + \sum_{i=1}^{m}b_{ij}w_i \\ &= \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)(v_j) + \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(B)(v_j) = \left(\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A) + \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(B)\right)(v_j)\end{aligned}$$

und

$$\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(\lambda A)(v_j) = \sum_{i=1}^{m}(\lambda a_{ij})w_i = \lambda\sum_{i=1}^{m}a_{ij}w_i = \lambda\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)(v_j) = (\lambda\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A))(v_j).$$

Damit sind die Gleichungen $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A+B) = \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A) + \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(B)$ und $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(\lambda A) = \lambda\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}$ bewiesen, und $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}$ ist tatsächlich eine lineare Abbildung. Um zu zeigen, dass die Abbildungen $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}$ und $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}$ zueinander invers sind, müssen die Gleichungen

$$\mathscr{M}_{\mathscr{B}}^{\mathscr{A}} \circ \mathscr{L}_{\mathscr{B}}^{\mathscr{A}} = \mathrm{id}_{\mathscr{M}_{m\times n,K}} \qquad \text{und} \qquad \mathscr{L}_{\mathscr{B}}^{\mathscr{A}} \circ \mathscr{M}_{\mathscr{B}}^{\mathscr{A}} = \mathrm{id}_{\mathrm{Hom}_K(V,W)}$$

überprüft werden. Zum Beweis der ersten Gleichung sei $A = (a_{ij}) \in \mathscr{M}_{m\times n,K}$ vorgegeben und $\phi = \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)$. Nach Definition von $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)$ gilt

$$\phi(v_j) = \sum_{i=1}^{m}a_{ij}w_i \qquad \text{für} \quad 1 \leq j \leq n.$$

Setzen wir $B = (b_{ij}) = \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$, dann gilt nach Definition der Darstellungsmatrix auch $\phi(v_j) = \sum_{i=1}^{m} b_{ij}w_i$ für $1 \leq j \leq n$. Weil $\mathscr{B}$ eine Basis und insbesondere linear unabhängig ist, folgt für $1 \leq j \leq n$ aus $\sum_{i=1}^{m} a_{ij}w_i = \sum_{i=1}^{m} b_{ij}w_i$ jeweils $a_{ij} = b_{ij}$ für $1 \leq i \leq m$, und damit $A = B$. Wir erhalten insgesamt

$$(\mathscr{M}_{\mathscr{B}}^{\mathscr{A}} \circ \mathscr{L}_{\mathscr{B}}^{\mathscr{A}})(A) = \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi) = B = A = \mathrm{id}_{\mathscr{M}_{m\times n,K}}(A).$$

Damit ist die erste Gleichung bewiesen.

Zum Beweis der zweiten Gleichung sei $\phi \in \mathrm{Hom}_K(V,W)$ vorgegeben und $A = \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$ mit $A = (a_{ij})$. Dann gilt

$$\phi(v_j) = \sum_{i=1}^{m}a_{ij}w_i = \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)(v_j) \qquad \text{für} \quad 1 \leq j \leq n.$$

Diese Gleichungen zeigen, dass die linearen Abbildungen ϕ und $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A)$ auf der Basis $\mathscr{A}$ von V übereinstimmen. Nach dem Existenz- und Eindeutigkeitssatz sind sie damit identisch. Es gilt also

$$(\mathscr{L}_{\mathscr{B}}^{\mathscr{A}} \circ \mathscr{M}_{\mathscr{B}}^{\mathscr{A}})(\phi) = \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)) = \mathscr{L}_{\mathscr{B}}^{\mathscr{A}}(A) = \phi = \mathrm{id}_{\mathrm{Hom}_K(V,W)}(\phi) \quad ,$$

also $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}} \circ \mathscr{M}_{\mathscr{B}}^{\mathscr{A}} = \mathrm{id}_{\mathrm{Hom}_K(V,W)}$. Insgesamt haben wir gezeigt, dass die Abbildungen $\mathscr{L}_{\mathscr{B}}^{\mathscr{A}}$ und $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}$ zueinander invers sind, damit insbesondere Umkehrabbildungen besitzen und folglich bijektiv sind. Als Umkehrabbildung einer linearen Abbildung ist $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}$ ebenfalls linear. □

(11.10) Folgerung Seien V, W endlich-dimensionale K-Vektorräume. Dann gilt

$$\dim \operatorname{Hom}_K(V,W) \quad = \quad (\dim V)(\dim W).$$

Beweis: Sei $m = \dim W$ und $n = \dim V$. Nach Satz (11.9) sind die K-Vektorräume $\operatorname{Hom}_K(V,W)$ und $\mathcal{M}_{m\times n,K}$ isomorph. Daraus folgt $\dim \operatorname{Hom}_K(V,W) = \dim \mathcal{M}_{m\times n,K} = mn$. □

(11.11) Lemma Sei V ein endlich-dimensionaler K-Vektorraum und $\mathcal{A}$ eine geordnete Basis von V. Dann gilt $\mathcal{M}_{\mathcal{A}}^{\mathcal{A}}(\mathrm{id}_V) = E^{(n)}$, d.h. die Darstellungsmatrix der identischen Abbildung ist die Einheitsmatrix.

Beweis: Sei $\mathcal{A} = (v_1, ..., v_n)$. Für $1 \le j \le n$ gilt nach Satz (11.7) dann jeweils

$$\mathcal{M}_{\mathcal{A}}^{\mathcal{A}}(\mathrm{id}_V)e_j \quad = \quad \mathcal{M}_{\mathcal{A}}^{\mathcal{A}}(\mathrm{id}_V)\Phi_{\mathcal{A}}(v_j) \quad = \quad \Phi_{\mathcal{A}}(\mathrm{id}_V(v_j)) \quad = \quad \Phi_{\mathcal{A}}(v_j) \quad = \quad e_j.$$

Die Spalten von $\mathcal{M}_{\mathcal{A}}^{\mathcal{A}}(\mathrm{id}_V)$ sind also gerade die Einheitsvektoren. Daraus folgt $\mathcal{M}_{\mathcal{A}}^{\mathcal{A}}(\mathrm{id}_V) = E^{(n)}$. □

Wir beweisen zwei wichtige Rechenregeln für Darstellungsmatrizen.

(11.12) Satz Seien U, V, W endlich-dimensionale K-Vektorräume mit geordneten Basen $\mathcal{A}$, $\mathcal{B}$ und $\mathcal{C}$. Seien $\phi : U \to V$ und $\psi : V \to W$ lineare Abbildungen. Dann gilt

$$\mathcal{M}_{\mathcal{C}}^{\mathcal{A}}(\psi \circ \phi) \quad = \quad \mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(\psi)\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi).$$

Das Matrixprodukt entspricht also der Komposition linearer Abbildungen.

Beweis: Sei $n = \dim U$ und $\mathcal{A} = (v_1, ..., v_n)$. Für $1 \le j \le n$ gilt nach Satz (11.9) dann einerseits

$$\mathcal{M}_{\mathcal{C}}^{\mathcal{A}}(\psi \circ \phi)e_j \quad = \quad \mathcal{M}_{\mathcal{C}}^{\mathcal{A}}(\psi \circ \phi)\Phi_{\mathcal{A}}(v_j) \quad = \quad \Phi_{\mathcal{C}}((\psi \circ \phi)(v_j)) \quad ,$$

andererseits aber auch

$$\mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(\psi)\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)e_j \quad = \quad \mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(\psi)\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)\Phi_{\mathcal{A}}(v_j) \quad = \quad \mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(\psi)\Phi_{\mathcal{B}}(\phi(v_j)) \quad =$$

$$\Phi_{\mathcal{C}}(\psi(\phi(v_j))) \quad = \quad \Phi_{\mathcal{C}}((\psi \circ \phi)(v_j)).$$

Also stimmt die j-te Spalte von $\mathcal{M}_{\mathcal{C}}^{\mathcal{A}}(\psi \circ \phi)$ mit der j-ten Spalte von $\mathcal{M}_{\mathcal{C}}^{\mathcal{B}}(\psi)\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$ überein, für $1 \le j \le n$. □

(11.13) Satz Seien V, W beides n-dimensionale K-Vektorräume mit geordneten Basen $\mathcal{A}$, $\mathcal{B}$. Eine lineare Abbildung $\phi : V \to W$ ist genau dann bijektiv, wenn die Darstellungsmatrix $\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)$ invertierbar ist, und in diesem Fall gilt

$$\mathcal{M}_{\mathcal{A}}^{\mathcal{B}}(\phi^{-1}) \quad = \quad \mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\phi)^{-1}.$$

Beweis: Sei $\mathscr{A} = (v_1, ..., v_n)$ und $\mathscr{B} = (w_1, ..., w_n)$. Setzen wir zunächst voraus, dass die Matrix $A = \mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\phi)$ invertierbar ist. Sei $B = A^{-1}$ die inverse Matrix und $\psi = \mathscr{L}^{\mathscr{B}}_{\mathscr{A}}(B)$. Weil die Abbildungen $\mathscr{L}^{\mathscr{B}}_{\mathscr{A}}$ und $\mathscr{M}^{\mathscr{B}}_{\mathscr{A}}$ nach Satz (11.9) zueinander invers sind, gilt $B = \mathscr{M}^{\mathscr{B}}_{\mathscr{A}}(\psi)$. Für $1 \leq j \leq n$ gilt dann einerseits

$$\mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\psi \circ \phi)e_j \quad = \quad \mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\psi \circ \phi)\Phi_{\mathscr{A}}(v_j) \quad = \quad \mathscr{M}^{\mathscr{B}}_{\mathscr{A}}(\psi)\mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\phi)\Phi_{\mathscr{A}}(v_j) \quad = \quad BA\Phi_{\mathscr{A}}(v_j) \quad = \quad \Phi_{\mathscr{A}}(v_j)$$

und andererseits

$$\mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\mathrm{id}_V)e_j \quad = \quad \mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\mathrm{id}_V)(\Phi_{\mathscr{A}}(v_j)) \quad = \quad \Phi_{\mathscr{A}}(\mathrm{id}_V(v_j)) \quad = \quad \Phi_{\mathscr{A}}(v_j).$$

Die j-te Spalte von $\mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\psi \circ \phi)$ stimmt also mit der j-ten Spalte von $\mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\mathrm{id}_V)$ überein. Also sind die beiden Matrizen gleich. Weil die Zuordnung $\mathscr{M}^{\mathscr{A}}_{\mathscr{A}}$ bijektiv ist, folgt $\psi \circ \phi = \mathrm{id}_V$. Nach dem gleichen Schema zeigt man $\phi \circ \psi = \mathrm{id}_W$. Damit ist die Bijektivität von ϕ bewiesen.

Gehen wir nun umgekehrt davon aus, dass ϕ bijektiv ist, und sei ψ die Umkehrabbildung. Mit Hilfe von Satz (11.11) erhalten wir

$$\mathscr{M}^{\mathscr{B}}_{\mathscr{A}}(\psi)\mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\phi) \quad = \quad \mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\psi \circ \phi) \quad = \quad \mathscr{M}^{\mathscr{A}}_{\mathscr{A}}(\mathrm{id}_V) \quad = \quad E^{(n)}$$

Dies zeigt die Invertierbarkeit von $\mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\phi)$ und beweist zugleich auch die Identität $\mathscr{M}^{\mathscr{B}}_{\mathscr{A}}(\phi^{-1}) = \mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\phi)^{-1}$. □

(11.14) Definition Seien V ein endlich-dimensionaler K-Vektorraum, und seien $\mathscr{A}, \mathscr{B}$ zwei geordnete Basen von V. Dann nennt man $\mathscr{T}^{\mathscr{A}}_{\mathscr{B}} = \mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\mathrm{id}_V)$ die ***Matrix des Basiswechsels*** von $\mathscr{A}$ nach $\mathscr{B}$ oder auch einfach eine ***Transformationsmatrix***.

Die wesentliche Eigenschaft der Transformationsmatrix $\mathscr{T}^{\mathscr{A}}_{\mathscr{B}}$ besteht darin, dass sie die $\mathscr{A}$-Koordinaten eines Vektors in $\mathscr{B}$-Koordinaten umrechnet.

(11.15) Proposition Seien Bezeichnungen wie in der Definition und $n = \dim V$.

(i) Für alle $v \in V$ gilt $\mathscr{T}^{\mathscr{A}}_{\mathscr{B}}\Phi_{\mathscr{A}}(v) = \Phi_{\mathscr{B}}(v)$.

(ii) Es gilt $\mathscr{T}^{\mathscr{A}}_{\mathscr{A}} = E^{(n)}$ und $\mathscr{T}^{\mathscr{B}}_{\mathscr{A}} = (\mathscr{T}^{\mathscr{A}}_{\mathscr{B}})^{-1}$.

Beweis: Für jeden Vektor $v \in V$ gilt nach Satz (11.7) jeweils

$$\mathscr{T}^{\mathscr{A}}_{\mathscr{B}}\Phi_{\mathscr{A}}(v) \quad = \quad \mathscr{M}^{\mathscr{A}}_{\mathscr{B}}(\mathrm{id}_V)\Phi_{\mathscr{A}}(v) \quad = \quad \Phi_{\mathscr{B}}(\mathrm{id}_V(v)) \quad = \quad \Phi_{\mathscr{B}}(v).$$

Die Gleichung $\mathscr{T}^{\mathscr{A}}_{\mathscr{A}} = E^{(n)}$ ist eine direkte Folgerung aus der Gleichung $\mathscr{T}^{\mathscr{A}}_{\mathscr{A}}\Phi_{\mathscr{A}}(v) = \Phi_{\mathscr{A}}(v)$, denn mit $v \in V$ durchläuft $\Phi_{\mathscr{A}}(v)$ alle Vektoren aus K^n. Schließlich liefert Satz (11.13) noch

$$(T^{\mathscr{A}}_{\mathscr{B}})^{-1} \quad = \quad (M^{\mathscr{A}}_{\mathscr{B}}(\mathrm{id}_V))^{-1} \quad = \quad M^{\mathscr{B}}_{\mathscr{A}}(\mathrm{id}_V^{-1}) \quad = \quad M^{\mathscr{B}}_{\mathscr{A}}(\mathrm{id}_V) \quad = \quad T^{\mathscr{B}}_{\mathscr{A}}.$$ □

Wir geben ein konkretes für die Bestimmung einer Transformationsmatrix und deren Verwendung an. Sei $K = \mathbb{R}$ und V der $\mathbb{R}$-Vektorraum der Polynomfunktionen vom Grad ≤ 2. Wir betrachten die geordneten Basen $\mathscr{A} = (f, g, h)$ und $\mathscr{B} = (u, v, w)$ bestehend aus den Elementen $f = 1$, $g = x$, $h = x^2$ sowie $u = 1$, $v = x + 1$, $w = x^2 + x$. Um die Transformationsmatrix $\mathscr{T}_{\mathscr{A}}^{\mathscr{B}}$ zu bestimmen, stellen wir die Elemente von $\mathscr{B}$ als Linearkombinationen der Elemente von $\mathscr{A}$ dar. Es gilt

$$\begin{aligned} u &= 1 = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 \\ v &= x + 1 = 1 \cdot 1 + 1 \cdot x + 0 \cdot x^2 \\ w &= x^2 + x = 0 \cdot 1 + 1 \cdot x + 1 \cdot x^2. \end{aligned}$$

Jede Rechnung liefert eine Spalte von $\mathscr{T}_{\mathscr{A}}^{\mathscr{B}}$; insgesamt erhalten wir

$$\mathscr{T}_{\mathscr{A}}^{\mathscr{B}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Der Algorithmus aus § 3 zur Invertierung von Matrizen liefert

$$\mathscr{T}_{\mathscr{B}}^{\mathscr{A}} = (\mathscr{T}_{\mathscr{A}}^{\mathscr{B}})^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Wir testen nun an einem Beispiel, dass mit $\mathscr{T}_{\mathscr{B}}^{\mathscr{A}}$ tatsächlich Koordinaten umgerechnet werden können, wie in Satz (11.7) angegeben. Das Element $r = x^2 - 2x + 1 \in V$ hat wegen $r = 1 \cdot 1 + (-2) \cdot x + 1 \cdot x^2$ die $\mathscr{A}$-Koordianten $\Phi_{\mathscr{A}}(r) = (1, -2, 1)$. Mit Satz (11.7) erhalten wir

$$\Phi_{\mathscr{B}}(r) = \mathscr{T}_{\mathscr{B}}^{\mathscr{A}} \Phi_{\mathscr{A}}(r) = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ -3 \\ 1 \end{pmatrix}.$$

Dies sind tatsächlich die $\mathscr{B}$-Koordinaten von r, denn es gilt $4 \cdot 1 + (-3) \cdot (x + 1) + 1 \cdot x^2 = x^2 - 2x + 1 = r$.

Zum Schluss sehen wir uns noch an, wie man Darstellungsmatrizen bezüglich unterschiedlicher Basen ineinander umrechnet.

(11.16) Satz *(Transformationsformel / Satz vom Basiswechsel)*

Seien V, W endlich-dimensionale K-Vektorräume, $\mathscr{A}, \mathscr{A}'$ zwei Basen von V und $\mathscr{B}, \mathscr{B}'$ zwei Basen von W. Für jede lineare Abbildung $\phi : V \to W$ gilt dann

$$\mathscr{M}_{\mathscr{B}'}^{\mathscr{A}'}(\phi) = \mathscr{T}_{\mathscr{B}'}^{\mathscr{B}} \, \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi) \, \mathscr{T}_{\mathscr{A}}^{\mathscr{A}'}.$$

Beweis: Die Gleichung erhält man direkt durch Anwendung von Satz (11.12). Es gilt

$$\begin{aligned} \mathscr{T}_{\mathscr{B}'}^{\mathscr{B}} \, \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi) \, \mathscr{T}_{\mathscr{A}}^{\mathscr{A}'} &= \mathscr{M}_{\mathscr{B}'}^{\mathscr{B}}(\mathrm{id}_W) \, \mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi) \, \mathscr{M}_{\mathscr{A}}^{\mathscr{A}'}(\mathrm{id}_V) = \mathscr{M}_{\mathscr{B}'}^{\mathscr{A}}(\mathrm{id}_W \circ \phi) \mathscr{M}_{\mathscr{A}}^{\mathscr{A}'}(\mathrm{id}_V) \\ &= \mathscr{M}_{\mathscr{B}'}^{\mathscr{A}'}(\mathrm{id}_W \circ \phi \circ \mathrm{id}_V) = \mathscr{M}_{\mathscr{B}'}^{\mathscr{A}'}(\phi). \end{aligned}$$

□

§ 12. Determinanten

Inhaltsübersicht

Jeder quadratischen Matrix $A \in \mathscr{M}_{n,K}$ kann auf natürliche Weise ein Wert $\det(A) \in K$ zugeordnet werden, die sog. *Determinante*, für die es eine ganze Reihe von Anwendungen gibt. Zum Beispiel lässt sich an der Determinante erkennen, ob A invertierbar ist. Auch die Inverse A^{-1} und die Lösungen von linearen Gleichungssystemen können durch die Determinante ausgedrückt werden. In der Geometrie dient die Determinante zur Berechnung von Flächeninhalten und Volumina.

Zunächst geben wir eine Charakterisierung der Determinantenfunktion durch drei Eigenschaften: Sie ist multilinear, alternierend und normiert. Um eine explizite Formel für die Determinante anzugeben, benötigen wir die sog. *symmetrischen Gruppen* S_n, deren Elemente als *Permutationen* bezeichnet werden. Jedes Element der S_n liefert einen Summanden in der Determinantenformel, mit einem Vorzeichen, dass durch das sog. *Signum* der Permutation festgelegt ist. Am effizientesten lässt sich die Determinante einer Matrix mit dem Gauß-Algorithmus (also durch Überführung in ZSF) berechnen. Auch die Blockgestalt von Matrizen kann zur Berechnung der Determinante genutzt werden. Mit dem Laplaceschen Entwicklungssatz kann die Berechnung der Determinante einer $n \times n$-Matrix auf kleinere Matrizen zurückgeführt werden.

Wichtige Begriffe und Sätze

- Eigenschaften *multilinear* und *alternierend* einer Abbildung
- Determinantenfunktionen und Determinante
- Permutation, symmetrische Gruppe S_n
- Signum, alternierende Gruppe A_n, Rechenregeln für das Signum
- Leibniz-Formel für Determinanten (mit der Sarrus-Regel als Spezialfall)
- Rechenregeln für Determinanten (Multiplikativität, Verhalten bei elementaren Zeilenumformungen, Formel für Dreiecksmatrizen, Invertierbarkeitskriterium)
- komplementäre Matrix
- Laplace'scher Entwicklungssatz und Cramersche Regel

(12.1) Definition Sei $n \in \mathbb{N}$, seien V, W zwei K-Vektorräume, und sei $\phi : V^n \to W$ eine Abbildung. Für jedes $k \in \{1, ..., n\}$ und jedes Tupel $\mathbf{v} = (v_1, ..., v_{k-1}, v_{k+1}, ..., v_n) \in V^{n-1}$ von Vektoren aus V können wir eine Abbildung $\phi_{\mathbf{v}}^{(k)} : V \to W$ definieren durch

$$\phi_{\mathbf{v}}^{(k)}(v) \quad = \quad \phi(v_1, ..., v_{k-1}, v_{k+1}, ..., v_n).$$

Man bezeichnet ϕ als ***multilinear***, wenn $\phi_{\mathbf{v}}^{(k)}$ für jedes $k \in \{1, ..., n\}$ und jedes $\mathbf{v} \in \mathbf{V^{n-1}}$ linear ist. Ferner bezeichnet man sie als ***alternierend***, wenn $\phi(v_1, ..., v_n) = 0_W$ gilt, sobald zwei der Vektoren $v_1, ..., v_n$ übereinstimmen.

In ausgeschriebener Form bedeutet die Multilinearität also, dass für jedes $k \in \{1, ..., n\}$, jedes $\lambda \in K$ und beliebige Vektoren $v_1, ..., v_{k-1}, v_k, v'_k, v_{k+1}, ..., v_n \in V$ jeweils die Gleichungen

$$\phi(v_1, ..., v_{k-1}, v_k + v'_k, v_{k+1}, ..., v_n) = \phi(v_1, ..., v_{k-1}, v_k, v_{k+1}, ..., v_n) + \phi(v_1, ..., v_{k-1}, v'_k, v_{k+1}, ..., v_n)$$

und $\phi(v_1, ..., v_{k-1}, \lambda v_k, v_{k+1}, ..., v_n) = \lambda\phi(v_1, ..., v_{k-1}, v_k, v_{k+1}, ..., v_n)$ erfüllt sind.

In diesem Abschnitt erweist es sich an vielen Stellen als praktisch, Matrizen als Tupel bestehend aus ihren Zeilenvektoren zu betrachten. Sei K ein Körper und $n \in \mathbb{N}$. Dann schreiben wir $(a_{1\bullet}, ..., a_{n\bullet})$ für die Matrix $A = (a_{ij}) \in \mathscr{M}_{n,K}$ mit den Zeilenvektoren $a_{k\bullet}$ für $1 \leq k \leq n$. Auf diese Weies wird $\mathscr{M}_{n,K}$ mit dem K-Vektorraum $(K^n)^n$ gleichgesetzt. Ist $v_k \in K^n$ ein beliebiger Vektor, dann schreiben wir $(a_{1\bullet}, ..., v_k, ..., a_{n\bullet})$ für die Matrix, die man erhält, wenn man die k-te Zeile $a_{k\bullet}$ durch den Vektor v_k ersetzt.

(12.2) Definition Eine Abbildung $d : \mathscr{M}_{n,K} \to K$ bezeichnet man als ***Determinantenfunktion***, wenn sie (aufgefasst als Abbildung auf $(K^n)^n$) multilinear und alternierend ist und außerdem $d(E^{(n)}) = 1$ gilt, wobei $E^{(n)} \in \mathscr{M}_{n,K}$ die Einheitsmatrix bezeichnet.

Wir zeigen anhand einiger konkreter Beispiele, wie die Eigenschaften einer Determinantenfunktion $d : \mathscr{M}_{3,\mathbb{R}} \to \mathbb{R}$ zu interpretieren sind. Die Multilinearität, angewendet auf die zweite Zeile der Matrizen, liefert beispielsweise

$$d\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} + d\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 7 & 8 & 9 \end{pmatrix} = d\begin{pmatrix} 1 & 2 & 3 \\ 4 & 6 & 7 \\ 7 & 8 & 9 \end{pmatrix}.$$

Ferner bedeutet die Multilinearität, dass man aus jeder einzelnen Zeile einen Faktor 2 „herausziehen“ kann, zum Beispiel in der Form

$$d\begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \\ 14 & 16 & 18 \end{pmatrix} = 2 \cdot d\begin{pmatrix} 1 & 2 & 3 \\ 8 & 10 & 12 \\ 14 & 16 & 18 \end{pmatrix} = 2 \cdot d\begin{pmatrix} 2 & 4 & 6 \\ 4 & 5 & 6 \\ 14 & 16 & 18 \end{pmatrix} = 2 \cdot d\begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \\ 7 & 8 & 9 \end{pmatrix}.$$

Diese Regel lässt sich natürlich auch mehrmals hintereinander anwenden. Man erhält so zum Beispiel

$$d\begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \\ 14 & 16 & 18 \end{pmatrix} = 2 \cdot d\begin{pmatrix} 1 & 2 & 3 \\ 8 & 10 & 12 \\ 14 & 16 & 18 \end{pmatrix} = 4 \cdot d\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 14 & 16 & 18 \end{pmatrix} = 8 \cdot d\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Allgemein gilt für eine beliebige quadratische Matrix $A \in \mathscr{M}_{n,K}$ und ein beliebiges $\lambda \in K$ jeweils die Gleichung $d(\lambda A) = \lambda^n d(A)$. Konkrete Beispiele für die Anwendung der anderen beiden Eigenschaften einer Determinantenfunktion sind zum Beispiel

$$d\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = 0 \quad \text{und} \quad d\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1.$$

Unser Hauptziel in diesem Abschnitt ist der Nachweis, dass für jeden Körper K und jedes $n \in \mathbb{N}$ genau eine Determinantenfunktion auf $\mathscr{M}_{n,K}$ existiert. Für den Nachweis der Existenz benötigen wir als algebraisches Hilfsmittel die symmetrischen Gruppen.

(12.3) Proposition Für jedes $n \in \mathbb{N}$ sei $M_n = \{1, ..., n\}$ die Menge der Zahlen von 1 bis n. Dann bilden die bijektiven Abbildungen $\sigma : M_n \to M_n$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe. Wir nennen sie die ***symmetrische Gruppe*** in n Elementen und bezeichnen sie mit S_n.

Beweis: Zunächst beweisen wir das Assoziativgesetz. Für alle $\rho, \sigma, \tau \in S_n$ und alle $x \in M_n$ gilt

$$((\rho \circ \sigma) \circ \tau)(x) \quad = \quad (\rho \circ \sigma)(\tau(x)) \quad = \quad \rho(\sigma(\tau(x))) \quad = \quad \rho((\sigma \circ \tau)(x)) \quad = \quad (\rho \circ (\sigma \circ \tau))(x)$$

und somit $(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)$. Damit ist die Assoziativität nachwiesen. Die identische Abbildung $\mathrm{id} \in S_n$ gegeben durch $\mathrm{id}(x) = x$ für alle $x \in M_n$ ist in $(S_n, \circ)$ das Neutralelement, denn für alle $\sigma \in S_n$ und alle $x \in M_n$ gilt

$$(\sigma \circ \mathrm{id})(x) \quad = \quad \sigma(\mathrm{id}(x)) \quad = \quad \sigma(x) \quad = \quad \mathrm{id}(\sigma(x)) \quad = \quad (\mathrm{id} \circ \sigma)(x)$$

also $\sigma \circ \mathrm{id} = \mathrm{id} \circ \sigma$. Weil jedes $\sigma \in S_n$ bijektiv ist, existiert jeweils die Umkehrabbildung σ^{-1}. Diese ist ebenfalls bijektiv, also ein Element in S_n. Für alle $x \in M_n$ gilt nach Definition der Umkehrabbildung

$$(\sigma^{-1} \circ \sigma)(x) \quad = \quad \sigma^{-1}(\sigma(x)) \quad = \quad x \quad = \quad \mathrm{id}(x)$$

und somit $\sigma^{-1} \circ \sigma = \mathrm{id}$. Ebenso zeigt man $\sigma \circ \sigma^{-1} = \mathrm{id}$. Damit ist nachgewiesen, dass σ^{-1} in $(S_n, \circ)$ das zu σ inverse Element ist. Jedes Element in S_n hat also ein Inverses, damit ist $(S_n, \circ)$ eine Gruppe. □

Elemente in S_n können durch Wertetabellen dargestellt werden. Beispielsweise schreibt man

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

für das Element $\sigma \in S_4$, das durch $\sigma(1) = 1$, $\sigma(2) = 4$, $\sigma(3) = 2$ und $\sigma(4) = 3$ gegeben ist. Aus der Analysis einer Variablen ist bekannt, dass für jedes $n \in \mathbb{N}$ und beliebige Mengen A, B mit $|A| = |B| = n$ jeweils genau $n!$ bijektive Abbildungen $A \to B$ existieren. Also gilt auch $|S_n| = n!$ für alle $n \in \mathbb{N}$.

Die Verknüpfung $\sigma \circ \tau$ zweier Elemente $\sigma, \tau \in S_n$ kommt dadurch zu Stande, dass auf jedes $k \in M_n$ erst die Abbildung τ und dann die Abbildung σ angewendet wird. Ist beispielsweise

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \text{und} \qquad \tau \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad ,$$

dann gilt $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(2) = 4$ und $(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(3) = 2$. Ebenso erhält man $(\sigma \circ \tau)(3) = 3$ und $(\sigma \circ \tau)(4) = 1$. Insgesamt gilt also

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

Wir werden nun sehen, wie die symmetrische Gruppe S_n mit Determinantenfunktionen auf $\mathscr{M}_{n,K}$ zusammenhängt. Dazu bezeichnen wir mit $\mathrm{Abb}(M_n)$ die Menge aller (nicht notwendig bijektiven) Abbildungen $M_n \to M_n$. Aus dem ersten Semester wissen wir, dass für eine Abbildung $\sigma \in \mathrm{Abb}(M_n)$ die Eigenschaften injektiv, surjektiv und bijektiv äquivalent sind. Ein Element aus $\mathrm{Abb}(M_n)$, das nicht in S_n liegt, ist also weder injektiv noch surjektiv.

Sei nun $d : \mathscr{M}_{n,K} \to K$ eine Determinantenfunktion und $A = (a_{ij}) \in \mathscr{M}_{n,K}$. Mit $e_1, ..., e_n$ bezeichnen wir wie immer die Einheitsvektoren in K^n. Die Darstellung der Zeilenvektoren als Linearkombination der Einheitsvektoren liefert $a_{k\bullet} = \sum_{i=1}^{n} a_{ki} e_i$ für $1 \le k \le n$. Auf Grund der Multilinearität von d gilt

$$\begin{aligned} d(A) &= d(a_{1\bullet}, ..., a_{n\bullet}) = d\left(\sum_{i_1=1}^{n} a_{1i_1} e_{i_1}, a_{2\bullet}, ..., a_{n\bullet}\right) = \\ \sum_{i_1=1}^{n} a_{1i_1} d(e_{i_1}, a_{2\bullet}, ..., a_{n\bullet}) &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} a_{1i_1} a_{2i_2} d(e_{i_1}, e_{i_2}, a_{3_\bullet}, ..., a_{n\bullet}) = ... = \\ \sum_{i_1=1}^{n} ... \sum_{i_n=1}^{n} a_{1i_1} ... a_{ni_n} d(e_{i_1}, ..., e_{i_n}) &= \sum_{\sigma \in \mathrm{Abb}(M_n)} a_{1\sigma(1)} ... a_{n\sigma(n)} d(e_{\sigma(1)}, ..., e_{\sigma(n)}) \end{aligned}$$

Jedes Element $\sigma \in \mathrm{Abb}(M_n)$ mit $\sigma \notin S_n$ ist auf Grund unserer Vorbemerkung insbesondere nicht injektiv, es gibt also $i, j \in M_n$ mit $i \neq n$ und $\sigma(i) = \sigma(j)$. Weil die Funktion d alternierend ist, gilt dann $d(e_{\sigma(1)}, ..., e_{\sigma(n)}) = 0$. Somit verschwinden in der Summe sämtliche Summanden, die zu Abbildungen $\sigma \in \mathrm{Abb}(M_n) \setminus S_n$ gehören. Wir erhalten

$$d(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} ... a_{n\sigma(n)} d(e_{\sigma(1)}, ..., e_{\sigma(n)}).$$

Eine Matrix der Form $P_\sigma = (e_{\sigma(1)}, ..., e_{\sigma(n)})$ mit $\sigma \in S_n$ bezeichnet man als ***Permutationsmatrix***. Insbesondere ist $P_{\mathrm{id}} = E^{(n)}$ die Einheitsmatrix. Unserer Rechnung hat ergeben

(12.4) Proposition Sei $d : \mathscr{M}_{n,K} \to K$ eine Determinantenfunktion und $A = (a_{ij}) \in \mathscr{M}_{n,K}$.
Dann gilt

$$d(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} ... a_{n\sigma(n)} d(P_\sigma).$$

Nun zeigen wir noch, dass auch die Werte $d(P_\sigma)$ durch die Eigenschaften der Determinantenfunktion eindeutig festgelegt sind. Sei $n \in \mathbb{N}$, und seien $k, \ell \in M_n$ zwei verschiedene Zahlen. Dann ist die Abbildung $\sigma : M_n \to M_n$ gegeben durch

$$\sigma(x) = \begin{cases} \ell & \text{falls } x = k \\ k & \text{falls } x = \ell \\ x & \text{sonst} \end{cases}$$

bijektiv, liegt also in S_n. Man verwendet für dieses spezielle Element von S_n die Notation $(k \ \ \ell)$. Allgemein werden Elemente in S_n in dieser Form als ***Transpositionen*** bezeichnet. Jede Transposition τ hat die Eigenschaft $\tau \circ \tau = \mathrm{id}$, denn die Vertauschung von je zwei Elementen wird durch Wiederholung des Vorgangs wieder rückgängig gemacht. Es gilt also

$$\tau = \tau^{-1} \qquad \text{für jede Transposition } \tau \in S_n.$$

Wir bestimmen nun das Bild $d(P_\sigma)$ unter einer Determinantenfunktion d zunächst für den Fall, dass σ eine Transposition ist. Allgemein gilt

(12.5) Lemma Sei $d : \mathscr{M}_{n,K} \to K$ eine Determinantenfunktion, und seien $A, B \in \mathscr{M}_{n,K}$. Entsteht B aus A durch Vertauschung zweier Zeilen, dann gilt $d(B) = -d(A)$.

Beweis: Seien $k, \ell \in M_n$ die beiden Zeilenindizes mit der Eigenschaft, dass B aus A durch Vertauschung der k-ten mit der ℓ-ten Zeile entsteht, wobei $k < \ell$ ist. Weil die Determinantenfunktion multilinear und alternierend ist, gilt

$$\begin{aligned} d(A) + d(B) &= d(..., a_{k\bullet}, ..., a_{\ell\bullet}, ...) + d(..., a_{\ell\bullet}, ..., a_{k\bullet}, ...) = \\ d(..., a_{k\bullet}, ..., a_{k\bullet}, ...) &+ d(..., a_{k\bullet}, ..., a_{\ell\bullet}, ...) + d(..., a_{\ell\bullet}, ..., a_{k\bullet}, ...) + d(..., a_{\ell\bullet}, ..., a_{\ell\bullet}, ...) = \\ d(..., a_{k\bullet}, ..., a_{k\bullet} + a_{\ell\bullet}, ...) &+ d(..., a_{\ell\bullet}, ..., a_{k\bullet} + a_{\ell\bullet}, ...) = d(..., a_{k\bullet} + a_{\ell\bullet}, ..., a_{k\bullet} + a_{\ell\bullet}, ...) = 0. \end{aligned}$$

Daraus folgt $d(B) = -d(A)$ □

Die Permutationsmatrix $P_{(k\ \ell)}$ entsteht aus der Einheitsmatrix $E^{(n)}$ durch Vertauschung der k-ten und ℓ-ten Zeile. Nach Eigenschaft (iii) der Determinatenfunktionen gilt also $d(P_{(k\ \ell)}) = -d(E^{(n)}) = -1$. Als nächstes bestimmen wir $d(P_\sigma)$ für beliebige Elemente $\sigma \in S_n$. Dazu bemerken wir zunächst, dass jede Permutation aus Transpositionen zusammengesetzt werden kann.

(12.6) Proposition Jedes Element aus S_n ist darstellbar als Produkt von Transpositionen.

Beweis: Sei $\sigma \in S_n$ vorgegeben. Wir beweisen durch vollständige Induktion über $k \in \{0, ..., n\}$: Es gibt ein Produkt τ von Transpositionen, so dass $(\tau \circ \sigma)(i) = i$ für $1 \le i \le k$ erfüllt ist. Die Aussage für $k = n$ liefert dann $\tau \circ \sigma = \mathrm{id} \Leftrightarrow \sigma = \tau^{-1}$. Mit τ ist dann auch das Element $\sigma = \tau^{-1}$ ein Produkt von Transpositionen. Ist nämlich $\tau = \tau_1 \circ ... \circ \tau_\ell$ mit Transpositionen τ_i, dann erhalten wir für τ^{-1} die Produktdarstellung

$$\tau^{-1} = \tau_\ell^{-1} \circ ... \circ \tau_1^{-1} = \tau_\ell \circ ... \circ \tau_1.$$

Kommen wir nun zum Induktionsbeweis. Für $k = 0$ ist nichts zu zeigen. Sei nun $k \in \{0, ..., n-1\}$, und setzen wir die Aussage für k voraus. Dann gibt es ein Produkt τ von Transpositionen, so dass die Permutation $\tilde{\sigma} = \tau \circ \sigma$ für $1 \le i \le k$ die Gleichung $\tilde{\sigma}(i) = i$ erfüllt. Gilt nun $\tilde{\sigma}(k+1) = k+1$, dann erfüllt τ die gewünschte Aussage auch für $k+1$. Ansonsten setzen wir $\ell = \tilde{\sigma}(k+1)$; auf Grund der Injektivität von $\tilde{\sigma}$ und wegen $\tilde{\sigma}(i) = i$ für $1 \le i \le k$ und $\tilde{\sigma}(k+1) \ne k+1$ ist $\ell > k+1$. Für das Produkt $\tau' = (k+1\ \ \ell) \circ \tau$ von Transpositionen gilt dann

$$(\tau' \circ \sigma)(k+1) = ((k+1\ \ \ell) \circ \tau \circ \sigma)(k+1) = ((k+1\ \ \ell) \circ \tilde{\sigma})(k+1) = (k+1\ \ \ell)(\ell) = k+1 \quad ,$$

wodurch der Induktionsschritt abgeschlossen ist. □

Es ist nicht schwierig, für ein gegebenes Element $\sigma \in S_n$ eine Darstellungs als Produkt von Transpostionen explizit zu bestimmen. Die Vorgehensweise ist folgende: Zunächst sucht man ein $k \in M_n$ mit $\ell = \sigma(k) \ne k$ und ersetzt den Eintrag ℓ an der k-ten Stelle durch k. Dann sucht man die Stelle m mit $\sigma(m) = k$ und ersetzt den Eintrag k dort

durch ℓ. Bezeichnet man die so modifizierte Permutation, dann gilt $\sigma = (k\ \ \ell) \circ \sigma'$. Denn für jedes $x \notin \{k, \ell, m\}$ gilt offenbar $\sigma(x) = \sigma'(x)$, und somit stimmen σ und $(k\ \ \ell) \circ \sigma'$ in x ebenfalls überein. Für $x \in \{k, \ell, m\}$ überprüft man die Gleichung unmittelbar durch Einsetzen: Es gilt

$$((k\ \ \ell) \circ \sigma')(k) = (k\ \ \ell)(k) = \ell = \sigma(k) \qquad \text{und} \qquad ((k\ \ \ell) \circ \sigma')(m) = (k\ \ \ell)(\ell) = k = \sigma(m).$$

Ist $\ell \neq m$, dann folgt $\sigma(\ell) = \sigma'(\ell)$ nach Definition von σ', außerdem $\sigma(\ell) \notin \{k, \ell\}$ und somit $((k\ \ \ell) \circ \sigma')(\ell) = (k\ \ \ell)(\sigma(\ell)) = \sigma(\ell)$. Im Fall $\ell = m$ ist die Gleichung $((k\ \ \ell) \circ \sigma')(\ell) = \sigma(\ell)$ bereits überprüft. Die Permutation σ' besitzt nun wegen $\sigma'(k) = k$ ein Element mehr als σ, das auf sich selbst abgebildet wird. Die Berechnung wird nun mit σ' an Stelle von σ fortgesetzt. Nach endlich vielen Schritten wird σ auf diese Weise in die identische Abbildung id umgewandelt, und man erhält eine Darstellung von σ als Produkt von Transpositionen.

Wir demonstrieren die Vorgehensweise an einem konkreten Beispiel und betrachten das Element $\sigma \in S_7$ gegeben durch

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 1 & 2 & 3 & 6 \end{pmatrix}.$$

Es gilt dann

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 1 & 2 & 3 & 6 \end{pmatrix} \quad = \quad (1\ \ 5) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 7 & 5 & 2 & 3 & 6 \end{pmatrix}$$

$$= \quad (1\ \ 5) \circ (2\ \ 4) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 7 & 5 & 4 & 3 & 6 \end{pmatrix} \quad = \quad (1\ \ 5) \circ (2\ \ 4) \circ (3\ \ 7) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 4 & 7 & 6 \end{pmatrix} \quad =$$

$$(1\ \ 5) \circ (2\ \ 4) \circ (3\ \ 7) \circ (4\ \ 5) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 7 & 6 \end{pmatrix} \quad =$$

$$(1\ \ 5) \circ (2\ \ 4) \circ (3\ \ 7) \circ (4\ \ 5) \circ (6\ \ 7) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} \quad =$$

$$(1\ \ 5) \circ (2\ \ 4) \circ (3\ \ 7) \circ (4\ \ 5) \circ (6\ \ 7) \circ \mathrm{id} \quad = \quad (1\ \ 5) \circ (2\ \ 4) \circ (3\ \ 7) \circ (4\ \ 5) \circ (6\ \ 7).$$

(12.7) Definition Sei $\sigma \in S_n$ ein beliebiges Element. Eine zweielementige Teilmenge $\{i, j\}$ von M_n wird ***Fehlstand*** von σ genannt, wenn $i < j$, aber $\sigma(i) > \sigma(j)$ gilt. Ist $k \in \mathbb{N}_0$ die Anzahl der Fehlstände von σ, dann nennt man $\mathrm{sgn}(\sigma) = (-1)^k$ das ***Signum*** oder ***Vorzeichen*** der Permutation.

Wir bestimmen das Signum des Elements $\sigma \in S_4$ gegeben durch

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

durch Abzählen der Fehlstände. Die Menge $M_4 = \{1,2,3,4\}$ besitzt genau sechs zweielementige Teilmengen, nämlich

$$\{1,2\} \quad , \quad \{1,3\} \quad , \quad \{1,4\} \quad , \quad \{2,3\} \quad , \quad \{2,4\} \quad \text{und} \quad \{3,4\}.$$

Die Menge $\{1,2\}$ ist ein Fehlstand von σ, denn es gilt $1 < 2$, aber $\sigma(1) = 3 > 2 = \sigma(2)$. Dagegen ist $\{1,3\}$ kein Fehlstand, denn es ist $1 < 3$ und $\sigma(1) = 3 < 4 = \sigma(3)$. Geht man alle zweielementigen Teilmengen auf diese Weise der Reihe nach durch, so kommt man zu dem Ergebnis, dass insgesamt vier Fehlstände existieren, nämlich $\{1,4\}$, $\{1,4\}$, $\{2,4\}$ und $\{3,4\}$. Somit gilt $\operatorname{sgn}(\sigma) = (-1)^4 = 1$.

Das Beispiel zeigt, dass die Berechnung des Signums direkt anhand der Definition für großes n sehr mühsam wird. Wir leiten deshalb einige Rechenregeln her, mit denen sich das Signum schneller bestimmen lässt.

(12.8) Lemma Für jede Transposition τ gibt es ein Element $\sigma \in S_n$ mit $\tau = \sigma \circ (1\ \ 2) \circ \sigma^{-1}$.

Beweis: Sei $\tau = (k\ \ell)$ mit $k, \ell \in \{1, ..., n\}$ und $\sigma \in S_n$ ein beliebiges Element mit $\sigma \in S_n$ mit $\sigma(1) = k$ und $\sigma(2) = \ell$. Setzen wir $\tau' = \sigma \circ (1\ \ 2) \circ \sigma^{-1}$, dann ist $\tau = \tau'$ zu überprüfen. Zunächt gilt

$$\tau'(k) \quad = \quad (\sigma \circ (1\ \ 2) \circ \sigma^{-1})(k) \quad = \quad (\sigma \circ (1\ \ 2))(1) \quad = \quad \sigma(2) \quad = \quad \ell$$

und $\tau'(\ell) = (\sigma \circ (1\ \ 2) \circ \sigma^{-1})(\ell) = (\sigma \circ (1\ \ 2))(2) = \sigma(1) = k$. Ist $i \notin \{k, \ell\}$, dann ist $\sigma^{-1}(i) \notin \{1,2\}$, denn die Elemente 1 und 2 werden in die Menge $\{k, \ell\}$ abgebildet. Wir erhalten $(1\ \ 2)(\sigma^{-1}(i)) = \sigma^{-1}(i)$ und somit

$$\tau'(i) \quad = \quad (\sigma \circ (1\ \ 2) \circ \sigma^{-1})(i) \quad = \quad (\sigma \circ (1\ \ 2))(\sigma^{-1}(i)) \quad = \quad \sigma(\sigma^{-1}(i)) \quad = \quad i.$$

Insgesamt gilt $\tau(i) = \tau'(i)$ für $1 \le i \le n$, also $\tau = \tau'$. □

(12.9) Lemma Für jedes $\sigma \in S_n$ gilt die Produktformel $\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Beweis: Sei $\sigma \in S_n$ und m die Anzahl der Fehlstände von σ. Dann gilt

$$\prod_{i<j} (\sigma(j) - \sigma(i)) \quad = \quad \prod_{\substack{i<j \\ \sigma(j)>\sigma(i)}} (\sigma(j) - \sigma(i)) \cdot \prod_{\substack{i<j \\ \sigma(j)<\sigma(i)}} (\sigma(j) - \sigma(i)) \quad =$$

$$\prod_{\substack{i<j \\ \sigma(j)>\sigma(i)}} (\sigma(j) - \sigma(i)) \cdot (-1)^m \prod_{\substack{i<j \\ \sigma(j)<\sigma(i)}} |\sigma(j) - \sigma(i)| \quad = \quad (-1)^m \prod_{i<j} |\sigma(j) - \sigma(i)|$$

Sei $\mathcal{T}$ die Menge der zweielementigen Teilmengen von $\{1, ..., n\}$. Dann entsprechen die Paare (i,j) mit $i < j$ und $i, j \in \{1, ..., n\}$ bijektiv den Mengen in $\mathcal{T}$. Weil σ bijektiv ist, ist mit $\{i,j\} \in \mathcal{T}$ auch $\{\sigma(i), \sigma(j)\}$ eine zweielementige Menge, also in $\mathcal{T}$ enthalten. Die Zuordnung $\mathcal{T} \to \mathcal{T}$, $\{i,j\} \mapsto \{\sigma(i), \sigma(j)\}$ ist bijektiv, da durch $\{i,j\} \mapsto \{\sigma^{-1}(i), \sigma^{-1}(j)\}$ eine Umkehrabbildung gegeben ist; wir bezeichnen diese ebenfalls mit σ. Für jedes $S = \{i,j\} \in \mathcal{T}$ sei außerdem $r_S = |i - j| \in \mathbb{N}$. Wir erhalten nun

$$(-1)^m \prod_{i<j} |\sigma(j) - \sigma(i)| \quad = \quad (-1)^m \prod_{\{i,j\} \in \mathcal{T}} |\sigma(j) - \sigma(i)| \quad = \quad (-1)^m \prod_{S \in \mathcal{T}} r_{\sigma(S)} \quad =$$

$$(-1)^m \prod_{S \in \sigma(\mathcal{T})} r_S \quad = \quad (-1)^m \prod_{S \in \mathcal{T}} r_S \quad = \quad (-1)^m \prod_{i<j} |j - i| \quad = \quad (-1)^m \prod_{i<j} (j - i).$$

Insgesamt haben wir also gezeigt, dass

$$\prod_{i<j}(\sigma(j)-\sigma(i)) \quad = \quad (-1)^m \prod_{i<j}(j-i) \quad = \quad \operatorname{sgn}(\sigma)\prod_{i<j}(j-i) \qquad \text{erfüllt ist.} \qquad \square$$

(12.10) Proposition Für beliebige Elemente $\sigma, \tau \in S_n$ gilt $\operatorname{sgn}(\tau \circ \sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$.

Beweis: Auf Grund des vorhergehenden Lemmas ist $\operatorname{sgn}(\tau \circ \sigma)$ gegeben durch

$$\prod_{i<j}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{j-i} \quad = \quad \prod_{i<j}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}.$$

Das zweite Produkt stimmt mit $\operatorname{sgn}(\sigma)$ überein. Es genügt also zu zeigen, dass das erste Produkt gleich $\operatorname{sgn}(\tau)$ ist. Es gilt

$$\prod_{i<j}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \quad = \quad \prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \cdot \prod_{\substack{i<j \\ \sigma(i)>\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \quad =$$

$$\prod_{\substack{i<j \\ \sigma(i)<\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \cdot \prod_{\substack{i>j \\ \sigma(i)<\sigma(j)}}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \quad = \quad \prod_{\sigma(i)<\sigma(j)}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \quad ,$$

wobei wir beim zweiten „=“ lediglich die Rollen von i und j im zweiten Faktor vertauscht haben. Um das Produkt weiter zu vereinfachen, beweisen wir die Gleichung

$$\{(k,\ell) \mid 1 \le k < \ell \le n\} \quad = \quad \{(\sigma(i),\sigma(j)) \mid 1 \le i,j \le n\ ,\ \sigma(i)<\sigma(j)\}.$$

Der Beweis der Inklusion „$\supseteq$“ ist offensichtlich, denn das Paar (k,ℓ) mit $k=\sigma(i)$, $j=\sigma(\ell)$ erfüllt nach Definition die Bedingungen an die Elemente in der Menge links. Zum Nachweis von „$\subseteq$“ sei ein Paar (k,ℓ) in der Menge links vorgegeben. Sei $i=\sigma^{-1}(k)$ und $j=\sigma^{-1}(\ell)$. Dann gilt $\sigma(i)=k<\ell=\sigma(j)$, also ist $(k,\ell)=(\sigma(i),\sigma(j))$ ein Element der Menge rechts. Es folgt nun

$$\prod_{\sigma(i)<\sigma(j)}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \quad = \quad \prod_{k<\ell}\frac{\tau(\ell)-\tau(k)}{\ell-k} \quad = \quad \operatorname{sgn}(\tau). \qquad \square$$

(12.11) Folgerung Für jede Permutation $\sigma \in S_n$ gilt $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

Beweis: Da das Neutralelement id der Gruppe keine Fehlstände besitzt, gilt $\operatorname{sgn}(\mathrm{id}) = 1$. Aus

$$\operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma^{-1}) \quad = \quad \operatorname{sgn}(\sigma \circ \sigma^{-1}) \quad = \quad \operatorname{sgn}(\mathrm{id}) = 1$$

folgt dann die behauptete Gleichung. $\square$

(12.12) Satz

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

(ii) Ist σ als Produkt von r Transpositionen darstellbar, dann gilt $\operatorname{sgn}(\sigma) = (-1)^r$.

Beweis: zu (i) Die Transposition $(1\ \ 2)$ hat offenbar $\{1,2\}$ als einzigen Fehlstand, also gilt $\operatorname{sgn}((1\ \ 2)) = -1$. Für eine beliebige Transposition τ finden wir nach (12.8) immer ein $\sigma \in S_n$ mit $\tau = \sigma \circ (1\ \ 2) \circ \sigma^{-1}$. Es folgt $\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}((1\ \ 2))\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^2\operatorname{sgn}((1\ \ 2)) = -1$.

zu (ii) Ist $\sigma = \tau_1 \circ \ldots \circ \tau_r$ bestehend aus Transpositionen $\tau_1, \ldots, \tau_r$, dann folgt aus Teil (i) die Gleichung $\operatorname{sgn}(\sigma) = \prod_{i=1}^r \operatorname{sgn}(\tau_i) = \prod_{i=1}^r (-1) = (-1)^r$. □

Mit Hilfe dieses Satzes haben wir nun eine effiziente Methode für die Berechnung des Signums zur Verfügung. Wir betrachten noch einmal das Beispiel im Anschluss an Definition (12.7) Für das dort betrachtete Element $\sigma \in S_4$ gilt

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \quad = \quad (1\ \ 3) \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad = \quad (1\ \ 3) \circ (3\ \ 4).$$

Also ist σ als Produkt von zwei Transpositionen darstellbar. Mit Satz (12.12) (ii) erhalten wir $\operatorname{sgn}(\sigma) = (-1)^2 = 1$.

Nun sind wir auch in der Lage, die Determinante der Permutationsmatrizen direkt anzugeben.

(12.13) Folgerung Sei $d : \mathscr{M}_{n,K} \to K$ eine Determinantenfunktion. Dann gilt

$$d(P_\sigma) \quad = \quad \operatorname{sgn}(\sigma) \qquad \text{für alle} \quad \sigma \in S_n.$$

Beweis: Ist $\rho \in S_n$ und $\tau = (k\ \ \ell)$ eine Transposition, dann gilt $d(P_{\rho\circ\tau}) = -d(P_\rho)$ nach Lemma (12.5), denn die Matrix $P_{\rho\circ\tau}$ entsteht aus P_ρ durch Vertauschung k-te und ℓ-ten Zeile: Für $i \neq k, \ell$ ist die i-te Zeile von $P_{\rho\circ\tau}$ gegeben durch $e_{(\rho\circ\tau)(i)} = e_{\rho(i)}$, und die k-te und ℓ-te Zeile sind $e_{(\rho\circ\tau)(k)} = e_{\rho(\ell)}$ bzw. $e_{(\rho\circ\tau)(\ell)} = e_{\rho(k)}$.

Sei nun $\sigma \in S_n$ beliebig vorgegeben. Nach Proposition (12.6) gibt es ein $r \in \mathbb{N}_0$ und Transpositionen $\tau_1, \ldots, \tau_r \in S_n$, so dass $\sigma = \tau_1 \circ \ldots \circ \tau_r$ erfüllt ist. Aus Lemma (12.9) folgt daraus $\operatorname{sgn}(\sigma) = (-1)^r$. Wir beweisen die behauptete Gleichung nun durch vollständige Induktion über r. Im Fall $r = 0$ gilt $\sigma = \mathrm{id}$ und $d(P_\sigma) = d(E^{(n)}) = 1$ auf Grund der Bedingung (iii) für Determinantenfunktionen.

Sei nun $r > 1$, und setzen wir die Gleichung für Werte $< r$ voraus. Definieren wir das Element $\sigma' \in S_n$ durch $\sigma' = \tau_1 \circ \ldots \circ \tau_{r-1}$, dann gilt $\sigma = \sigma' \circ \tau_r$, außerdem $\operatorname{sgn}(\sigma') = (-1)^{r-1}$ und auf Grund unserer Vorüberlegung

$$d(P_\sigma) \quad = \quad d(P_{\sigma'\circ\tau_r}) \quad = \quad -d(P_{\sigma'}) \quad = \quad -(-1)^{r-1} \quad = \quad (-1)^r \quad = \quad \operatorname{sgn}(\sigma).$$ □

Setzen wir dieses Ergebnis in Proposition (12.4) ein, so erhalten wir

(12.14) Folgerung Sei $d : \mathscr{M}_{n,K} \to K$ eine Determinantenfunktion und $A = (a_{ij}) \in \mathscr{M}_{n,K}$. Dann gilt

$$d(A) \quad = \quad \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}.$$

Nach diesen Vorbereitungen können wir nun endlich definieren

(12.15) Definition Sei $A = (a_{ij})_{n \in \mathbb{N}} \in \mathscr{M}_{n,K}$. Dann nennen wir

$$\det(A) \quad = \quad \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)} \qquad \text{die } \textbf{\textit{Determinante}} \text{ der Matrix } A.$$

Der Summenausdruck in der Definition von $\det(A)$ wird auch die ***Leibniz-Formel*** für die Determinante genannt. Wir geben die Formel für die Werte $n = 1, 2, 3$ noch einmal explizit an. Für $n = 1$ ist $S_n = \{\mathrm{id}\}$. In diesem Fall besteht die Summe also nur aus einem einzigen Term. Es gilt $\det(A) = \operatorname{sgn}(\mathrm{id}) a_{1\mathrm{id}(1)} = a_{11}$, also zum Beispiel

$$\det\begin{pmatrix} 3 \end{pmatrix} \quad = \quad 3.$$

Im Fall $n = 2$ gilt $S_2 = \{\ \mathrm{id}, (1\ 2)\}$, und die Transposition $\tau = (1\ 2)$ hat nach

(12.12) ein negatives Signum. Damit erhalten wir $\det(A) = \operatorname{sgn}(\mathrm{id}) a_{1\mathrm{id}(1)} a_{2\mathrm{id}(2)} + \operatorname{sgn}(\tau) a_{1\tau(1)} a_{2\tau(2)} = a_{11}a_{22} - a_{21}a_{12}$. Beispielsweise ist

$$\det\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad = \quad 1 \cdot 4 - 2 \cdot 3 \quad = \quad 4 - 6 \quad = \quad -2.$$

Für $n = 3$ besteht S_3 bereits aus $3! = 6$ Elementen, es gilt $S_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$ mit den Elementen

$$\sigma_1 = (2\ 3) \circ (1\ 3) \ , \ \ \sigma_2 = (1\ 3) \circ (2\ 3) \ , \ \ \tau_1 = (1\ 3) \ , \ \ \tau_2 = (2\ 3) \quad \text{und} \quad \tau_3 = (1\ 2).$$

Zum Beweis genügt es zu überprüfen, dass diese sechs Elemente tatsächlich *verschiedene* Elemente von S_3 sind. Nach Satz (12.12) gilt $\operatorname{sgn}(\mathrm{id}) = \operatorname{sgn}(\sigma_1) = \operatorname{sgn}(\sigma_2) = 1$ und $\operatorname{sgn}(\tau_1) = \operatorname{sgn}(\tau_2) = \operatorname{sgn}(\tau_3) = -1$.

Mit den sechs Elemente der Gruppe S_3 können wir nun die Formel für die Determinante im Fall $n = 3$ aufstellen.

$$\begin{aligned} \det(A) \quad = \quad & a_{1\mathrm{id}(1)} a_{2\mathrm{id}(2)} a_{3\mathrm{id}(3)} + a_{1\sigma_1(1)} a_{2\sigma_1(2)} a_{3\sigma_1(3)} + a_{1\sigma_2(1)} a_{2\sigma_2(2)} a_{3\sigma_2(3)} \\ & - a_{1\tau_1(1)} a_{2\tau_1(2)} a_{3\tau_1(3)} - a_{1\tau_2(1)} a_{2\tau_2(2)} a_{3\tau_2(3)} - a_{1\tau_3(1)} a_{2\tau_3(2)} a_{3\tau_3(3)} \quad = \\ & a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}. \end{aligned}$$

Man bezeichnet diese Formel auch als ***Sarrus-Regel*** zur Berechnung der Determinante. Die drei positiven Summanden entsprechen im Zahlenschema

$$\begin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

den drei nebeneinanderliegenden Diagonalen von links oben nach rechts unten. Die drei negativen Summanden entsprechen den drei Diagonalen, die von links unten nach rechts oben verlaufen. Mit der Sarrus-Regel erhält man zum Beispiel

$$\begin{aligned}\det\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix} &= 1\cdot5\cdot9+2\cdot6\cdot7+3\cdot4\cdot8-7\cdot5\cdot3-8\cdot6\cdot1-9\cdot4\cdot2\\ &= 45+84+96-105-48-72 \quad = \quad 225-255 \quad = \quad 0.\end{aligned}$$

Zu beachten ist, dass ein Analogon der Sarrus-Regel für $n=4$ ***falsch*** ist. Die Leibniz-Formel für eine Matrix $A\in\mathscr{M}_{4,K}$ besteht aus $4!=24$ Summanden, wärend in der Sarrus-Regel nur acht Terme vorkommen würden.

Nun beweisen wir noch, dass durch die Leibniz-Formel tatsächlich eine Determinantenfunktion definiert ist. Dazu benötigen wir weitere Grundlagen über die symmetrische Gruppe S_n. Für jedes $n\in\mathbb{N}$ bilden die Permutationen mit positivem Signum die sogenannte ***alternierende Gruppe***

$$A_n \quad = \quad \{\sigma\in S_n \mid \operatorname{sgn}(\sigma)=1\}.$$

Die Gruppe S_n setzt sich zu gleichen Teilen aus Elementen mit positivem und negativem Signum zusammen. Genauer gilt

> **(12.16) Proposition** Sei $A_n=\{\sigma\in S_n \mid \operatorname{sgn}(\sigma)=1\}$ und $\tau\in S_n$ ein beliebiges Element mit $\operatorname{sgn}(\tau)=-1$. Dann ist durch $S_n=A_n\cup(A_n\circ\tau)$ mit $A_n\circ\tau=\{\sigma\circ\tau \mid \sigma\in A_n\}$ eine Darstellung von S_n als disjunkte Vereinigung gegeben. Zwischen A_n und $A_n\circ\tau$ ist durch $\sigma\mapsto\sigma\circ\tau$ eine Bijektion definiert.

Beweis: Zunächst beweisen wir die Gleichung $S_n=A_n\cup A_n\circ\tau$. Die Inklusion „$\supseteq$“ ist offensichtlich, denn beide Mengen rechts bestehen aus Elementen von S_n. Zum Nachweis von „$\subseteq$“ sei $\sigma\in S_n$ vorgegeben. Liegt σ in A_n, dann ist nichts zu zeigen. Im Fall $\operatorname{sgn}(\sigma)=-1$ liegt $\sigma\circ\tau^{-1}$ in A_n, denn es gilt $\operatorname{sgn}(\sigma\circ\tau^{-1})=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)^{-1}=(-1)(-1)^{-1}=1$. Also ist $\sigma=(\sigma\circ\tau^{-1})\circ\tau$ in $A_n\circ\tau$ enthalten.

Die Elemente in A_n haben positives Signum. Jedes Element in $A_n\circ\tau$ der Form $\sigma\circ\tau$ mit $\sigma\in A_n$ hat wegen $\operatorname{sgn}(\sigma\circ\tau)=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)=1\cdot(-1)=-1$ negatives Signum. Dies zeigt, dass die Mengen A_n und $A_n\circ\sigma$ disjunkt sind.

Die Abbildung $\sigma\mapsto\sigma\circ\tau$ zwischen A_n und $A_n\circ\sigma$ ist surjektiv, denn jedes Element in $A_n\circ\tau$ kann in der Form $\sigma\circ\tau$ mit $\sigma\in A_n$ geschrieben werden. Sind $\sigma_1,\sigma_2\in A_n$ mit $\sigma_1\circ\tau=\sigma_2\circ\tau$, dann folgt $\sigma_1\circ\tau\circ\tau^{-1}=\sigma_2\circ\tau\circ\tau^{-1}$ und damit $\sigma_1=\sigma_2$. Damit ist auch die Injektivität der Abbildung nachgewiesen. □

> **(12.17) Satz** Für jedes $n\in\mathbb{N}$ ist $\det:\mathscr{M}_{n,K}\to K$ eine Determinantenfunktion.

Beweis: Wir müssen überprüfen, dass die Abbildung det die drei Bedingungen aus Definition (12.2) erfüllt. Sei $k\in\{1,\ldots,n\}$, und seien $A,B\in\mathscr{M}_{n,K}$ zwei Matrizen, die in allen Zeilen mit Ausnahme der k-ten übereinstimmen. Sei

außerdem $C \in \mathscr{M}_{n,K}$ die Matrix mit $c_{k\bullet} = a_{k\bullet} + b_{k\bullet}$ und $c_{\ell\bullet} = a_{\ell\bullet} = b_{\ell\bullet}$ für $\ell \neq k$. Zu zeigen ist $\det(C) = \det(A) + \det(B)$. Tatsächlich gilt

$$\begin{aligned}
\det(C) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{n} c_{\ell\sigma(\ell)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) c_{k\sigma(k)} \prod_{\ell\neq k} c_{\ell\sigma(\ell)} = \\
&\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)(a_{k\sigma(k)} + b_{k\sigma(k)}) \prod_{\ell\neq k} c_{\ell\sigma(\ell)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{k\sigma(k)} \prod_{\ell\neq k} c_{\ell\sigma(\ell)} + \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{k\sigma(k)} \prod_{\ell\neq k} c_{\ell\sigma(\ell)} = \\
&\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{k\sigma(k)} \prod_{\ell\neq k} a_{\ell\sigma(\ell)} + \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{k\sigma(k)} \prod_{\ell\neq k} b_{\ell\sigma(\ell)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{n} a_{\ell\sigma(\ell)} + \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{n} b_{\ell\sigma(\ell)} \\
&= \det(A) + \det(B).
\end{aligned}$$

Sei nun $\lambda \in K$ und $D \in \mathscr{M}_{n,K}$ die Matrix gegeben durch $d_{k\bullet} = \lambda a_{k\bullet}$ und $d_{\ell\bullet} = a_{\ell\bullet}$ für $\ell \neq k$. Dann gilt

$$\begin{aligned}
\det(D) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{n} d_{\ell\sigma(\ell)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) d_{k\sigma(k)} \prod_{\ell\neq k} d_{\ell\sigma(\ell)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)(\lambda a_{k\sigma(k)}) \prod_{\ell\neq k} a_{\ell\sigma(\ell)} \\
&= \lambda \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{k\sigma(k)} \prod_{\ell\neq k} a_{\ell\sigma(\ell)} = \lambda \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{n} a_{\ell\sigma(\ell)} = \lambda \det(A).
\end{aligned}$$

Damit ist die Eigenschaft (i) aus Definition (12.2) verifiziert. Zum Nachweis von (ii) sei $A \in \mathscr{M}_{n,K}$ eine Matrix, in der die k-te und ℓ-te Zeile übereinstimmen, wobei $k \neq \ell$ sei. Für die Transposition $\tau = (k\ \ell)$ gilt $S_n = A_n \cup A_n \circ \tau$ nach (12.16). Weil die Elemente in A_n positives und die Elemente in $A_n \circ \tau$ negatives Signum haben, erhalten wir für $\det(A)$ den Ausdruck

$$\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\sigma\in A_n} \prod_{i=1}^{n} a_{i\sigma(i)} - \sum_{\sigma\in A_n\circ\tau} \prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\sigma\in A_n} \prod_{i=1}^{n} a_{i\sigma(i)} - \sum_{\sigma\in A_n} \prod_{i=1}^{n} a_{i\sigma(\tau(i))}$$

Weil die k-te und die ℓ-te Zeile von A übereinstimmen, gilt für die einzelnen Terme der rechten Summe

$$\begin{aligned}
\prod_{i=1}^{n} a_{i\sigma(\tau(i))} &= a_{k\sigma(\tau(k))} a_{\ell\sigma(\tau(\ell))} \prod_{i\neq k,\ell} a_{i\sigma(\tau(i))} = a_{k\sigma(\ell)} a_{\ell\sigma(k)} \prod_{i\neq k,\ell} a_{i\sigma(\tau(i))} \\
&= a_{\ell\sigma(\ell)} a_{k\sigma(k)} \prod_{i\neq k,\ell} a_{i\sigma(\tau(i))} = \prod_{i=1}^{n} a_{i\sigma(i)}.
\end{aligned}$$

Also heben sich die beiden Summen auf, und es folgt $\det(A) = 0$. Nun beweisen wir noch die Eigenschaft (iii). Die Determinante der Einheitsmatrix ist nach Definition gegeben durch

$$\det(E^{(n)}) = \sum_{\sigma\in S_n} s_\sigma \quad , \qquad s_\sigma = \operatorname{sgn}(\sigma)\delta_{1\sigma(1)} \cdots \delta_{n\sigma(n)}.$$

Gilt $\sigma(i) \neq i$ für ein i, dann folgt $\delta_{i\sigma(i)} = 0$ und somit $s_\sigma = 0$. Also ist s_{id} der einzige nicht-verschwindende Summand in der Leibniz-Formel, und dieser ist gleich 1. □

In der folgenden Situation lässt sich die Determinante einer Matrix leicht ausrechnen.

(12.18) Satz Man bezeichnet eine Matrix $A = (a_{ij}) \in \mathscr{M}_{n,K}$ als ***obere Dreiecksmatrix***, wenn $a_{ij} = 0$ für alle $i, j \in \{1, ..., n\}$ mit $i > j$ erfüllt ist. Für jede Matrix dieser Form gilt

$$\det(A) \quad = \quad a_{11} \cdot a_{22} \cdot ... \cdot a_{nn}.$$

Beweis: Zunächst zeigen wir, dass für jede Permutation $\sigma \in S_n \setminus \{\mathrm{id}\}$ ein $k \in M_n$ mit $\sigma(k) < k$ existiert. Anderfalls müsste $\sigma(\ell) \geq \ell$ für $1 \leq \ell \leq n$ gelten. Wegen $\sigma \neq \mathrm{id}$ gibt es andererseits auch ein maximales $k \in M_n$ mit $\sigma(k) > k$. Aber auf Grund der Maximalität müsste dann $\sigma(\sigma(k)) = \sigma(k)$ gelten, im Widerspruch zur Injektivität von σ.

Sei nun $\sigma \in S_n \setminus \{\mathrm{id}\}$ und $k \in M_n$ mit $\sigma(k) < k$. Dann folgt $a_{k\sigma(k)} = 0$ nach Definition der oberen Dreiecksmatrix, und zu σ gehörende Summand $\mathrm{sgn}(\sigma) \prod_{\ell=1}^{n} a_{\ell\sigma(\ell)}$ ist ebenfalls gleich null. Der einzige eventuell nicht verschwindende Summand in der Leibniz-Formel ist also der zum Element id Summand; wegen $\mathrm{sgn}(\mathrm{id}) = 1$ ist dieser Summand gleich dem Produkt $\prod_{\ell=1}^{n} a_{\ell\ell}$. □

Es gilt also beispielsweise

$$\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} \quad = \quad 1 \cdot 4 \cdot 6 \quad = \quad 24.$$

(12.19) Satz Für alle $A \in \mathscr{M}_{n,K}$ gilt $\det(A) = \det({}^{\mathrm{t}}A)$.

Beweis: Hier verwenden wir zum Beweis die Leibnizformel. Setzen wir $B = {}^{\mathrm{t}}A$, dann sind die Einträge b_{ij} von B gegeben durch $b_{ij} = a_{ji}$ für $1 \leq i, j \leq n$. Es gilt

$$\det({}^{\mathrm{t}}A) \quad = \quad \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} b_{i\sigma(i)} \quad = \quad \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i} \quad = \quad \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i)\sigma^{-1}(\sigma(i))}$$

Weil jedes σ bijektiv ist, durchläuft mit i auch $\sigma(i)$ alle Zahlen in $\{1, ..., n\}$. Wir können im Produkt also $\sigma(i)$ durch i ersetzen und erhalten

$$\prod_{i=1}^{n} a_{\sigma(i)\sigma^{-1}(\sigma(i))} \quad = \quad \prod_{i=1}^{n} a_{i\sigma^{-1}(i)}.$$

Nach (12.11) gilt $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$ für alle $\sigma \in S_n$. Somit gilt insgesamt

$$\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i)\sigma^{-1}(\sigma(i))} \quad = \quad \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma^{-1}) \prod_{i=1}^{n} a_{i\sigma^{-1}(i)} \quad = \quad \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \quad = \quad \det(A).$$

Beim vorletzten „=“ haben wir verwendet, dass mit σ auch σ^{-1} die gesamte Gruppe S_n durchläuft, so dass wir in jedem Summanden jeweils σ^{-1} durch σ ersetzen können. □

Als nächstes untersuchen wir, wie sich Zeilenumformungen auf die Determinante einer Matrix auswirken. Im ersten Semester haben wir die Elementarmatrizen

$$\mathrm{M}_{k,\lambda} = E^{(m)} + (\lambda - 1)\mathrm{B}_{kk}^{(m\times m)} \qquad \text{und} \qquad \mathrm{A}_{k,\ell,\lambda} = E^{(m)} + \lambda \mathrm{B}_{\ell k}^{(m\times m)}$$

eingeführt. Die Matrix $\mathrm{M}_{k,\lambda}$ entsteht aus der Einheitsmatrix $E^{(n)}$ durch Multiplikation der k-ten Zeilen mit dem Wert λ. Auf Grund der Multilinearität der Determinantenfunktion gilt deshalb $\det(\mathrm{M}_{k,\lambda}) = \lambda \det E^{(n)} = \lambda \cdot 1_K = \lambda$. Ist $A \in \mathscr{M}_{n,K}$ eine beliebige Matrix, dann entsteht $\mathrm{M}_{k,\lambda}A$ aus A durch Multiplikation der k-ten Zeile mit dem Wert λ. Wir erhalten somit die Rechenregel

$$\det(\mathrm{M}_{k,\lambda}A) \quad = \quad \lambda \det(A) \quad = \quad \det(\mathrm{M}_{k,\lambda}) \det(A) \qquad \text{für alle} \quad A \in \mathscr{M}_{n,K}.$$

Allgemein gilt: Entsteht eine Matrix $B = (b_{ij})$ aus $A = (a_{ij}) \in \mathscr{M}_{n,K}$ durch Addition des λ-fachen der k-ten Zeile zur ℓ-ten, dann gilt $\det(A) = \det(A')$, denn aus den Eigenschaften der Determinantenfunktion folgt

$$\det B \quad = \quad \det(..., b_{k\bullet}, ..., b_{\ell\bullet}, ...) \quad = \quad \det(..., a_{k\bullet}, ..., \lambda a_{k\bullet} + a_{\ell\bullet}, ...) \quad =$$

$$\lambda \det(..., a_{k\bullet}, ..., a_{k\bullet}, ...) + \det(..., a_{k\bullet}, ..., a_{\ell\bullet}, ...) \quad = \quad \lambda \cdot 0 + \det(A) \quad = \quad \det(A).$$

Insbesondere entsteht die Matrix $\mathrm{A}_{k,\ell,\lambda}$ aus $E^{(n)}$ durch Addition des λ-fachen der k-ten Zeile zur ℓ-ten. Somit gilt $\det \mathrm{A}_{k,\ell,\lambda} = E^{(n)} = 1$ und allgemein

$$\det(\mathrm{A}_{k,\ell,\lambda}A) \quad = \quad \det(\mathrm{A}_{k,\ell,\lambda}) \det(A) \qquad \text{für alle} \quad A \in \mathscr{M}_{n,K}.$$

Zusammenfassend kann also formuliert werden

(12.20) Lemma Ist $T, A \in \mathscr{M}_{n,K}$ und T eine Elementarmatrix, dann gilt

$$\det(TA) \quad = \quad \det(T) \det(A).$$

Eine quadratische Matrix in Zeilenstufenform ist insbesondere eine obere Dreiecksmatrix, und deren Determinante erhält man nach Satz (12.18) aus dem Produkt der Diagonalelemente. Wir haben gesehen, wie sich elementare Zeilenumformungen vom Typ $(\mathrm{M}_{k,\lambda})$ und $(\mathrm{A}_{k,\ell,\lambda})$ auf die Determinante auswirken. Außerdem führt die Vertauschung zweier Zeilen nach Lemma (12.5) lediglich zu einem Vorzeichenwechsel bei der Determinante. Dies zusammen liefert uns folgende Strategie für die Berechnung von $\det(A)$ für eine beliebige Matrix $A \in \mathscr{M}_{n,K}$.

(i) Forme A mit Hilfe des Gaußverfahrens in eine Matrix B in Zeilenstufenform um.
(ii) Bestimme anhand der durchgeführten Zeilenumformungen den Faktor $\mu \in K^\times$ mit $\det(B) = \mu \det(A)$.
(iii) Berechne $\det(B)$ durch Multiplikation der Diagonalelemente b_{11},...,b_{nn} von B.
Das Endergebnis der Rechnung ist dann $\det(A) = \mu^{-1} \det(B)$.

Wir demonstrieren die Funktionsweise des Verfahrens anhand der Matrix

$$A \quad = \quad \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 2 & 1 & 4 \\ 1 & 0 & -1 & 1 \\ -2 & 3 & 0 & 2 \end{pmatrix}.$$

Mit dem Gaußverfahren erhalten wir

$$\begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 2 & 1 & 4 \\ 1 & 0 & -1 & 1 \\ -2 & 3 & 0 & 2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 2 & 1 & 4 \\ 0 & 0 & -4 & -6 \\ 0 & 3 & 6 & 16 \end{pmatrix} \overset{(*)}{\mapsto} \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 3 & 6 & 16 \\ 0 & 0 & -4 & -6 \\ 0 & 2 & 1 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 1 & 5 & 12 \\ 0 & 0 & -4 & -6 \\ 0 & 2 & 1 & 4 \end{pmatrix} \mapsto$$

$$\begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 1 & 5 & 12 \\ 0 & 0 & -4 & -6 \\ 0 & 0 & -9 & -20 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 1 & 5 & 12 \\ 0 & 0 & -4 & -6 \\ 0 & 0 & -1 & -8 \end{pmatrix} \overset{(*)}{\mapsto} \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 1 & 5 & 12 \\ 0 & 0 & -1 & -8 \\ 0 & 0 & -4 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 1 & 5 & 12 \\ 0 & 0 & -1 & -8 \\ 0 & 0 & 0 & 26 \end{pmatrix}$$

Bezeichnen wir die Matrix am Ende der Rechnung mit B, dann gilt $\det(B) = 1 \cdot 1 \cdot (-1) \cdot 26 = -26$. In der Rechnung kommen an den beiden mit (*) markierten Stellen Zeilenvertauschungen vor, die jeweils einen Vorzeichenwechsel bewirken. Insgesamt gilt also $\det(B) = (-1)^2 \det(A) = \det(A)$ und damit $\det(A) = \det(B) = -26$.

Neben diesem praktischen Rechenverfahren führen unsere Überlegungen auch zu neuen theoretischen Resultaten.

(12.21) Satz *(Charakterisierung invertierbarer Matrizen)*

Für eine Matrix $A \in \mathscr{M}_{n,K}$ sind folgende Aussagen äquivalent.

(i) $A \in \mathrm{GL}_n(K)$ (d.h. die Matrix A ist invertierbar)
(ii) $\mathrm{rg}(A) = n$
(iii) $\det(A) \neq 0$

Beweis: Zunächst beweisen wir die Äquivalenz „(i) $\Leftrightarrow$ (ii)“. Sei $\phi_A : K^n \to K^n$ gegeben durch $v \mapsto Av$. Nach dem Dimensionssatz für lineare Abbildungen gilt $n = \dim \ker(\phi_A) + \dim \mathrm{im}(\phi_A)$. Aus §8 wissen wir auch, dass $\mathrm{rg}(A) = \dim \mathrm{im}(\phi_A)$ gilt. Also ist $\mathrm{rg}(A) = n$ genau dann erfüllt, wenn

$$\dim \ker(\phi_A) = 0 \quad \text{und} \quad \dim \mathrm{im}(\phi_A) = n$$

erfüllt gilt. Dies wiederum ist genau dann der Fall, wenn ϕ_A bijektiv ist. Nach Satz (11.9), angewendet auf die kanonische Basis $\mathscr{E}$ von K^n, ist die Bijektivität von ϕ_A wiederum äquivalent zur Invertierbarkeit von A.

An Stelle der Äquivalenz „(ii) $\Leftrightarrow$ (iii)“ beweisen wir, dass genau dann $\det(A) = 0$ ist, wenn $\mathrm{rg}(A) < n$ gilt. Weil sich die Determinante der Matrix bei Zeilenumformungen höchstens um einen Faktor $\lambda \in K^\times$ ändert, können wir voraussetzen, dass sich die Matrix A in Zeilenstufenform befindet. Der Zeilenrang von A ändert sich durch diese Umformungen nicht. Seien $j_1 < \ldots < j_r$ die Kennzahlen der Zeilenstufenform mit $r = \mathrm{rg}(A)$. Ist $r < n$, dann ist $a_{nn} = 0$, und somit gilt auch $\det(A) = \prod_{i=1}^n a_{ii} = 0$. Ist dagegen $r = n$, dann muss $j_i = i$ für $1 \leq i \leq n$ gelten, und die Einträge $a_{ij_i} = a_{ii}$ sind nach Definition der Zeilenstufenform ungleich Null. Also ist auch $\det(A)$ als Produkt der Diagonaleinträge ungleich Null. □

(12.22) Satz *(Multiplikationssatz für Determinanten)*

Seien $A, B \in \mathscr{M}_{n,K}$. Dann gilt $\det(AB) = \det(A)\det(B)$.

Beweis: Wie immer bezeichnen wir mit ϕ_A bzw. ϕ_B die linearen Abbildungen $K^n \to K^n$ gegeben durch $v \mapsto Av$ bzw. $v \mapsto Bv$. Nehmen wir zunächst an, dass $\det(A) = 0$ ist. Dann folgt $\dim \operatorname{im}(\phi_A) = \operatorname{rg}(A) < n$ und somit auch

$$\operatorname{rg}(AB) \quad = \quad \dim \operatorname{im}(\phi_A \circ \phi_B) \quad \leq \quad \dim \phi_A(K^n) \quad < \quad n.$$

Dies wiederum bedeutet $\det(AB) = 0$, d.h. in diesem Fall ist die Gleichung $\det(AB) = \det(A)\det(B)$ erfüllt. Nun betrachten wir den Fall, dass A invertierbar (also $\det(A) \neq 0$) ist. Für den Fall $A = E^{(n)}$ ist die Aussage trivial, und im Fall, dass es sich bei A um eine Elementarmatrix handelt, ist sie nach Lemma (12.20) erfüllt. Im allgemeinen Fall ist aus § 3 bekannt, dass A als Produkt $T_1 \cdot \ldots \cdot T_r$ von Elementarmatrizen darstellbar ist. Wir beweisen nun die Gleichung $\det(AB) = \det(A)\det(B)$ durch vollständige Induktion über r. Der Fall $r = 1$ ist bereits erledigt, denn in diesem Fall ist A selbst eine Elementarmatrix. Ist nun $r > 1$ und setzen wir die Gleichung für Werte $< r$ voraus, dann können wir $A' = T_1 \cdot \ldots \cdot T_{r-1}$ setzen und erhalten

$$\det(AB) \quad = \quad \det(A'T_rB) \quad = \quad \det(A')\det(T_rB) \quad =$$

$$\det(A')\det(T_r)\det(B) \quad = \quad \det(A'T_r)(\det B) \quad = \quad \det(A)\det(B). \qquad \square$$

Gelegentlich ist auch die folgende Rechenregel nützlich.

(12.23) Satz Sei $M \in \mathscr{M}_{n,K}$ eine Blockmatrix der Form

$$M \quad = \quad \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

mit $A \in \mathscr{M}_{r,K}$, $B \in \mathscr{M}_{r\times(n-r),K}$ und $C \in \mathscr{M}_{n-r,K}$. Dann gilt $\det(M) = \det(A)\det(C)$.

Beweis: Aus dem ersten Semester ist bekannt, dass es Elementarmatrizen $T_1, \ldots, T_k \in \mathrm{GL}_r(K)$ und $U_1, \ldots, U_\ell \in \mathrm{GL}_n(K)$ gibt, so dass $A' = T_k \cdots T_1 A$ und $C' = U_\ell \cdots U_1 C$ in Zeilenstufenform vorliegen, also insbesondere obere Dreiecksmatrizen sind. Für jede Matrix $B' \in \mathscr{M}_{r\times(n-r),K}$ ist dann auch die Blockmatrix

$$M' \quad = \quad \begin{pmatrix} A' & B' \\ 0 & C' \end{pmatrix}$$

eine obere Dreiecksmatrix, und es gilt

$$\det M' \quad = \quad \left(\prod_{i=1}^{r} a'_{ii}\right)\left(\prod_{j=1}^{n} c'_{jj}\right) \quad = \quad \det(A')\det(C').$$

Man überprüft unmittelbar, dass mit T_i und U_j auch

$$\hat{T}_i = \begin{pmatrix} T_i & 0 \\ 0 & E^{(n-r)} \end{pmatrix} \qquad \text{und} \qquad \hat{U}_j = \begin{pmatrix} E^{(r)} & 0 \\ 0 & U_j \end{pmatrix}$$

Elementarmatrizen sind, für die $\det T_i = \det \hat{T}_i$ sowie $\det U_j = \det \hat{U}_j$ gilt. Auf Grund der Rechenregeln für Produkte von Blockmatrizen aus dem ersten Semester gilt

$$\hat{T}_k \cdots \hat{T}_1 M = \begin{pmatrix} T_k & 0 \\ 0 & E^{(n-r)} \end{pmatrix} \cdots \begin{pmatrix} T_1 & 0 \\ 0 & E^{(n-r)} \end{pmatrix} \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \begin{pmatrix} T_k \cdots T_1 A & T_k \cdots T_1 B \\ 0 & C \end{pmatrix} = \begin{pmatrix} A' & B' \\ 0 & C \end{pmatrix}$$

mit $B' = T_k \cdots T_1 B$ und ebenso

$$\hat{U}_\ell \cdots \hat{U}_1 \begin{pmatrix} A' & B' \\ 0 & C \end{pmatrix} = \begin{pmatrix} E^{(r)} & 0 \\ 0 & U_\ell \end{pmatrix} \cdots \begin{pmatrix} E^{(r)} & 0 \\ 0 & U_1 \end{pmatrix} \begin{pmatrix} A' & B' \\ 0 & C \end{pmatrix} = \begin{pmatrix} A' & B' \\ 0 & U_\ell \cdots U_1 C \end{pmatrix} = \begin{pmatrix} A' & B' \\ 0 & C' \end{pmatrix}$$

Damit erhalten wir insgesamt

$$\left(\prod_{i=1}^{k} \det T_i\right)\left(\prod_{j=1}^{\ell} \det U_j\right) \det(A) \det(C) = \det(A') \det(C') = \det M' =$$

$$\left(\prod_{i=1}^{k} \det \hat{T}_i\right)\left(\prod_{j=1}^{\ell} \det \hat{U}_j\right) \det(M) = \left(\prod_{i=1}^{k} \det T_i\right)\left(\prod_{j=1}^{\ell} \det U_j\right) \det(M)$$

und somit $\det(A)\det(C) = \det(M)$. □

Bevor wird den Laplaceschen Entwicklungssatz formulieren und beweisen können, benötigen wir ein wenig zusätzliche Notation. Sei $A = (a_{ij}) \in \mathscr{M}_{n,K}$. Für beliebige $i, j \in \{1, ..., n\}$ sei dann $A'_{ij} = (a'_{k\ell})$ die Matrix in $\mathscr{M}_{n,K}$ mit den Einträgen

$$a'_{k\ell} = \begin{cases} a_{k\ell} & \text{für } k \neq i, \ell \neq j \\ 0 & \text{für } k = i, \ell \neq j \\ 0 & \text{für } k \neq i, \ell = j \\ 1 & \text{für } k = i, \ell = j \end{cases}$$

Die Matrix A'_{ij} hat also die Form

$$A'_{ij} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & 0 & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix}$$

Mit $A_{ij} \in \mathscr{M}_{n-1,K}$ bezeichnen wir die Matrix, die aus A durch Streichung der i-ten Zeile und j-ten Spalten zu Stande kommt, also

$$A_{ij} \quad = \quad \begin{pmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix}$$

(12.24) Lemma Es gilt $\det(A'_{ij}) = (-1)^{i+j} \det(A_{ij})$.

Beweis: Durch $i-1$ Zeilenvertauschungen bewegt man die i-te Zeile von A'_{ij} nach oben in die erste Zeile. Anschließend führt man $j-1$ Spaltenvertauschungen durch, um die j-te Spalte ganz nach links zu bewegen. Insgesamt ändert sich das Vorzeichen dadurch um den Faktor $(-1)^{(i-1)+(j-1)} = (-1)^{i+j}$, und man erhält eine Matrix der Form

$$\begin{pmatrix} 1 & 0 \\ 0 & A_{ij} \end{pmatrix}$$

Auf Grund der Formel in Satz (12.23) über die Determinante von Blockmatrizen stimmt die Determinante dieser Matrix mit $\det(A_{ij})$ überein. □

(12.25) Definition Sei $A \in \mathscr{M}_{n,K}$. Die Matrix $\tilde{A} \in \mathscr{M}_{n,K}$ mit den Einträgen

$$\tilde{a}_{ij} \quad = \quad \det(A'_{ji}) \quad = \quad (-1)^{i+j} \det(A_{ji})$$

wird die zu A ***komplementäre*** oder ***adjunkte*** Matrix genannt. (Man beachte die Vertauschung von Zeilen- und Spaltenindex, dies ist kein Tippfehler!)

(12.26) Lemma Sei $A \in \mathscr{M}_{n,K}$. Dann gilt für $1 \leq i, j \leq n$ jeweils

$$\det(A'_{ij}) \quad = \quad \det(a_{1\bullet}, \ldots, a_{i-1\bullet}, e_j, a_{i+1\bullet}, \ldots, a_{n\bullet})$$

Beweis: Sei B die Matrix auf der rechten Seite der Gleichung. Dann kann B in A'_{ij} umgeformt werden, indem man für alle k mit $1 \leq k \leq n$ und $i \neq k$ jeweils das a_{kj}-fache der i-ten Zeile von der k-ten Zeile von B subtrahiert. Dies zeigt, dass die beiden Determinanten übereinstimmen. □

(12.27) Proposition Sei $\tilde{A}$ die zu $A \in \mathscr{M}_{n,K}$ komplementäre Matrix. Dann gilt

$$\tilde{A}A \quad = \quad A\tilde{A} \quad = \quad \det(A)E^{(n)}.$$

Beweis: Zunächst zeigen wir die Gleichung $A\tilde{A} = \det(A)E^{(n)}$. Für den Eintrag von $A\tilde{A}$ an der Stelle (i,k) gilt nach Lemma (12.26) und der Rechenregeln für die Determinante jeweils

$$\sum_{j=1}^{n} a_{ij}\tilde{a}_{jk} \quad = \quad \sum_{j=1}^{n} a_{ij}\det(A'_{kj}) \quad = \quad \sum_{j=1}^{n} a_{ij}\det(a_{1\bullet},...,a_{k-1\bullet},e_j,a_{k+1\bullet},...,a_{n\bullet}) \quad =$$

$$\det\left(a_{1\bullet},...,a_{k-1\bullet},\sum_{j=1}^{n} a_{ij}e_j,a_{k+1\bullet},...,a_{n\bullet}\right) \quad = \quad \det(a_{1\bullet},...,a_{k-1\bullet},a_{i\bullet},a_{k+1\bullet},...,a_{n\bullet}) \quad = \quad \delta_{ik}\det(A).$$

Der Eintrag von $A\tilde{A}$ an der Stelle (i,k) stimt also mit dem entsprechenden Eintrag von $(\det A)E^{(n)}$ überein. Für den Beweis der zweiten Gleichung bemerken wir zunächst, dass ${}^t\tilde{A}$ nach Definition die zu ${}^tA$ komplementäre Matrix ist. Auf Grund der bereits bewiesenen Gleichung gilt also

$$\tilde{A}A \quad = \quad {}^t({}^tA\,{}^t\tilde{A}) \quad = \quad {}^t(\det(A)E^{(n)}) \quad = \quad \det(A)E^{(n)}. \qquad \square$$

Wir demonstrieren die Berechnung der komplentären Matrix am Beispiel von

$$A \quad = \quad \begin{pmatrix} 6 & 0 & 4 \\ -2 & 2 & -2 \\ 14 & 0 & 10 \end{pmatrix}.$$

Die Einträge der komplementären Matrix $\tilde{A}$ sind gegeben durch

$$\tilde{a}_{11} = (-1)^{1+1}\det(A_{11}) = \det\begin{pmatrix} 2 & -2 \\ 0 & 10 \end{pmatrix} = 20 \quad , \quad \tilde{a}_{12} = (-1)^{1+2}\det(A_{21}) = -\det\begin{pmatrix} 0 & 4 \\ 0 & 10 \end{pmatrix} = 0 \quad ,$$

$$\tilde{a}_{13} = (-1)^{1+3}\det(A_{31}) = \det\begin{pmatrix} 0 & 4 \\ 2 & -2 \end{pmatrix} = -8 \quad , \quad \tilde{a}_{21} = (-1)^{2+1}\det(A_{12}) = -\det\begin{pmatrix} -2 & -2 \\ 14 & 10 \end{pmatrix} = -8 \quad ,$$

$$\tilde{a}_{22} = (-1)^{2+2}\det(A_{22}) = \det\begin{pmatrix} 6 & 4 \\ 14 & 10 \end{pmatrix} = 4 \quad , \quad \tilde{a}_{23} = (-1)^{2+3}\det(A_{32}) = -\det\begin{pmatrix} 6 & 4 \\ -2 & -2 \end{pmatrix} = -(-4) = 4 \quad ,$$

$$\tilde{a}_{31} = (-1)^{3+1}\det(A_{13}) = \det\begin{pmatrix} -2 & 2 \\ 14 & 0 \end{pmatrix} = -28 \quad , \quad \tilde{a}_{32} = (-1)^{3+2}\det(A_{23}) = -\det\begin{pmatrix} 6 & 0 \\ 14 & 0 \end{pmatrix} = 0 \quad ,$$

$$\tilde{a}_{33} = (-1)^{3+3}\det(A_{33}) = \det\begin{pmatrix} 6 & 0 \\ -2 & 2 \end{pmatrix} = 12$$

also gilt

$$\tilde{A} \quad = \quad \begin{pmatrix} 20 & 0 & -8 \\ -8 & 4 & 4 \\ -28 & 0 & 12 \end{pmatrix}.$$

Wie nach (12.27) zu erwarten, gilt

$$A\cdot\tilde{A} \quad = \quad \begin{pmatrix} 6 & 0 & 4 \\ -2 & 2 & -2 \\ 14 & 0 & 10 \end{pmatrix}\begin{pmatrix} 20 & 0 & -8 \\ -8 & 4 & 4 \\ -28 & 0 & 12 \end{pmatrix} \quad = \quad \begin{pmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{pmatrix} \quad = \quad 8\cdot E^{(3)}.$$

Daraus folgt $A \cdot (\frac{1}{8}\tilde{A}) = E^{(3)}$. Die zu A inverse Matrix ist also gegeben durch

$$A^{-1} \quad = \quad \tfrac{1}{8}\tilde{A} \quad = \quad \begin{pmatrix} \frac{5}{2} & 0 & -1 \\ -1 & \frac{1}{2} & \frac{1}{2} \\ -\frac{7}{2} & 0 & \frac{3}{2} \end{pmatrix}.$$

(12.28) Satz *(Laplacescher Entwicklungssatz)*
Sei $A \in \mathscr{M}_{n,K}$.

(i) Für alle $i \in \{1, \ldots, n\}$ gilt $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$.

(ii) Für alle $j \in \{1, \ldots, n\}$ gilt $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$.

Wird die Determinante von A mittels (i) berechnet, spricht man von einer ***Entwicklung zur i-ten Zeile***. Die Berechnung mittels (ii) bezeichnet man als Entwicklung zur j-ten Spalte.

Beweis: Auf Grund der Proposition ist der Eintrag von $A\tilde{A}$ an der Stelle (i,i) gleich $\det(A)$. Es gilt also

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

Auch der Eintrag von $\tilde{A}A$ an der Stelle (j,j) ist gleich $\det(A)$. Folglich gilt

$$\det(A) \quad = \quad \sum_{i=1}^{n} \tilde{a}_{ji} a_{ij} \quad = \quad \sum_{i=1}^{n} a_{ij} \det(A'_{ij}) \quad = \quad \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}). \qquad \square$$

Wir demonstrieren die Anwendung des Laplaceschen Entwicklungssatzes anhand der Matrix

$$A \quad = \quad \begin{pmatrix} 1 & 0 & 3 & 7 \\ 0 & 2 & 1 & 4 \\ 1 & 0 & -1 & 1 \\ -2 & 3 & 0 & 2 \end{pmatrix}.$$

Bei jeder Entwicklung müssen die Determinanten der Teilmatrizen nach folgendem Schema mit einem Vorzeichen versehen werden

$$\begin{pmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{pmatrix}$$

denn es ist $(-1)^{1+1} = +1$, $(-1)^{1+2} = -1$, $(-1)^{1+3} = +1$ usw. Die Entwicklung von $\det(A)$ nach der ersten Zeile ergibt nun

$$\begin{aligned}\det(A) &= 1 \cdot \det\begin{pmatrix} 2 & 1 & 4 \\ 0 & -1 & 1 \\ 3 & 0 & 2 \end{pmatrix} - 0 \cdot \det\begin{pmatrix} 0 & 1 & 4 \\ 1 & -1 & 1 \\ -2 & 0 & 2 \end{pmatrix} + 3 \cdot \det\begin{pmatrix} 0 & 2 & 4 \\ 1 & 0 & 1 \\ -2 & 3 & 2 \end{pmatrix} - 7 \cdot \det\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & -1 \\ -2 & 3 & 0 \end{pmatrix} \\ &= 1 \cdot 11 + 3 \cdot 4 - 7 \cdot 7 = -26.\end{aligned}$$

Durch Entwicklung zur zweiten Zeile erhalten wir ebenso

$$\begin{aligned}\det(A) &= 1 \cdot \det\begin{pmatrix} 0 & 3 & 7 \\ 2 & 1 & 4 \\ 3 & 0 & 2 \end{pmatrix} - 0 \cdot \det\begin{pmatrix} 1 & 3 & 7 \\ 0 & 1 & 4 \\ -2 & 0 & 2 \end{pmatrix} + (-1) \cdot \det\begin{pmatrix} 1 & 0 & 7 \\ 0 & 2 & 4 \\ -2 & 3 & 2 \end{pmatrix} - 1 \cdot \det\begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \\ -2 & 3 & 0 \end{pmatrix} \\ &= 1 \cdot 3 + (-1) \cdot 20 - 1 \cdot 9 = -26.\end{aligned}$$

Eine weitere Möglichkeit wäre die Entwicklung zur zweiten Spalte.

$$\begin{aligned}\det(A) &= -0 \cdot \det\begin{pmatrix} 0 & 1 & 4 \\ 1 & -1 & 1 \\ -2 & 0 & 2 \end{pmatrix} + 2 \cdot \det\begin{pmatrix} 1 & 3 & 7 \\ 1 & -1 & 1 \\ -2 & 0 & 2 \end{pmatrix} - 0 \cdot \det\begin{pmatrix} 1 & 3 & 7 \\ 0 & 1 & 4 \\ -2 & 0 & 2 \end{pmatrix} + 3 \cdot \det\begin{pmatrix} 1 & 3 & 7 \\ 0 & 1 & 4 \\ 1 & -1 & 1 \end{pmatrix} \\ &= 2 \cdot (-28) + 3 \cdot 10 = -26.\end{aligned}$$

Insgesamt gibt es $4 + 4 = 8$ verschiedene Möglichkeiten, $\det(A)$ durch Entwicklung zu einer Zeile oder Spalte zu entwickeln, also noch fünf weitere. Besonders günstig ist natürlich, eine Zeile oder Spalte mit möglichst vielen Nulleinträgen zu wählen, weil dann nur wenige Determinanten von 3×3-Matrizen ausgerechnet werden müssen.

Wir behandeln noch eine Anwendung des Laplace'schen Entwicklungssatzes.

(12.29) Satz *(Cramersche Regel)*

Sei $A \in \mathcal{M}_{n,K}$ invertierbar und $b \in K^n$. Für $1 \leq j \leq n$ bezeichnen wir mit $A^{(j)} \in \mathcal{M}_{n,K}$ die Matrix, die dadurch entsteht, dass man in A die j-te Spalte durch b ersetzt. Dann ist der Vektor $v = (v_1, \ldots, v_n) \in K^n$ mit den Komponenten

$$v_j = \frac{\det A^{(j)}}{\det A} \qquad \text{für } 1 \leq j \leq n$$

die eindeutig bestimmte Lösung des linearen Gleichungssystems $Ax = b$.

Beweis: Die Entwicklung von $A^{(j)}$ zur j-ten Spalte mit dem Laplace'schen Entwicklungssatz liefert für $1 \leq j \leq n$ jeweils

$$\det A^{(j)} = \sum_{k=1}^{n} (-1)^{k+j} b_k \det(A_{kj}).$$

Für $1 \leq i \leq n$ erhalten wir somit

$$\sum_{j=1}^{n} a_{ij} v_j \quad = \quad (\det A)^{-1} \sum_{j=1}^{n} a_{ij} \det A^{(j)} \quad = \quad (\det A)^{-1} \sum_{j=1}^{n} \sum_{k=1}^{n} (-1)^{k+j} a_{ij} b_k \det A_{kj} \quad = \quad (\det A)^{-1} \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} \tilde{a}_{jk} b_k$$

wobei im letzten Schritt die Definition der adjunkten Matrix $\tilde{A}$ verwendet wurde. Die Summe $\sum_{j=1}^{n} a_{ij} \tilde{a}_{jk}$ ist jeweils gleich dem Eintrag des Matrixprodukts $A\tilde{A}$ an der Stelle (i,k). Nach Proposition (12.27) ist dieses Produkt gleich $(\det A)E^{(n)}$, der Eintrag an der Stelle (i,k) ist also gleich $\delta_{ik} \det A$. Setzen wir dies ein, so erhalten wir

$$\sum_{j=1}^{n} a_{ij} v_j \quad = \quad (\det A)^{-1} \sum_{k=1}^{n} \delta_{ik} (\det A) b_k \quad = \quad \sum_{k=1}^{n} \delta_{ik} b_k \quad = \quad b_i .$$

Der Eintrag des Vektors Av an der Stelle i stimmt also mit b_i überein, für $1 \leq i \leq n$. Es gilt also tatsächlich $Av = b$, d.h. v ist eine Lösung des Linearen Gleichungssytems. □

Als Anwendungsbeispiel für die Cramersche Regel betrachten wir das lineare Gleichungssystem über $\mathbb{R}$ gegeben durch

$$\begin{array}{rcrcrcl} 3x_1 & - & 2x_2 & + & 2x_3 & = & 1 \\ -2x_1 & + & 5x_2 & - & 6x_3 & = & 0 \\ 4x_1 & + & 3x_2 & - & 2x_3 & = & 3 \end{array}$$

Mit der Notation aus Satz (12.29) gilt

$$A = \begin{pmatrix} 3 & -2 & 2 \\ -2 & 5 & -6 \\ 4 & 3 & -2 \end{pmatrix} \quad , \quad A^{(1)} = \begin{pmatrix} 1 & -2 & 2 \\ 0 & 5 & -6 \\ 3 & 3 & -2 \end{pmatrix} \quad , \quad A^{(2)} = \begin{pmatrix} 3 & 1 & 2 \\ -2 & 0 & -6 \\ 4 & 3 & -2 \end{pmatrix} \quad , \quad A^{(3)} = \begin{pmatrix} 3 & -2 & 1 \\ -2 & 5 & 0 \\ 4 & 3 & 3 \end{pmatrix} .$$

Es ist $\det A = 28$, $\det A^{(1)} = \det A^{(2)} = 14$ und $\det A^{(3)} = 7$. Aus der Cramerschen Regel folgt also, dass $v = (\frac{1}{2}, \frac{1}{2}, \frac{1}{4})$ die eindeutig bestimmte Lösung des Systems ist.

§ 13. Eigenwerte und Diagonalisierbarkeit

Inhaltsübersicht

Ein *Eigenvektor* einer linearen Abbildung $\phi : V \to V$ ist ein Vektor $v \neq 0_V$, der von ϕ auf ein Vielfaches λv von sich selbst abgebildet wird. In diesem Fall bezeichnet man λ dann als *Eigenwert* von ϕ. Zunächst werden wir sehen, wie man Eigenvektoren und -werte einer vorgegebenen linearen Abbildung ϕ ausrechnet; für die Eigenwerte benötigt man das *charakteristische Polynom* einer Matrix.

In einigen Fällen ist es mit Hilfe der Eigenwerte und -vektoren möglich, eine Basis $\mathscr{A}$ zu finden, bezüglich der die Darstellungsmatrix $\mathscr{M}_{\mathscr{A}}^{\mathscr{A}}(\phi)$ eine besonders einfache Form, nämlich Diagonalgestalt, annimmt. Man bezeichnet ϕ in diesem Fall als *diagonalisierbar*. Hauptergebnis dieses Abschnitts wird ein einfaches Kriterium sein, mit dem sich die Diagonalisierbarkeit von ϕ testen lässt. Die hier entwickelte Theorie spielt unter anderem beim Lösen von Differenzialgleichungen eine wichtige Rolle. Auch in der Physik, zum Beispiel in der klassischen Mechanik und in der Quantenmechanik, wird mit diagonalisierbaren linearen Abbildungen gearbeitet.

Wichtige Begriffe und Sätze

- Eigenwert und Eigenvektor eines Endomorphismus
- Eigenwert und Eigenvektor einer Matrix
- Ähnlichkeit von Matrizen
- Vielfachheit $\mu_a(f, \lambda)$ der Nullstelle a eines Polynoms f
- charakteristisches Polynom χ_ϕ bzw. χ_A eines Endomorphismus, einer Matrix, Zusammenhang zwischen Nullstellen und Eigenwerten
- Diagonalmatrix, Diagonalisierbarkeit von Endomorphismen und Matrizen
- algebraische Vielfachheit $\mu_a(A, \lambda)$ eines Eigenwerts
- geometrische Vielfachheit $\mu_g(A, \lambda)$ eines Eigenwerts
- Hauptergebnis: Diagonalisierbarkeitskriterium

Im gesamten Text bezeichnet K stets einen beliebigen Körper.

(13.1) Definition Sei V ein K-Vektorraum und ϕ ein Endomorphismus von V, also eine lineare Abbildung $V \to V$. Man nennt

(i) $\lambda \in K$ einen ***Eigenwert*** von ϕ, wenn es ein $v \in V$ mit $v \neq 0_V$ und $\phi(v) = \lambda v$, und
(ii) $v \in V$ einen ***Eigenvektor*** von ϕ, wenn $v \neq 0_V$ ist und ein $\lambda \in K$ mit $\phi(v) = \lambda v$ existiert.

Seien nun $v \in V$ und $\lambda \in K$ vorgegeben. Man nennt v einen Eigenvektor zum Eigenwert λ, wenn $v \neq 0_V$ und die Gleichung $\phi(v) = \lambda v$ erfüllt ist.

Betrachten wir zum Beispiel über $K = \mathbb{Q}$ die beiden Matrizen

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \qquad \text{und} \qquad B = \begin{pmatrix} -2 & -10 & 0 & -40 \\ -24 & -13 & -8 & -68 \\ 15 & 30 & 3 & 120 \\ 6 & 4 & 2 & 20 \end{pmatrix}.$$

Die Zahlen $1, 2, 3$ sind Eigenwerte von A, und die Einheitsvektoren e_1, e_2, e_3 sind zugehörige Eigenvektoren, denn es gilt $Ae_1 = 1 \cdot e_1$, $Ae_2 = 2 \cdot e_2$ und $Ae_3 = 3 \cdot e_3$.

Die Matrix B hat die Zahlen -2, 3 und 4 als Eigenwerte. Die Vektoren $u = (1, 0, -3, 0)$, $v = (16, 0, -31, -2)$ und $w = (0, 4, 0, -1)$ sind zugehörige Eigenvektoren, denn es gilt

$$\begin{pmatrix} -2 & -10 & 0 & -40 \\ -24 & -13 & -8 & -68 \\ 15 & 30 & 3 & 120 \\ 6 & 4 & 2 & 20 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -3 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 6 \\ 0 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 0 \\ -3 \\ 0 \end{pmatrix} \quad , \quad \begin{pmatrix} -2 & -10 & 0 & -40 \\ -24 & -13 & -8 & -68 \\ 15 & 30 & 3 & 120 \\ 6 & 4 & 2 & 20 \end{pmatrix} \begin{pmatrix} 16 \\ 0 \\ -31 \\ -2 \end{pmatrix} = \begin{pmatrix} 48 \\ 0 \\ -93 \\ -6 \end{pmatrix} = 3 \begin{pmatrix} 16 \\ 0 \\ -31 \\ -2 \end{pmatrix}$$

$$\text{und} \quad \begin{pmatrix} -2 & -10 & 0 & -40 \\ -24 & -13 & -8 & -68 \\ 15 & 30 & 3 & 120 \\ 6 & 4 & 2 & 20 \end{pmatrix} \begin{pmatrix} 0 \\ 4 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 16 \\ 0 \\ -4 \end{pmatrix} = 4 \begin{pmatrix} 0 \\ 4 \\ 0 \\ -1 \end{pmatrix}.$$

(13.2) Definition Sei V ein K-Vektorraum und $\phi \in \mathrm{End}_K(V)$. Für jedes $\lambda \in K$ bezeichnet man die Menge $\mathrm{Eig}(\phi, \lambda) = \{v \in V \mid \phi(v) = \lambda v\}$ als den ***Eigenraum*** von ϕ zum Wert $\lambda \in K$. Er besteht aus dem Nullvektor 0_V und den Eigenvektoren zum Eigenwert λ.

(13.3) Proposition Sei V ein K-Vektorraum und $\phi \in \mathrm{End}_K(V)$. Für jedes $\lambda \in K$ ist der Eigenraum gegeben durch $\mathrm{Eig}(\phi, \lambda) = \ker(\phi - \lambda \mathrm{id}_V)$. Das Element λ ist ein Eigenwert von ϕ genau dann, wenn $\mathrm{Eig}(\phi, \lambda) \neq \{0_V\}$ gilt.

Beweis: Für jeden Vektor $v \in V$ gilt die Äquivalenz

$$\begin{aligned} v \in \mathrm{Eig}(\phi, \lambda) \quad &\Leftrightarrow \quad \phi(v) = \lambda v \quad \Leftrightarrow \quad \phi(v) - \lambda v = 0_V \quad \Leftrightarrow \quad \phi(v) - \lambda \mathrm{id}_V(v) = 0_V \\ &\Leftrightarrow \quad (\phi - \lambda \mathrm{id}_V)(v) = 0_V \quad \Leftrightarrow \quad v \in \ker(\phi - \lambda \mathrm{id}_V). \end{aligned}$$

Daraus folgt $\mathrm{Eig}(\phi, \lambda) = \ker(\phi - \lambda \mathrm{id}_V)$. Ein Element $\lambda \in K$ ist nach Definition Eigenwert genau dann, wenn ein $v \in V$ mit $v \neq 0_V$ und $\phi(v) = \lambda v$ existiert, also genau dann, wenn es ein Element ungleich 0_V in $\mathrm{Eig}(\phi, \lambda)$ gibt. Weil 0_V auf jeden Fall in $\mathrm{Eig}(\phi, \lambda)$ liegt, ist dies wiederum äquivalent zu $\mathrm{Eig}(\phi, \lambda) \neq \{0_V\}$. □

Aus dem ersten Semester ist bekannt, dass Kerne von linearen Abbildungen Untervektorräume sind. Die Proposition zeigt also, dass $\mathrm{Eig}(\phi, \lambda)$ für jedes $\lambda \in K$ und jedes $\phi \in \mathrm{End}_K(V)$ ein Untervektorraum von V ist. Natürlich kann diese Eigenschaft auch direkt nachgerechnet werden.

Als nächstes sehen wir uns an, wie das Matrixkalkül zur Untersuchung von Eigenwerten und Eigenvektoren eingesetzt werden kann. Sei nun $A \in \mathscr{M}_{n,K}$ eine quadratische Matrix. Wir bezeichnen $v \in K^n$ als einen ***Eigenvektor von*** A, wenn v ein Eigenvektor der Abbildung $\phi_A : K^n \to K^n$, $v \mapsto Av$ ist.

Ebenso sind die ***Eigenwerte von*** A nach Definition die Eigenwerte des Endomorphismus ϕ_A. Für jedes $\lambda \in K$ definieren wir

$$\operatorname{Eig}(A,\lambda) \quad = \quad \operatorname{Eig}(\phi_A,\lambda) \quad = \quad \{v \in K^n \mid Av = \lambda v\}.$$

Wiederum besteht $\operatorname{Eig}(A,\lambda)$ aus den Eigenvektoren von A zum Eigenwert λ und dem Nullvektor 0_{K^n}, und darüber hinaus gilt

$$\operatorname{Eig}(A,\lambda) \quad = \quad \ker(A - \lambda E^{(n)}).$$

Der Kern einer Matrix kann mit dem Gaußverfahren berechnet werden, also erhalten wir auch die Eigenräume einer Matrix mit dem Gaußverfahren. Betrachten wir zum Beispiel den Eigenraum $\operatorname{Eig}(A,-2)$ der Matrix

$$A \quad = \quad \begin{pmatrix} -2 & -5 & 10 \\ -20 & -17 & 40 \\ -10 & -10 & 23 \end{pmatrix}$$

zum Eigenwert $\lambda = -2$. Es gilt

$$\operatorname{Eig}(A,-2) \quad = \quad \ker(A + 2E^{(3)}) \quad = \quad \ker \begin{pmatrix} 0 & -5 & 10 \\ -20 & -15 & 40 \\ -10 & -10 & 25 \end{pmatrix}.$$

Wir wenden auf diese Matrix den Gauß-Algorithmus an.

$$\begin{pmatrix} 0 & -5 & 10 \\ -20 & -15 & 40 \\ -10 & -10 & 25 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 0 & 1 & -2 \\ 4 & 3 & -8 \\ 2 & 2 & -5 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 2 & 2 & -5 \\ 4 & 3 & -8 \\ 0 & 1 & -2 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 2 & 2 & -5 \\ 0 & -1 & 2 \\ 0 & 1 & -2 \end{pmatrix} \quad \mapsto$$

$$\begin{pmatrix} 2 & 2 & -5 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}$$

Die letzte Matrix entspricht dem LGS $x_1 - \frac{1}{2}x_3 = 0$, $x_2 - 2x_3 = 0$, und wir erhalten

$$\operatorname{Eig}(A,-2) \quad = \quad \ker(A + 2E^{(3)}) \quad = \quad \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Q}^3 \;\middle|\; x_1 - \tfrac{1}{2}x_3 = 0, x_2 - 2x_3 = 0 \right\} \quad = \quad \left\{ \begin{pmatrix} \frac{1}{2}x_3 \\ 2x_3 \\ x_3 \end{pmatrix} \;\middle|\; x_3 \in \mathbb{R} \right\}$$

$$= \quad \left\langle \begin{pmatrix} \frac{1}{2} \\ 2 \\ 1 \end{pmatrix} \right\rangle \quad = \quad \left\langle \begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix} \right\rangle.$$

Tatsächlich ist $(1,4,2)$ ein Eigenvektor von A zum Eigenwert -2, denn es gilt

$$A\begin{pmatrix}1\\4\\2\end{pmatrix} \quad = \quad \begin{pmatrix}-2 & -5 & 10\\ -20 & -17 & 40\\ -10 & -10 & 23\end{pmatrix}\begin{pmatrix}1\\4\\2\end{pmatrix} \quad = \quad \begin{pmatrix}-2\\-8\\-4\end{pmatrix} \quad = \quad (-2)\cdot\begin{pmatrix}1\\4\\2\end{pmatrix}.$$

Aus § 4 wissen wir, dass jede lineare Abbildung $\phi : V \to W$ zwischen endlich-dimensionalen K-Vektorräumen V, W auf eindeutige Weise durch eine Matrix beschrieben werden kann, sobald man für V und W Basen festgelegt hat. Ist $\mathscr{A}$ eine Basis von V und $\mathscr{B}$ eine Basis von W, dann haben wir die Bezeichung

$$\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$$

für die Darstellungsmatrix von ϕ bezüglich der Basen $\mathscr{A}$ und $\mathscr{B}$ eingeführt. Wir erinnern an den wichtigen Zusammenhang

$$\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)\Phi_{\mathscr{A}}(v) \quad = \quad \Phi_{\mathscr{B}}(\phi(v)).$$

Die Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}^{\mathscr{A}}(\phi)$ ist also dadurch gekennzeichnet, dass sie den Vektor v in $\mathscr{A}$-Koordinaten entgegennimmt und den Vektor $\phi(v)$ in $\mathscr{B}$-Koordinaten als Ergebnis liefert.

Ist nun $V = W$, die Abbildung ϕ also ein ***Endomorphismus*** des Vektorraums V, dann braucht man nur noch ***eine*** Basis von V, um ϕ zu beschreiben. Wir setzen $\mathscr{M}_{\mathscr{A}}(\phi) = \mathscr{M}_{\mathscr{A}}^{\mathscr{A}}(\phi)$ und nennen diese quadratische Matrix die ***Darstellungsmatrix*** von ϕ bezüglich der Basis $\mathscr{A}$.

(13.4) Definition Zwei Matrizen $A, B \in \mathscr{M}_{n,K}$ werden ***ähnlich*** genannt, wenn eine invertierbare Matrix $T \in \mathrm{GL}_n(K)$ mit $B = TAT^{-1}$ existiert. Zwei Matrizen $A, B \in \mathscr{M}_{m\times n,K}$ bezeichnet man als ***äquivalent***, wenn Elemente $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ mit $B = SAT$ existieren.

Ähnliche Matrizen sind also stets äquivalent zueinander. Die Umkehrung ist im Allgemeinen falsch.

(13.5) Proposition Sei V ein n-dimensionaler K-Vektorraum, und sei $\phi \in \mathrm{End}_K(V)$. Sind $A, B \in \mathscr{M}_{n,K}$ Darstellungsmatrizen von ϕ bezüglich unterschiedlicher Basen von V, dann sind A und B ähnlich.

Beweis: Seien $\mathscr{A}$ und $\mathscr{B}$ Basen von V, so dass $A = \mathscr{M}_{\mathscr{A}}(\phi)$ und $B = \mathscr{M}_{\mathscr{B}}(\phi)$ erfüllt ist. Sei außerdem $T = \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}$ die Matrix des Basiswechsels von A nach B, also die eindeutig bestimmte Matrix $T \in \mathrm{GL}_n(K)$ mit $T\Phi_{\mathscr{A}}(v) = \Phi_{\mathscr{B}}(v)$ für alle $v \in V$. Auf Grund der Transformationsformel aus Satz (11.16) gilt

$$B \quad = \quad \mathscr{M}_{\mathscr{B}}(\phi) \quad = \quad \mathscr{M}_{\mathscr{B}}^{\mathscr{B}}(\phi) \quad = \quad \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}\mathscr{M}_{\mathscr{A}}^{\mathscr{A}}(\phi)\mathscr{T}_{\mathscr{A}}^{\mathscr{B}} \quad = \quad \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}\mathscr{M}_{\mathscr{A}}(\phi)\left(\mathscr{T}_{\mathscr{B}}^{\mathscr{A}}\right)^{-1} \quad = \quad TAT^{-1}. \qquad \square$$

(13.6) Proposition Sei V ein endlich-dimensionaler K-Vektorraum, $\phi \in \mathrm{End}_K(V)$ und $A \in \mathscr{M}_{n,K}$ die Darstellungsmatrix von ϕ bezüglich einer beliebigen Basis $\mathscr{A}$ von V. Genau dann ist $v \in V$ ein Eigenvektor von ϕ zu einem Eigenwert $\lambda \in K$, wenn der Koordinatenvektor $\Phi_{\mathscr{A}}(v)$ ein Eigenvektor von A zum Eigenwert λ ist.

Beweis: Nach Definition der Darstellungsmatrix gilt $A\Phi_{\mathscr{A}}(v) = \mathscr{M}_{\mathscr{A}}(\phi)\Phi_{\mathscr{A}}(v) = \Phi_{\mathscr{A}}(\phi(v))$ für jedes $v \in V$. Sei nun $\lambda \in K$ vorgegeben. Ein Vektor v ist genau dann Eigenvektor von ϕ zum Eigenwert λ, wenn $v \neq 0_V$ und $\phi(v) = \lambda v$ erfüllt ist. Auf Grund der Bijektivitiät und der Linearität der Koordinatenabbildung $\Phi_{\mathscr{A}}$ ist $v \neq 0_V$ äquivalent zu $\Phi_{\mathscr{A}}(v) \neq 0_{K^n}$, außerdem gilt

$$\phi(v) = \lambda v \quad \Leftrightarrow \quad \Phi_{\mathscr{A}}(\phi(v)) = \Phi_{\mathscr{A}}(\lambda v) \quad \Leftrightarrow \quad \Phi_{\mathscr{A}}(\phi(v)) = \lambda\Phi_{\mathscr{A}}(v) \quad \Leftrightarrow \quad A\Phi_{\mathscr{A}}(v) = \lambda\Phi_{\mathscr{A}}(v). \qquad \square$$

Die Proposition zeigt, dass die Eigenwerte von ϕ genau die Eigenwerte der Darstellungsmatrix $\mathscr{M}_{\mathscr{A}}(\phi)$ sind.

Im folgenden beschäftigen wir uns mit der Frage, wie man die Eigenwerte eines Endomorphismus findet. Dafür benötigen wir einige Grundbegriffe und elementare Aussagen über Polynome. Wir nennen ein Polynom $f \in K[x]$ genau dann ***konstant***, wenn $f = 0_K$ oder $\operatorname{grad}(f) = 0$ gilt, wenn f also in K liegt.

(13.7) Satz *(Division mit Rest)*

Seien $f, g \in K[x]$, wobei g nicht-konstant ist. Dann gibt es $q, r \in K[x]$ mit $f = qg + r$, wobei $r = 0_K$ ist oder zumindest $\operatorname{grad}(r) < \operatorname{grad}(g)$ gilt.

Wir verzichten an dieser Stelle auf einen Beweis, weil dieser eher in die Algebra-Vorlesung gehört. Aus dem Schulunterricht ist zumindest für $K = \mathbb{R}$ bekannt, dass die Polynome q und r durch Polynomdivision bestimmt werden können.

Jedem Polynom $f \in K[x]$ kann durch $a \mapsto f(a)$ eine Abbildung $K \to K$ zugeordnet werden, die dadurch zu Stande kommt, dass die Elemente $a \in K$ in die Unbestimmte x eingesetzt werden. Man bezeichnet diese Abbildung auch als die dem Polynom f zugeordnete ***Polynomfunktion***.

Für unendliche Körper gilt allgemein, dass verschiedene Polynome auch verschiedene Polynomfunktionen definieren. Für endliche Körper ist das aber nicht mehr richtig: Beispielsweise definieren die Polynome $f, g \in \mathbb{F}_2[x]$ gegeben durch $f = x$ und $g = x^2$ dieselbe Polynomfunktion, denn es gilt

$$f(\bar{0}) = g(\bar{0}) = \bar{0} \qquad \text{und} \qquad f(\bar{1}) = g(\bar{1}) = \bar{1}.$$

Ein Element $a \in K$ wird ***Nullstelle*** von $f \in K[x]$ genannt, wenn $f(a) = 0_K$ gilt. Man nennt ein Polynom $g \in K[x]$ einen ***Teiler*** von f, wenn ein $h \in K[x]$ mit $f = gh$ existiert. Ist $\operatorname{grad}(g) = 1$, dann nennt man g auch einen ***Linearfaktor*** des Polynoms f. Auch die folgende Aussage ist im Grunde schon aus der Schulmathematik bekannt.

(13.8) Satz Sei $f \in K[x]$ und $a \in K$. Genau dann gilt $f(a) = 0_K$, wenn $x - a$ ein Linearfaktor von f ist.

Beweis: Nach (13.7) gibt es Polynome $g, r \in K[x]$ mit $f = (x-a)g + r$, wobei das Polynom r wegen $r = 0_K$ oder $\operatorname{grad}(r) < \operatorname{grad}(x-a) = 1$ konstant ist. Ist nun a eine Nullstelle von f, dann gilt $r = r(a) = f(a) - (a-a)g(a) = 0_K - 0_K = 0_K$ und somit $f = (x-a)g$. Ist umgekehrt $x - a$ ein Linearfaktor von f, dann gibt es ein $g \in K[x]$ mit $f = (x-a)g$, und es folgt $f(a) = (a-a)g(a) = 0_K$. $\square$

(13.9) Definition Sei $f \in K[x]$ mit $f \neq 0_K$ und $a \in K$ eine Nullstelle von f. Das maximale $r \in \mathbb{N}$ mit der Eigenschaft, dass $(x-a)^r$ ein Teiler von f ist, wird die ***Vielfachheit*** $\mu(f,a)$ der Nullstelle a genannt.

Nach (13.7) gilt also $\mu(f,a) \geq 1$ für jede Nullstelle a von f. Ist $f(a) \neq 0_K$, dann setzen wir $\mu(f,a) = 0$. Das folgende Kriterium ist für die Bestimmung der Vielfachheit einer Nullstelle hilfreich.

(13.10) Proposition Sei $f \in K[x]$ ein Polynom mit einer Zerlegung $f = (x-a)^r g$, wobei $r \in \mathbb{N}_0$ und $g(a) \neq 0_K$ ist. Dann gilt $r = \mu(f,a)$.

Beweis: Die Gleichung $f = (x-a)^r g$ zeigt jedenfalls, dass $\mu(f,a) \geq r$ gilt. Nehmen wir nun an, dass sogar $\mu(f,a) > r$ erfüllt ist. Dann gibt es ein $h \in K[x]$ mit $f = (x-a)^{r+1}h$. Teilt man die Polynomgleichung

$$(x-a)^r g \quad = \quad (x-a)^{r+1}h$$

durch $(x-a)^r$, dann folgt $g = (x-a)h$ und $g(a) = (a-a)h(a) = 0_K$, im Widerspruch zur Voraussetzung $g(a) \neq 0_K$. □

Sei $f \in K[x]$ ein Polynom vom Grad ≥ 1. Man sagt, f ***zerfällt in Linearfaktoren***, wenn es als Produkt von Linearfaktoren geschrieben werden kann. In ausgeschriebener Form bedeutet dies, dass Elemente $c, \lambda_1, ..., \lambda_r \in K$ existieren, so dass

$$f \quad = \quad c\prod_{k=1}^{r}(x-\lambda_k) \qquad \text{gilt.}$$

Ein Körper K wird ***algebraisch abgeschlossen*** genannt, wenn jedes Polynom vom Grad ≥ 1 in $K[x]$ in Linearfaktoren zerfällt. In der Funktionentheorie zeigt man, dass zum Beispiel der Körper $\mathbb{C}$ der komplexen Zahlen diese Eigenschaft besitzt.

Dagegen ist $\mathbb{R}$ nicht algebraisch abgeschlossen, denn das Polynom x^2+1 hat keine Nullstellen in $\mathbb{R}$ und kann deshalb nach (13.8) nicht in Linearfaktoren zerlegt werden. In der Algebra-Vorlesung wird aber gezeigt, dass zu einem Körper K ein algebraisch abgeschlossener Erweiterungskörper existiert. Im Fall $K = \mathbb{R}$ ist dies gerade der Körper $\mathbb{C}$.

Nun werden wir sehen, inwiefern Polynome bei der Bestimmung der Eigenwerte einer Matrix weiterhelfen.

(13.11) Definition Für jede Matrix $A \in \mathscr{M}_{n,K}$ nennt man

$$\chi_A \quad = \quad (-1)^n \det(A - xE^{(n)}) \quad = \quad \det(xE^{(n)} - A) \quad \in K[x]$$

das ***charakteristische Polynom*** von A.

Bei der Definition von χ_A gibt es ein technisches Problem: Wir haben die Determinante nur für Matrizen über Körpern definiert. Aber $A - xE^{(n)}$ ist eine Matrix über $K[x]$, und dies ist ein Ring, aber kein Körper. In der Algebra-Vorlesung

wird aber gezeigt, dass $K[x]$ in einem Körper $K(x)$ enthalten ist, dem sogenannten ***rationalen Funktionenkörper*** über K, dessen Elemente Quotienten f/g mit $f, g \in K[x]$, $g \neq 0$ sind. Wir können $A - xE^{(n)}$ also als Matrix über dem Körper $K(x)$ betrachten, und dann ist wieder alles in Ordnung.

(13.12) Satz Die Eigenwerte einer Matrix $A \in \mathscr{M}_{n,K}$ sind genau die Nullstellen des charakteristischen Polynoms χ_A.

Beweis: Für jedes $\lambda \in K$ gilt $\mathrm{Eig}(A, \lambda) = \ker(A - \lambda E^{(n)})$. Genau dann ist λ ein Eigenwert von A, wenn die Ungleichung $\ker(A - \lambda E^{(n)}) \neq \{0_V\}$ gilt, siehe Proposition (13.3). Nach dem Dimensionssatz für lineare Abbildungen gilt weiter

$$\dim\ker(A - \lambda E^{(n)}) > 0 \quad \Leftrightarrow \quad \mathrm{rg}(A - \lambda E^{(n)}) < n \quad \Leftrightarrow \quad \det(A - \lambda E^{(n)}) = 0_K \quad \Leftrightarrow \quad \chi_A(\lambda) = 0_K \qquad \square$$

(13.13) Definition Ist V ein endlich-dimensionaler K-Vektorraum, $\phi \in \mathrm{End}_K(V)$ und $A \in \mathscr{M}_{n,K}$ die Darstellungsmatrix von V bezüglich einer beliebig gewählten Basis, dann bezeichnen wir $\chi_\phi = \chi_A$ als ***charakteristisches Polynom*** von ϕ.

(13.14) Proposition Das charakteristische Polynom χ_ϕ ist unabhängig von der gewählten Basis des Vektorraums V.

Beweis: Sind $A, B \in \mathscr{M}_{n,K}$ die Darstellungsmatrizen von ϕ bezüglich verschiedener Basen, dann sind A und B nach Proposition (13.5) ähnlich. Es gibt also ein $T \in \mathrm{GL}_n(K)$ mit $B = TAT^{-1}$. Auf Grund der Multiplikativität der Determinantenfunktion folgt

$$\begin{aligned} \chi_B &= \det(xE^{(n)} - B) = \det(T(xE^{(n)})T^{-1} - TAT^{-1}) = \det(T(xE^{(n)} - A)T^{-1}) \\ &= \det(T)\det(xE^{(n)} - A)\det(T)^{-1} = \det(xE^{(n)} - A) = \chi_A. \end{aligned} \qquad \square$$

(13.15) Folgerung Auch für jeden Endomorphismus $\phi \in \mathrm{End}_K(V)$ eines endlich-dimensionalen K-Vektorraums V gilt: Die Eigenwerte von ϕ sind genau die Nullstellen des Polynoms χ_ϕ.

Beweis: Sei A die Darstellungsmatrix von ϕ bezüglich einer beliebigen Basis von V. Dann gilt $\chi_\phi = \chi_A$ nach Definition. Auf Grund von Proposition (13.6) sind darüber hinaus die Eigenwerte von ϕ genau die Eigenwerte von A. Also sind die Eigenwerte von ϕ nach Satz (13.12) genau die Nullstellen von χ_A und damit auch genau die Nullstellen von χ_ϕ. $\square$

Als Anwendungsbeispiel bestimmen wir die Eigenwerte der Matrix

$$A \quad = \quad \begin{pmatrix} -2 & -5 & 10 \\ -20 & -17 & 40 \\ -10 & -10 & 23 \end{pmatrix} \quad \in \quad \mathscr{M}_{3,\mathbb{R}}$$

mit Hilfe des charakteristischen Polynoms χ_A. Zunächst ermitteln wir dieses Polynom mit Hilfe der Sarrus-Regel.

$$\chi_A \quad = \quad \det(xE^{(3)} - A) \quad = \quad \det\left(\begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix} - \begin{pmatrix} -2 & -5 & 10 \\ -20 & -17 & 40 \\ -10 & -10 & 23 \end{pmatrix}\right) \quad = \quad \det\begin{pmatrix} x+2 & 5 & -10 \\ 20 & x+17 & -40 \\ 10 & 10 & x-23 \end{pmatrix}$$

$$= \quad (x+2)(x+17)(x-23) + 5\cdot(-40)\cdot 10 + (-10)\cdot 20\cdot 10 - 10\cdot(x+17)\cdot(-10) - 10\cdot(-40)\cdot(x+2)$$

$$-(x-23)\cdot 20\cdot 5 \quad = \quad (x^2+2x+17x+34)(x-23) - 2000 - 2000 + 100x + 1700 + 400x + 800 - 100x + 2300$$

$$= \quad x^3 + 19x^2 + 34x - 23x^2 - 437x - 782 + 400x + 800 \quad = \quad x^3 - 4x^2 - 3x + 18.$$

Durch probeweises Einsetzen von 0, ±1, ±2,... in das Polynom χ_A finden wir die Nullstelle -2. Nach Satz (13.8) ist $x+2$ ein Linearfaktor von χ_A. Durch Polynomdivision erhält man die Zerlegung $\chi_A = (x+2)(x^2-6x+9)$. Die Nullstellen des quadratischen Faktors bestimmt man nun mit der p-q-Formel aus der Schulmathematik: Die Diskriminante des Polynoms $g = x^2-6x+9$ mit $p=-6$ und $q=9$ ist $d = p^2-4q = (-6)^2-4\cdot 9 = 36-36 = 0$. Die beiden Nullstellen von g sind mit Vielfachheiten gegeben durch $-\frac{1}{2}p \pm \frac{1}{2}\sqrt{d}$; wegen $d=0$ ist $-\frac{1}{2}p = -\frac{1}{2}\cdot(-6) = 3$ eine doppelte Nullstelle von g. Es gilt also $g = (x-3)^2$ und somit $\chi_A = (x+2)(x-3)^2$.

Also sind -2 und 3 die beiden Eigenwerte von A. Die beiden zugehörigen Eigenräume lassen sich wiederum mit dem Gaußverfahren ermitteln. Man erhält

$$\mathrm{Eig}(A,-2) = \langle \left\{ \begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix} \right\rangle_K \quad \text{und} \quad \mathrm{Eig}(A,3) = \langle \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} \right\rangle_K.$$

(13.16) Definition Sind $\lambda_1, ..., \lambda_n \in K$, dann bezeichnen wir mit $\mathrm{diag}(\lambda_1, ..., \lambda_n)$ die Matrix $D = (d_{ij})$ mit den Einträgen

$$d_{ij} \quad = \quad \begin{cases} \lambda_k & \text{falls } i = j = k \\ 0 & \text{falls } i \neq j. \end{cases}$$

Eine Matrix dieser Form wird ***Diagonalmatrix*** genannt. Man bezeichnet eine Matrix $A \in \mathscr{M}_{n,K}$ als ***diagonalisierbar***, wenn sie ähnlich zu einer Diagonalmatrix ist.

(13.17) Definition Einen Endomorphismus ϕ eines endlich-dimensionalen K-Vektorraums V heißt ***diagonalisierbar***, wenn eine Basis von V existiert, so dass die Darstellungsmatrix von ϕ bezüglich dieser Basis eine Diagonalmatrix ist.

(13.18) Proposition Sei V ein endlich-dimensionaler K-Vektorraum, $\phi \in \mathrm{End}_K(V)$ und $A \in \mathscr{M}_{n,K}$ die Darstellungsmatrix von ϕ bezüglich einer geordneten Basis von V. Genau dann ist A diagonalisierbar, wenn ϕ diagonalisierbar ist.

Beweis: Sei $\mathscr{A}$ eine Basis von V, so dass $A = \mathscr{M}_{\mathscr{A}}(\phi)$ erfüllt ist.

„⇐“ Weil ϕ nach Voraussetzung diagonalisierbar ist, gibt es eine Basis $\mathscr{B}$ von V, so dass $D = \mathscr{M}_{\mathscr{B}}(\phi)$ eine Diagonalmatrix ist. Die Matrizen A und D sind also die Darstellungsmatrizen von ϕ bezüglich der Basen $\mathscr{A}, \mathscr{B}$. Nach Proposition (13.5) sind A und D ähnlich, und damit ist A nach Definition diagonalisierbar.

„⇒“ Ist A diagonalisierbar, dann gibt es ein $T \in \mathrm{GL}_n(K)$ mit der Eigenschaft, dass $D = TAT^{-1}$ eine Diagonalmatrix ist. Nach Lemma (13.19) (siehe unten) existiert eine Basis $\mathscr{B}$ mit der Eigenschaft, dass $T = \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}$ erfüllt ist. Auf Grund des Satzes (11.16) vom Basiswechsel erhalten wir

$$D \quad = \quad TAT^{-1} \quad = \quad \mathscr{T}_{\mathscr{B}}^{\mathscr{A}} \mathscr{M}_{\mathscr{A}}(\phi)(\mathscr{T}_{\mathscr{B}}^{\mathscr{A}})^{-1} \quad = \quad \mathscr{T}_{\mathscr{B}}^{\mathscr{A}} \mathscr{M}_{\mathscr{A}}(\phi)\mathscr{T}_{\mathscr{A}}^{\mathscr{B}} \quad = \quad \mathscr{M}_{\mathscr{B}}(\phi).$$

Es gibt also eine geordnete Basis $\mathscr{B}$ von V mit der Eigenschaft, dass die Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}(\phi)$ eine Diagonalmatrix ist. Also ist ϕ ein diagonalisierbarer Endomorphismus. □

Beim Beweis von Proposition (13.18) wurde verwendet

(13.19) Lemma Sei V ein endlich-dimensionaler K-Vektorraum, $\mathscr{A}$ eine geordnete Basis von V und $T \in \mathrm{GL}_n(K)$ eine invertierbare Matrix. Dann gibt es eine geordnete Basis $\mathscr{B}$ von V mit $T = \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}$.

Beweis: Die Gleichung $T = \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}$ ist äquivalent zu $T^{-1} = \mathscr{T}_{\mathscr{A}}^{\mathscr{B}}$, nach Proposition (11.15) (ii). Sei $C = (c_{ij}) = T^{-1}$. Sei nun $\mathscr{A} = (v_1, ..., v_n)$, und sei $\mathscr{B} = (w_1, ..., w_n)$ die gesuchte Basis. Die Gleichung $C = \mathscr{T}_{\mathscr{A}}^{\mathscr{B}}$ ist nach Definition der Transformationsformel gerade äquivalent dazu, dass $\Phi_{\mathscr{A}}(w_j)$ für $1 \le j \le n$ die Spalten von C sind. Dies ist offenbar genau dann der Fall, wenn die Elemente von $\mathscr{B}$ durch

$$w_j \quad = \quad \sum_{i=1}^{n} c_{ij} v_i \qquad \text{für} \quad 1 \le j \le n$$

definiert sind, denn $(c_{1j}, ..., c_{nj})$ ist genau der Koordinatenvektor von $\sum_{i=1}^{n} c_{ij} v_i$ bezüglich $\mathscr{A}$.

Wir müssen nun noch zeigen, dass die so definierten Vektoren $w_1, ..., w_n$ tatsächlich eine Basis von V bilden. Für $1 \le k \le n$ gilt jeweils

$$\sum_{j=1}^{n} t_{jk} w_j \quad = \quad \sum_{j=1}^{n} \sum_{i=1}^{n} t_{jk} c_{ij} v_i.$$

Nun ist $\sum_{j=1}^{n} t_{jk} c_{ij}$ genau der Eintrag von CT an der Stelle (i,k). Wegen $CT = E^{(n)}$ ist der Eintrag also gleich δ_{ik}. Es folgt

$$\sum_{j=1}^{n} t_{jk} w_j \quad = \quad \sum_{i=1}^{n} \delta_{ik} v_i \quad = \quad v_k \qquad \text{für} \quad 1 \le k \le n.$$

Dies zeigt, dass $v_1, ..., v_n$ in $\langle w_1, ..., w_n \rangle_K$ enthalten sind. Weil $\{v_1, ..., v_n\}$ eine Basis von V ist, folgt daraus, dass $\{w_1, ..., w_n\}$ ein Erzeugendensystem von V ist, wegen $n = \dim V$ sogar eine Basis, nach Satz (9.9). Damit ist dann das Tupel $\mathscr{B} = (w_1, ..., w_n)$ eine geordnete Basis von V mit der gewünschten Eigenschaft $\mathscr{T}_{\mathscr{B}}^{\mathscr{A}} = T$. □

Wir können nun ein neues Kriterium für die Diagonalisierbarkeit herleiten.

(13.20) Proposition Sei $V \neq \{0_V\}$ ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$. Dann sind die folgenden Aussagen äquivalent:

(i) Der Endomorphismus ϕ ist diagonalisierbar.
(ii) Der Vektorraum V besitzt eine Basis bestehend aus Eigenvektoren von ϕ.

Beweis: „(i) ⇒ (ii)“ Nach Voraussetzung gibt es eine Basis $\mathscr{A} = (v_1, ..., v_n)$ von V mit der Eigenschaft, dass $D = \mathscr{M}_{\mathscr{A}}(\phi)$ eine Diagonalmatrix ist, $D = \mathrm{diag}(\lambda_1, ..., \lambda_n)$ mit $\lambda_k \in K$ für $1 \leq k \leq n$. Der k-te Spaltenvektor von D ist jeweils das λ_k-fache des k-ten Einheitsvektors e_k. Es folgt

$$De_k = \lambda_k e_k \quad \Leftrightarrow \quad \mathscr{M}_{\mathscr{A}}(\phi)\Phi_{\mathscr{A}}(v_k) = \lambda_k \Phi_{\mathscr{A}}(v_k) \quad \Leftrightarrow \quad \Phi_{\mathscr{A}}(\phi(v_k)) = \Phi_{\mathscr{A}}(\lambda_k v_k) \quad \Leftrightarrow \quad \phi(v_k) = \lambda_k v_k$$

für $1 \leq k \leq n$, wobei im letzten Schritt die Bijektivität von $\Phi_{\mathscr{A}}$ verwendet wurde. Als Element einer Basis ist $v_k \neq 0_V$; zusammen mit der Gleichung $\phi(v_k) = \lambda_k v_k$ zeigt dies, dass $\mathscr{A}$ aus Eigenvektoren von ϕ besteht.

„(ii) ⇒ (i)“ Sei $\mathscr{A} = (v_1, ..., v_n)$ eine Basis von V, wobei v_k jeweils ein Eigenvektor von ϕ zum Eigenwert λ_k ist, für $1 \leq k \leq n$. Außerdem sei $D = \mathscr{M}_{\mathscr{A}}(\phi)$. Dann gilt jeweils $\phi(v_k) = \lambda_k v_k$, und die Rechnung aus dem vorherigen Absatz hat gezeigt, dass dies äquivalent zu $De_k = \lambda_k e_k$ ist. Die k-te Spalte von D ist also gleich $\lambda_k e_k$, für $1 \leq k \leq n$. Daraus folgt $D = \mathrm{diag}(\lambda_1, ..., \lambda_n)$, also ist D eine Diagonalmatrix und ϕ damit diagonalisierbar. □

Als nächstes zeigen wir, dass der Vektorraum V bezüglich eines diagonalisierbaren Endomorphismus in Eigenräume zerlegt werden kann. Die folgende Aussage dient zur Vorbereitung des Beweises.

(13.21) Proposition Sei $r \in \mathbb{N}$, ϕ ein Endomorphismus eines K-Vektorraums V, und seien $\lambda_1, ..., \lambda_r$ verschiedene Elemente des Körpers K. Dann gilt

$$\mathrm{Eig}(\phi, \lambda_k) \cap \left(\sum_{\ell \neq k} \mathrm{Eig}(\phi, \lambda_\ell) \right) \quad = \quad \{0_V\} \qquad \text{für} \quad 1 \leq k \leq r.$$

Beweis: Wir beweisen die Aussage durch vollständige Induktion über r. Im Fall $r = 1$ ist nichts zu zeigen, weil in diesem Fall $\sum_{\ell \neq 1} \mathrm{Eig}(\phi, \lambda_\ell)$ gleich $\{0_V\}$ ist. Sei nun $r \in \mathbb{N}$ beliebig, und setzen wir die Aussage für r voraus. Seien $\lambda_1, ..., \lambda_{r+1}$ verschiedene Elemente aus K; weil wir diese beliebig vertauschen können, genügt es, $\sum_{\ell=1}^{r} \mathrm{Eig}(\phi, \lambda_\ell) \cap \mathrm{Eig}(\phi, \lambda_{r+1}) = \{0_V\}$ zu zeigen. Auf Grund der Induktionsvoraussetzung können wir Satz (10.4) auf die Untervektorräume $U_\ell = \mathrm{Eig}(\phi, \lambda_\ell)$ mit $1 \leq \ell \leq r$ anwenden und kommen zu dem Ergebnis, dass diese eine direkte Summe bilden. Nach Folgerung (10.7) können wir Basen der Eigenräume U_ℓ wählen und diese zu einer Basis $B = \{v_1, ..., v_m\}$ von $U = \bigoplus_{\ell=1}^{r} U_\ell$ zusammensetzen, wobei $m = \dim U$ ist. Dann gilt nach Konstruktion für $1 \leq k \leq m$ jeweils $\phi(v_k) = \mu_k v_k$, mit $\mu_k \in \{\lambda_1, ..., \lambda_r\}$.

Nehmen wir nun an, dass U einen Vektor v aus $\mathrm{Eig}(\phi, \lambda_{r+1})$ mit $v \neq 0_V$ enthält. Stellen wir v als Linearkombination von B dar, $v = \sum_{k=1}^{m} \alpha_k v_k$ mit $\alpha_1, ..., \alpha_m \in K$, dann gilt

$$\begin{aligned}\sum_{k=1}^{m} \mu_k \alpha_k v_k &= \sum_{k=1}^{m} \alpha_k \phi(v_k) = \phi\left(\sum_{k=1}^{m} \alpha_k v_k\right) = \phi(v) = \lambda_{r+1} v \\ &= \lambda_{r+1}\left(\sum_{k=1}^{m} \alpha_k v_k\right) = \sum_{k=1}^{m} \lambda_{r+1} \alpha_k v_k.\end{aligned}$$

Durch Umstellen erhalten wir $\sum_{k=1}^{m} (\mu_k - \lambda_{r+1}) \alpha_k v_k = 0_V$. Wegen $\mu_k \in \{\lambda_1, ..., \lambda_r\}$ gilt jeweils $\mu_k - \lambda_{r+1} \neq 0$ für $1 \leq k \leq m$, und wegen $v \neq 0_V$ ist $\alpha_k \neq 0$ für mindestens ein k. Der Nullvektor kann also als Linearkombination des $(v_1, ..., v_m)$ dargestellt werden, ohne dass alle Koeffizienten $(\mu_k - \lambda_{r+1})\alpha_k$ gleich null sind. Dies steht im Widerspruch zur Basiseigenschaft von B. Die Annahme war also falsch, und es gilt $U \cap \mathrm{Eig}(\phi, \lambda_{r+1}) = \{0_V\}$. □

Mit diesen Ergebnissen erhalten wir ein neues Kriterium für die Diagonalisierbarkeit eines Endomorphismus.

(13.22) Proposition Sei $V \neq \{0_V\}$ endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$. Dann sind die folgenden Aussagen äquivalent:

(i) Der Endomorphismus ϕ ist diagonalisierbar.

(ii) Es gibt verschiedene Elemente $\lambda_1, ..., \lambda_r \in K$, so dass

$$V = \bigoplus_{\ell=1}^{r} \mathrm{Eig}(\phi, \lambda_\ell) \qquad \text{erfüllt ist.}$$

Beweis: „(i) ⇒ (ii)“ Auf Grund der Voraussetzung existiert nach Proposition (13.20) eine Basis $\mathscr{A} = \{v_1, ..., v_n\}$ von V bestehend aus Eigenvektoren. Seien $\lambda_1, ..., \lambda_r$ die verschiedenen Eigenwerte von ϕ. Weil alle Elemente der Basis Eigenvektoren sind, gibt es für jedes $k \in \{1, ..., n\}$ ein $\ell \in \{1, ..., r\}$ mit $\phi(v_k) = \lambda_\ell v_k$. Es gilt dann also $v_k \in \mathrm{Eig}(\phi, \lambda_\ell)$. Setzen wir $U = \sum_{\ell=1}^{r} \mathrm{Eig}(\phi, \lambda_\ell)$, dann gilt insgesamt $\mathscr{A} \subseteq U$. Weil $\mathscr{A}$ eine Basis und U ein Untervektorraum von V ist, stimmt V mit der Summe U ein, und nach Proposition (13.21) ist dies eine direkte Summe.

„(ii) ⇒ (i)“ Für jedes $\ell \in \{1, ..., r\}$ sei $\mathscr{A}_\ell$ eine Basis von $\mathrm{Eig}(\phi, \lambda_\ell)$. Auf Grund der direkten Summenzerlegung ist dann $\mathscr{A} = \bigcup_{\ell=1}^{r} \mathscr{A}_\ell$ nach Folgerung (10.7) eine Basis von V. Jedes $\mathscr{A}_\ell$ besteht aus Eigenvektoren von ϕ, somit auch die Basis $\mathscr{A}$. Nach Proposition (13.20) folgt daraus die Diagonalisierbarkeit von ϕ. □

(13.23) Definition Sei V ein endlich-dimensionaler K-Vektorraum, ϕ ein Endomorphismus von V und $\lambda \in K$ ein Eigenwert von ϕ.

(i) Die Vielfachheit $\mu(\chi_\phi, \lambda)$ von λ als Nullstelle des Polynoms χ_ϕ bezeichnet man als ***algebraische*** Vielfachheit $\mu_a(\phi, \lambda)$ des Eigenwerts λ.

(ii) Die Eigenraum-Dimension $\mu_g(\phi, \lambda) = \dim \mathrm{Eig}(\phi, \lambda)$ nennt man die ***geometrische*** Vielfachheit von λ.

Für eine quadratische Matrix $A \in \mathscr{M}_{n,K}$ definiert man algebraische und geometrische Vielfachheit eines Eigenwerts λ auf analoge Weise: Man setzt $\mu_a(A,\lambda) = \mu(\chi_A,\lambda)$ und $\mu_g(A,\lambda) = \dim \mathrm{Eig}(A,\lambda)$.

In Beweisen ist es oft günstig, wenn die algebraische und geometrische Vielfachheit auch für Nicht-Eigenwerte eines Endomorphismus ϕ definiert sind, weil dadurch lästige Fallunterscheidungen vermieden werden. Wenn $\lambda \in K$ kein Eigenwert von ϕ ist, dann setzt man $\mu_a(\phi,\lambda) = \mu_g(\phi,\lambda) = 0$.

(13.24) Proposition Sei V ein n-dimensionaler K-Vektorraum, $\phi : V \to V$ ein Endomorphismus und $\lambda \in K$ ein Eigenwert mit algebraischer Vielfachheit μ_a und geometrischer Vielfachheit μ_g. Dann gilt $1 \le \mu_g \le \mu_a$.

Beweis: Wir haben bereits gesehen, dass λ genau dann ein Eigenwert ist, wenn $\mathrm{Eig}(\phi,\lambda) \neq \{0_V\}$ ist. Deshalb gilt $\mu_g \ge 1$. Sei nun $(v_1,\ldots,v_r)$ eine Basis von $\mathrm{Eig}(\phi,\lambda)$, die wir durch $v_{r+1},\ldots,v_n$ zu einer Basis $\mathscr{A}$ von V ergänzen. Wegen $\phi(v_i) = \lambda v_i$ für $1 \le i \le r$ hat A die Form

$$A \quad = \quad \begin{pmatrix} \lambda E^{(r)} & B \\ 0 & C \end{pmatrix}$$

mit geeignet gewählten Matrizen $B \in \mathscr{M}_{r\times(n-r),K}$ und $C \in \mathscr{M}_{n-r,K}$. Sei nun $\chi \in K[x]$ das charakteristische Polynom von ϕ. Es gilt dann

$$\chi \quad = \quad \det(xE^{(n)} - A) \quad = \quad \det\begin{pmatrix} (x-\lambda)E^{(r)} & -B \\ 0 & xE^{(n-r)} - C \end{pmatrix} \quad = \quad (x-\lambda)^r \det(xE^{(n-r)} - C) \quad = \quad (x-\lambda)^r \chi_C\,,$$

wobei wir im vorletzten Schritt Satz (12.23) für Blockmatrizen angewendet haben. Dies zeigt, dass Vielfachheit von λ als Nullstelle von χ mindestens gleich r ist, also $\mu_g = r \le \mu_a$ gilt. □

(13.25) Satz Sei $n \in \mathbb{N}$, V ein n-dimensionaler K-Vektorraum, ϕ ein Endomorphismus von V und $\chi \in K[x]$ sein charakteristisches Polynom. Dann sind die folgenden Aussagen äquivalent:

(i) Der Endomorphismus ϕ ist diagonalisierbar

(ii) Der Vektorraum V besitzt eine Basis bestehend aus Eigenvektoren von ϕ.

(iii) Das Polynom χ_ϕ zerfällt in Linearfaktoren, und für jeden Eigenwert λ von ϕ stimmen algebraische und geometrische Vielfachheit überein.

(iv) Es gibt $\lambda_1,\ldots,\lambda_r \in K$, so dass $V = \mathrm{Eig}(\phi,\lambda_1) \oplus \ldots \oplus \mathrm{Eig}(\phi,\lambda_r)$ gilt.

Beweis: Die Äquivalenz von (i), (ii) und (iv) wurde bereits bewiesen.

„(i) ⇒ (iii)“ Sei $\mathscr{A} = (v_1,\ldots,v_n)$ eine Basis, und seien $\lambda_1,\ldots,\lambda_n \in K$, so dass $A = \mathscr{M}_{\mathscr{A}}(\phi) = \mathrm{diag}(\lambda_1,\ldots,\lambda_n)$ gilt. Für das charakteristische Polynom gilt dann

$$\chi \quad = \quad \chi_A \quad = \quad \det(xE^{(n)} - A) \quad = \quad \det(\mathrm{diag}(x-\lambda_1,\ldots,x-\lambda_n)) \quad = \quad \prod_{i=1}^{n}(x-\lambda_i) \quad ,$$

es zerfällt also in Linearfaktoren. Zu zeigen bleibt, dass für jeden Eigenwert λ_i jeweils algebraische und geometrische Vielfachheit übereinstimmen. Für jeden Eigenwert λ von ϕ sei $S(\lambda) = \{i \mid \lambda_i = \lambda\}$. Dann können wir das charakteristische Polynom in der Form $\chi = gh$ mit

$$g \quad = \quad \prod_{i \in S(\lambda)} (x - \lambda_i) \quad = \quad (x-\lambda)^{|S(\lambda)|} \qquad \text{und} \qquad h \quad = \quad \prod_{i \notin S(\lambda)} (x - \lambda_i)$$

zerlegen. Wegen $h(\lambda) \neq 0$ ist $\mu = |S(\lambda)|$ die Vielfachheit der Nullstelle λ von f, also die algebraische Vielfachheit des Eigenwerts λ. Für jedes $i \in S(\lambda)$ ist aber auch v_i ein Eigenvektor zum Eigenwert λ, es gilt also $\dim \mathrm{Eig}(\phi, \lambda) \geq \mu$. Weil die geometrische Vielfachheit nach Proposition (13.24) immer durch die algebraische Vielfachheit beschränkt ist, folgt $\mathrm{Eig}(\phi, \lambda) = \mu$.

„(iii) ⇒ (iv)“ Sei $\chi = \prod_{i=1}^{r} (x - \lambda_i)^{\mu_i}$ eine Zerlegung des charakteristischen Polynoms in Linearfaktoren, wobei die Nullstellen $\lambda_1, \ldots, \lambda_r \in K$ paarweise verschieden und $\mu_i \in \mathbb{N}$ jeweils die Vielfachheiten der Nullstellen λ_i sind. Wegen $\mathrm{grad}(\chi) = n$ gilt $\sum_{i=1}^{r} \mu_i = n$.

Für jedes $i \in \{1, \ldots, r\}$ definieren wir nun $U_i = \mathrm{Eig}(\phi, \lambda_i)$, außerdem sei $V_r = \sum_{i=1}^{r} U_i$. Da algebraische und geometrische Vielfachheit übereinstimmen, gilt $\mu_i = \dim U_i$ für $1 \leq i \leq r$. Nach Proposition (13.21) ist der Durchschnitt von U_i mit $\sum_{j \neq i} U_j$ jeweils gleich $\{0_V\}$. Dies zeigt, dass V_r die *direkte* Summe der Untervektorräume U_i ist. Nach Folgerung (10.7) erhalten wir

$$\dim V_r \quad = \quad \sum_{i=1}^{r} \dim U_i \quad = \quad \sum_{i=1}^{r} \mu_i \quad = \quad n \quad = \quad \dim V.$$

Aus $V_r \subseteq V$ und $\dim V_r = \dim V$ wiederum folgt $V = V_r$. □

Die Diagonalisierbarkeitskriterien lassen sich ohne großen Aufwand auf Matrizen übertragen. Hier gilt entsprechend

(13.26) Folgerung Für jede Matrix $A \in \mathscr{M}_{n,K}$ sind folgende Aussagen äquivalent.

(i) Die Matrix A ist diagonalisierbar.

(ii) Der Vektorraum K^n besitzt eine Basis bestehend aus Eigenvektoren von A.

(iii) Das Polynom χ_A zerfällt in Linearfaktoren, und es gilt $\mu_a(A, \lambda) = \mu_g(A, \lambda)$ für jeden Eigenwert λ von A.

(iv) Es gibt $\lambda_1, \ldots, \lambda_r \in K$, so dass $K^n = \mathrm{Eig}(A, \lambda_1) \oplus \ldots \oplus \mathrm{Eig}(A, \lambda_r)$ gilt.

Beweis: Sei ϕ_A der Endomorphismus von K^n gegeben durch $\phi_A(v) = Av$. Dann ist A die Darstellungsmatrix von ϕ_A bezüglich der Einheitsbasis $\mathscr{E}_n$ von K^n, siehe Proposition (11.8). Somit ist (i) nach Proposition (13.18) äquivalent zur Diagonalisierbarkeit von ϕ_A, also zur Ausage (i) in Satz (13.25) für den Endomorphismus ϕ_A. Ebenso leicht überprüft man mit Hilfe der Übereinstimmungen $\mathrm{Eig}(A, \lambda_i) = \mathrm{Eig}(\phi_A, \lambda_i)$ und $\chi_A = \chi_{\phi_A}$, dass die Aussagen (ii),(iii),(iv) äquivalent zu ihrem jeweiligen Pendant in Satz (13.25) sind. Damit ist die Äquivalenz der Aussagen (i) bis (iv) auf Satz (13.25) zurückgeführt. □

Wir demonstrieren die Anwendung des Diagonalisierbarkeitskriteriums an einem etwas größeren Rechenbeispiel und testen die Matrix

$$A \quad = \quad \begin{pmatrix} -2 & -10 & 0 & -40 \\ -24 & -13 & -8 & -68 \\ 15 & 30 & 3 & 120 \\ 6 & 4 & 2 & 20 \end{pmatrix}$$

auf Diagonalisierbarkeit über dem Körper $K = \mathbb{Q}$. (Das ist die Matrix vom Beginn des Kapitels.) Wir beginnen mit der Bestimmung des charakteristischen Polynoms. Durch Anwendung des Laplaceschen Entwicklungssatzes erhalten wir

$$\chi_A \quad = \quad \det(xE^{(4)} - A) \quad = \quad \det \begin{pmatrix} x+2 & 10 & 0 & 40 \\ 24 & x+13 & 8 & 68 \\ -15 & -30 & x-3 & -120 \\ -6 & -4 & -2 & x-20 \end{pmatrix} \quad =$$

$$(x+2) \cdot \det \begin{pmatrix} x+13 & 8 & 68 \\ -30 & x-3 & -120 \\ -4 & -2 & x-20 \end{pmatrix} - 10 \cdot \det \begin{pmatrix} 24 & 8 & 68 \\ -15 & x-3 & -120 \\ -6 & -2 & x-20 \end{pmatrix} - 40 \cdot \det \begin{pmatrix} 24 & x+13 & 8 \\ -15 & -30 & x-3 \\ -6 & -4 & -2 \end{pmatrix}$$

$$= \quad (x+2)(x^3 - 10x^2 + 33x - 36) + (-10)(24x^2 - 24x - 144) + (-40)(-6x^2 + 6x + 36)$$

$$= \quad x^4 - 8x^3 + 13x^2 + 30x - 72.$$

Als nächstes bestimmen wir die Eigenwerte von A, also die Nullstellen von χ_A. Durch probeweises Einsetzen findet man die Nullstelle $\lambda_1 = -2$, und Polynomdivision liefert die Zerlegung $\chi_A = (x+2)(x^3 - 10x^2 + 33x - 36)$. Erneutes probeweises Einsetzen in den Faktor $g = x^3 - 10x^2 + 33x - 36$ vom Grad 3 liefert die Nullstelle $\lambda_2 = 3$. Durch Polynomdivision erhalten wir $g = (x-3)(x^2 - 7x + 12)$. Die Nullstellen des quadratischen Faktors können wir nun durch Anwendung der p-q-Formel (auf $p = -7$, $q = 12$) ermitteln: Die Diskriminante des quadratischen Polynoms ist $d = p^2 - 4q = (-7)^2 - 4 \cdot 12 = 49 - 48 = 1$, die Nullstellen somit $-\frac{1}{2}p \pm \frac{1}{2}\sqrt{d} = \frac{7}{2} \pm \frac{1}{2}$, also $\lambda_3 = 3$ und $\lambda_4 = 4$. Insgesamt erhalten wir damit die Zerlegung

$$\chi_A \quad = \quad (x+2)(x-3)^2(x-4).$$

Die Eigenwerte von A sind also -2, 3 und 4, mit den algebraischen Vielfachheiten $\mu_a(A,-2) = 1$, $\mu_a(A,3) = 2$ und $\mu_a(A,4) = 2$. Die Gleichung zeigt auch, dass χ_A in Linearfaktoren zerfällt. Damit haben wir bereits einen Teil des Diagonalisierbarkeitskriteriums verifiziert.

Nun müssen wir noch die geometrischen Vielfachheiten der Eigenwerte bestimmen. Nach Proposition (13.24) gilt $1 \leq \mu_g(A,\lambda) \leq \mu_a(A,\lambda)$ für jeden Eigenwert λ von A. Wegen $\mu_a(A,-2) = 1$ folgt daraus $\mu_g(A,-2) = 1$, und ebenso erhalten wir $\mu_g(A,4) = 1$. Für $\mu_g(A,3)$ sind wegen $\mu_a(A,3) = 2$ noch zwei Möglichkeiten offen, nämlich $\mu_g(A,3) \in \{1,2\}$. Um festzustellen, welcher Fall vorliegt, bestimmen wir die Dimension von $\mathrm{Eig}(A,3) = \ker(A - 3E^{(4)})$ mit dem

Gaußverfahren.

$$A-3E^{(4)} = \begin{pmatrix} -5 & -10 & 0 & -40 \\ -24 & -16 & -8 & -68 \\ 15 & 30 & 0 & 120 \\ 6 & 4 & 2 & 17 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 2 & 0 & 8 \\ -6 & -4 & -2 & -17 \\ 1 & 2 & 0 & 8 \\ 6 & 4 & 2 & 17 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 2 & 0 & 8 \\ -6 & -4 & -2 & -17 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 2 & 0 & 8 \\ 0 & 8 & -2 & 31 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Die letzte Matrix liegt in ZSF vor, mit Zeilenrang $r = 2$. Durch Anwendung von Satz (10.16) erhalten wir die geometrische Vielfachheit $\mu_g(A,3) = \dim \mathrm{Eig}(A,3) = \dim \ker(A-3E^{(4)}) = 4-r = 4-2 = 2 = \mu_a(A,3)$. Insgesamt ist damit $\mu_g(A,\lambda) = \mu_a(A,\lambda)$ für alle Eigenwert λ der Matrix erfüllt. Dass χ_A über $\mathbb{Q}$ in Linearfaktoren zerfällt, haben wir bereits oben festgestellt. Nach Folgerung (13.26) ist A also eine diagonalisierbare Matrix.

Betrachten wir nun noch zwei Beispiele, in denen das Diagonalisierbarkeitskriterium nicht erfüllt ist. Beispielsweise ist die Matrix

$$B \quad = \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

über dem Körper $K = \mathbb{R}$ nicht diagonalisierbar. Zwar zerfällt das charakteristsiche Polynom wegen

$$\chi_B \quad = \quad \det(xE^{(2)} - B) \quad = \quad \det\begin{pmatrix} x-1 & 1 \\ 0 & x-1 \end{pmatrix} \quad = \quad (x-1)^2$$

über $\mathbb{R}$ in Linearfaktoren. Wie man aber leicht überprüft, gilt $\mathrm{Eig}(B,1) = \langle e_1 \rangle_{\mathbb{R}}$, der Eigenraum von B zum Eigenwert 1 ist also nur eindimensional. Es gilt also $\mu_g(B,1) = 1$, andererseits aber $\mu_a(B,1) = 2$, weil 1 eine doppelte Nullstelle von B ist. Aus $\mu_g(B,1) < \mu_a(B,1)$ ergibt sich nach Folgerung (13.26), dass B über $\mathbb{R}$ nicht diagonalisierbar ist.

Auch die Matrix

$$C \quad = \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

ist über $\mathbb{R}$ nicht diagonalisierbar. Das charakteristische Polynom $\chi_C = x^2 + 1$ besitzt nämlich in $\mathbb{R}$ keine Nullstellen und zerfällt somit über $\mathbb{R}$ auch nicht in Linearfaktoren. Anders sieht die Sache allerdings aus, wenn man C als Matrix über dem Körper $\mathbb{C}$ betrachtet. Dann besitzt χ_C eine Produktzerlegung $(x-i)(x+i)$. Aus den Ungleichungen $1 \leq \mu_g(C,\lambda) \leq \mu_a(C,\lambda)$ für $\lambda \in \{\pm i\}$ folgt, dass auch die Bedingungen $\mu_g(C,i) = \mu_a(C,i)$ und $\mu_g(C,-i) = \mu_a(C,-i)$ erfüllt sind. Also ist die Matrix C über dem Körper $\mathbb{C}$ diagonalisierbar.

§ 14. Abstände und Winkel, Bilinearformen

Inhaltsübersicht

Für die Formulierung elementarer geometrischer Aussagen sind Begriffe wie „Abstand“, „Länge“ und „Winkel“ unverzichtbar. Im vorliegenden Kapitel werden wir sehen, wie solche Begriffe axiomatisch eingeführt werden können; bezüglich des Abstands sind solche Axiome beispielsweise in der Definition der *Metrik* enthalten. Anschließend beschäftigen uns mit der Frage, wie sie sich diese geometrischen Begriffe auf (möglichst allgemeinen) $\mathbb{R}$-Vektorräumen definieren lassen, wobei wir neben der Existenz auch auf die Eindeutigkeit eingehen. Wie wir sehen werden, ist für diese Problemstellung das Konzept der *Bilinearform*, speziell des *Skalarprodukts* das zentrale Hilfsmittel.

Wichtige Begriffe und Sätze

- Norm, normierter $\mathbb{R}$-Vektorraum
- Metrik, metrischer Raum
- Orthogonalität, Winkelfunktion
- Bilinearform (Eigenschaften „symmetrisch“, „positiv definit“)
- Skalarprodukt, euklidischer Vektorraum
- euklidisches Standard-Skalarprodukt
- Orthonormalbasis
- Orthogonalprojektion auf einen Untervektorraum
- Cauchy-Schwarz’sche Ungleichung und Dreiecksungleichung
- Parallelogrammgleichung

(14.1) Definition Eine ***Norm*** auf einem $\mathbb{R}$-Vektorraum V ist eine Abbildung $\|\cdot\| : V \to \mathbb{R}_+$, die folgende Bedingungen erfüllt.

(i) Für alle $v \in V$ gilt $\|v\| = 0$ genau dann, wenn $v = 0_V$ ist.
(ii) Es gilt $\|\lambda v\| = |\lambda|\|v\|$ für alle $\lambda \in \mathbb{R}$ und $v \in V$.
(iii) Für alle $v, w \in V$ gilt $\|v + w\| \leq \|v\| + \|w\|$.

Das Paar $(V, \|\cdot\|)$ bezeichnet man als ***normierten Vektorraum***.

Die Ungleichung (iii) in der Normdefinition wird ***Dreiecks-Ungleichung*** genannt. Sind v, w zwei Elemente eines normierten $\mathbb{R}$-Vektorraums, dann kann $\|w - v\|$ als Abstand von v und w interpretiert werden. Das Konzept eines Abstandes zweier Punkte kann auch für beliebige Mengen (ohne Vektorraumstruktur) definiert werden.

(14.2) Definition Sei X eine Menge. Eine ***Metrik*** auf X ist eine Abbildung $d : X \times X \to \mathbb{R}_+$ mit den folgenden Eigenschaften.

(i) Für alle $x, y \in X$ gilt $d(x,y) = 0$ genau dann, wenn $x = y$ ist.
(ii) Es gilt $d(x,y) = d(y,x)$ für alle $x, y \in X$.
(iii) Für alle x, y, z gilt $d(x,z) \leq d(x,y) + d(y,z)$. *(Dreiecksungleichung)*

Das Paar (X,d) bezeichnet man als ***metrischen Raum***.

Mit den metrischen Räumen werden wir uns im Analysis-Teil der Vorlesung ausführlicher beschäftigen. Dort werden wir sehen, dass sich viele Begriffe der Analysis, beispielsweise die Konvergenz von Folgen und Stetigkeit von Abbildungen, auch auf dieser Basis formulieren lassen. An dieser Stelle halten wir zunächst nur fest, dass jeder normierte $\mathbb{R}$-Vektorraum auch die Struktur eines metrischen Raums besitzt.

(14.3) Proposition Sei $(V, \|\cdot\|)$ ein normierter $\mathbb{R}$-Vektorraum und $X \subseteq V$ eine Teilmenge. Dann ist durch die Definition $d(x,y) = \|x - y\|$ für $x, y \in X$ eine Metrik auf X gegeben. Man nennt sie die von der Norm $\|\cdot\|$ ***induzierte*** Metrik.

Beweis: Wir überprüfen die Bedingungen (i) bis (iii) aus der Definition. Für alle $x \in X$ gilt $d(x,x) = \|x - x\| = \|0_V\| = 0$. Sind umgekehrt $x, y \in X$ mit $d(x,y) = \|x - y\| = 0$, dann folgt $x - y = 0_V$ aus der Normdefinition und somit $x = y$. Damit ist (i) bewiesen. Für alle $x, y \in X$ gilt

$$d(x,y) \quad = \quad \|x-y\| \quad = \quad \|(-1)(y-x)\| \quad = \quad |-1|\|y-x\| \quad = \quad \|y-x\| \quad = \quad d(y,x) \quad ,$$

also ist auch Bedingung (ii) gültig. Seien schließlich $x, y, z \in X$ vorgegeben. Aus der Dreiecksungleichung für die Norm folgt dann $d(x,z) = \|x-z\| = \|(x-y)+(y-z)\| \leq \|x-y\| + \|y-z\| = d(x,y) + d(y,z)$. □

Um Geometrie zu betreiben, zum Beispiel Dreiecksgeometrie, benötigen wir im Allgemeinen nicht nur einen Längen- und Abstandsbegriff, sondern auch Winkel. Wir konzentrieren uns zunächst auf das Konzept des rechten Winkels.

(14.4) Definition Sei $(V, \|\cdot\|)$ ein normierter $\mathbb{R}$-Vektorraum, so bezeichnen wir eine Relation $\perp$ auf V als ***Orthogonalität***, wenn folgende Bedingungen erfülllt sind.

(i) Die Relation ist symmetrisch.

(ii) Sind $u, v, w \in V$ und $\lambda \in \mathbb{R}$, dann folgt aus $u \perp v$ und $u \perp w$ jeweils $u \perp (v + w)$ und $u \perp (\lambda v)$.

(iii) Es gilt $v \perp w \Leftrightarrow \|v\|^2 + \|w\|^2 = \|v + w\|^2$ für alle $v, w \in V$.

Die Bedingung (iv) wird auch als ***Satz des Pythagoras*** bezeichnet.

Aus dem Satz des Pythagoras folgt, dass der Nullvektor der einzige zu sich selbst orthogonale Vektor ist, denn auf Grund der Normeigenschaften (i) und (ii) gilt für alle $v \in V$ die Äquivalenz $v \perp v \Leftrightarrow 2\|v\|^2 = \|2v\|^2 \Leftrightarrow 2\|v\|^2 = |2|^2\|v\|^2 = 4\|v\|^2 \Leftrightarrow \|v\|^2 = 0 \Leftrightarrow v = 0_V$.

(14.5) Definition Eine ***Bilinearform*** auf einem $\mathbb{R}$-Vektorraum V ist eine Abbildung $b : V \times V \to \mathbb{R}$ mit der Eigenschaft, dass für alle $v, v', w, w' \in V$ und alle $\lambda \in \mathbb{R}$ die folgenden Bedingungen erfüllt sind.

(i) $b(v + v', w) = b(v, w) + b(v', w)$
(ii) $b(v, w + w') = b(v, w) + b(v, w')$
(iii) $b(\lambda v, w) = b(v, \lambda w) = \lambda b(v, w)$

Man bezeichnet die Bilinearform b als ***symmetrisch***, wenn $b(v, w) = b(w, v)$ für alle $v, w \in V$ gilt, und als ***positiv definit***, wenn außerdem $b(v, v) > 0$ für alle $v \in V$ mit $v \neq 0_V$ gilt.

Man kann die Bedingungen an eine Bilinearform b auch folgendermaßen zusammenfassen: Für jeden Vektor $w \in V$ ist $V \to \mathbb{R}$, $v \mapsto b(v, w)$ eine lineare Abbildung, und ebenso ist $V \to V$, $w \mapsto b(v, w)$ für jedes $v \in V$ linear.

(14.6) Definition Sei V ein $\mathbb{R}$-Vektorraum. Ein ***Skalarprodukt*** auf V ist eine symmetrische, positiv definite Bilinearform b auf V. Ein Paar (V, b) bestehend aus einem $\mathbb{R}$-Vektorraum V und einem Skalarprodukt b auf V nennt man einen ***euklidischen Vektorraum***.

(14.7) Proposition Sei $n \in \mathbb{N}$, und sei $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ die Abbildung definiert durch $\langle v, w \rangle = \sum_{j=1}^n v_j w_j$ für $v = (v_1, ..., v_n)$, $w = (w_1, ..., w_n) \in \mathbb{R}^n$. Dann ist $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf $\mathbb{R}^n$. Man bezeichnet es als das ***euklidische Standard-Skalarprodukt*** auf dem $\mathbb{R}^n$.

Beweis: Sämtliche in Definition (14.5) genannten Eigenschaften können mühelos nachgerechnet werden. Für alle $v, v', w \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gilt sowohl

$$\langle v + v', w \rangle \quad = \quad \sum_{j=1}^n (v_j + v'_j) w_j \quad = \quad \sum_{j=1}^n (v_j w_j + v'_j w_j) \quad = \quad \sum_{j=1}^n v_j w_j + \sum_{j=1}^n v'_j w_j \quad = \quad \langle v, w \rangle + \langle v', w \rangle$$

als auch $\langle \lambda v, w \rangle = \sum_{j=1}^n (\lambda v_j) w_j = \lambda \sum_{j=1}^n v_j w_j = \lambda \langle v, w \rangle$, und ebenso $\langle v, w \rangle = \sum_{j=1}^n v_j w_j = \sum_{j=1}^n w_j v_j = \langle w, v \rangle$. Damit erhalten wir für alle $v, w, w' \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ auch $\langle v, w + w' \rangle = \langle w + w', v \rangle = \langle w, v \rangle + \langle w', v \rangle = \langle v, w \rangle + \langle v, w' \rangle$. Zum Schluss überprüfen wir noch, dass die symmetrische Bilinearform auch positiv definit ist. Ist $v \in \mathbb{R}^n$ mit $v \neq 0_{\mathbb{R}^n}$, dann gilt $v_k \neq 0$ für mindestens ein $k \in \{1, ..., n\}$. Es folgt dann $\langle v, v \rangle = \sum_{j=1}^n v_j^2 \geq v_k^2 > 0$. □

(14.8) Lemma Sei $\phi : V \to W$ ein Isomorphismus von $\mathbb{R}$-Vektorräumen, und sei $\| \cdot \|$ eine Norm auf V. Dann ist durch $\|w\|_W = \|\phi^{-1}(w)\|$ eine Norm auf W definiert.

Beweis: Alle drei Normeigenschaften können unmittelbar überprüft werden. Seien dazu $w, w' \in W$ und $\lambda \in \mathbb{R}$ vorgegeben. Auf Grund der Injektivität von $\phi^{-1} : W \to V$ und der Normeigenschaft von $\|\cdot\|$ gilt die Äquivalenz $\|w\|_W = 0 \Leftrightarrow \|\phi^{-1}(w)\| = 0 \Leftrightarrow \phi^{-1}(w) = 0_V \Leftrightarrow w = 0_W$. Ebenso gilt auf Grund der Normeigenschaft von $\|\cdot\|$ sowohl die Gleichung $\|\lambda w\|_W = \|\phi^{-1}(\lambda w)\| = \|\lambda\phi^{-1}(w)\| = |\lambda|\|\phi^{-1}(w)\| = |\lambda|\|w\|_W$ als auch die Dreiecks-Ungleichung $\|w + w'\|_W = \|\phi^{-1}(w + w')\| = \|\phi^{-1}(w) + \phi^{-1}(w')\| \leq \|\phi^{-1}(w)\| + \|\phi^{-1}(w')\| = \|w\|_W + \|w'\|_W$. □

(14.9) Satz Sei $\|\cdot\|$ eine Norm auf dem $\mathbb{R}^n$, und sei $\perp$ eine Orthogonalität auf dem normierten $\mathbb{R}$-Vektorraum $(\mathbb{R}^n, \|\cdot\|)$ mit der zusätzlichen Eigenschaft, dass für alle $1 \leq j < k \leq n$ die Einheitsvektoren $e_j, e_k \in \mathbb{R}^n$ die Bedingungen $\|e_j\| = 1$ und $e_j \perp e_k$ erfüllen. Dann sind die Norm und die Orthogonalität auf dem $\mathbb{R}^n$ gegeben durch $\|v\| = \sqrt{\langle v, v\rangle}$ und $v \perp w \Leftrightarrow \langle v, w\rangle = 0$.

Beweis: Wir führen den Beweis durch vollständige Induktion über n. Für den Induktionsanfang seien $v, w \in \mathbb{R}^1$ mit $v = (v_1)$, $w = (w_1)$ vorgeben. Auf Grund der Normeigenschaft (ii) und der Voraussetzung an die Einheitsvektoren gilt $\|v\| = \|v_1 e_1\| = |v_1|\|e_1\| = |v_1| \cdot 1 = |v_1| = \sqrt{v_1^2} = \sqrt{\langle v, v\rangle}$. Auf Grund der Orthogonalitätsregel (iii), dem Satz des Pythagoras, gilt außerdem

$$\begin{aligned} v \perp w \quad &\Leftrightarrow \quad \|v + w\|^2 = \|v\|^2 + \|w\|^2 \quad \Leftrightarrow \quad (v_1 + w_1)^2 = v_1^2 + w_1^2 \quad \Leftrightarrow \quad v_1^2 + 2v_1w_1 + w_1^2 = v_1^2 + w_1^2 \\ &\Leftrightarrow \quad v_1w_1 = 0 \quad \Leftrightarrow \quad \langle v, w\rangle = 0. \end{aligned}$$

Sei nun $n \in \mathbb{N}$ beliebig, und setzen wir die Aussage für den $\mathbb{R}^n$ voraus. Die Abbildung $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ gegeben durch $(v_1, ..., v_n, v_{n+1}) \mapsto (v_1, ..., v_n)$ definiert offenbar einen Isomorphismus $\tilde{\pi} = \pi|_{(\mathbb{R}^{n+1})_0}$ zwischen dem Untervektorraum $(\mathbb{R}^{n+1})_0 = \mathbb{R}^n \times \{0\}$ und dem $\mathbb{R}^n$. Nach Lemma (14.8) ist durch $\|v\|_n = \|\tilde{\pi}^{-1}(v)\|$ eine Norm $\|\cdot\|_n$ auf dem $\mathbb{R}^n$ definiert, und man überprüft unmittelbar, dass $v \perp_n w \Leftrightarrow \tilde{\pi}^{-1}(v) \perp \tilde{\pi}^{-1}(w)$ eine Orthogonalitätsrelation auf $(\mathbb{R}^n, \|\cdot\|_n)$ ist. Auf Grund der Induktionsvoraussetzung gilt nun $\|v\|_n = \sqrt{\langle v, v\rangle_n}$ für alle $v \in \mathbb{R}^n$, wobei $\langle\cdot,\cdot\rangle_n$ das Standard-Skalarprodukt auf dem $\mathbb{R}^n$ bezeichnet. Daraus wiederum folgt $\|v\| = \|\pi(v)\| = \sqrt{\langle \pi(v), \pi(v)\rangle_n} = \sqrt{\langle v, v\rangle}$ für alle v aus dem Untervektorraum $(\mathbb{R}^{n+1})_0$ von $\mathbb{R}^{n+1}$.

Sei nun $v \in \mathbb{R}^{n+1}$ vorgegeben. Dann gilt $v = v' + v_{n+1}e_{n+1}$ mit $v' = (v_1, ..., v_n, 0) \in (\mathbb{R}^{n+1})_0$. Auf Grund der Voraussetzung $e_k \perp e_{n+1}$ für $1 \leq k \leq n$ erhalten wir mit Hilfe der Orthogonalitätsregeln (i) und (ii), dass auch $v' = \sum_{k=1}^n v_k e_k$ zu e_{n+1}, und damit auch zu $v_{n+1}e_{n+1}$, orthogonal ist. Mit Regel (iii), dem Satz des Pythagoras, erhalten wir nun

$$\begin{aligned} \|v\|^2 \quad &= \quad \|v' + v_n e_{n+1}\|^2 \quad = \quad \|v'\|^2 + \|v_n e_{n+1}\|^2 \quad = \quad \|v'\|^2 + |v_{n+1}|^2\|e_{n+1}\|^2 \\ &= \quad \sum_{k=1}^n v_k^2 + v_{n+1}^2 \quad = \quad \sum_{k=1}^{n+1} v_k^2 \quad = \quad \langle v, v\rangle. \end{aligned}$$

Es folgt $\|v\| = \sqrt{\langle v, v\rangle}$. Nun überprüfen wir noch, dass die Orthogonalität $\perp$ auf dem $\mathbb{R}^{n+1}$ die angegebene Form hat. Seien dazu $v, w \in \mathbb{R}^{n+1}$ vorgegeben. Dann gilt die Äquivalenz

$$\begin{aligned} v \perp w \quad &\Leftrightarrow \quad \|v + w\|^2 = \|v\|^2 + \|w\|^2 \quad \Leftrightarrow \quad \langle v + w, v + w\rangle = \langle v, v\rangle + \langle w, w\rangle \quad \Leftrightarrow \\ \langle v, v + w\rangle + \langle w, v + w\rangle = \langle v, v\rangle + \langle w, w\rangle \quad &\Leftrightarrow \quad \langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle + \langle w, w\rangle = \langle v, v\rangle + \langle w, w\rangle \quad \Leftrightarrow \\ \langle v, v\rangle + 2\langle v, w\rangle + \langle w, w\rangle = \langle v, v\rangle + \langle w, w\rangle \quad &\Leftrightarrow \quad 2\langle v, w\rangle = 0 \quad \Leftrightarrow \quad \langle v, w\rangle = 0. \end{aligned}$$

□

(14.10) Definition Sei $(V, \|\cdot\|)$ ein normierter $\mathbb{R}$-Vektorraum mit einer Orthogonalität $\perp$ und $V^\times = V \setminus \{0_V\}$. Eine ***Winkelfunktion*** bezüglich $(V, \|\cdot\|, \perp)$ ist eine Abbildung $\sphericalangle : V^\times \times V^\times \to [0, \pi]$, die für alle $v, w \in V^\times$ folgende Bedingungen erfüllt.

(i) $\sphericalangle(v, v) = 0$ und $\sphericalangle(v, w) = \sphericalangle(w, v)$
(ii) $\sphericalangle(v, w) = \sphericalangle(v, \lambda w)$ für alle $\lambda \in \mathbb{R}^+$
(iii) $\sphericalangle(v, w) + \sphericalangle(w, -v) = \pi$
(iv) Aus $v \perp w$ folgt $\sphericalangle(v, w) = \frac{1}{2}\pi$.
(v) Aus $v \perp (w - v)$ folgt $\cos \sphericalangle(v, w) = \frac{\|v\|}{\|w\|}$.

Auch eine Winkelfunktion auf dem $\mathbb{R}^n$ ist unter wenigen naheliegenden Voraussetzungen eindeutig bestimmt.

(14.11) Satz Sei $\|\cdot\|$ eine Norm auf dem $\mathbb{R}^n$, und sei $\perp$ eine Orthogonalität auf dem normierten $\mathbb{R}$-Vektorraum $(\mathbb{R}^n, \|\cdot\|)$ mit der Eigenschaft, dass für alle $1 \le j < k \le n$ die Einheitsvektoren $e_j, e_k \in \mathbb{R}^n$ die Bedingungen $\|e_j\| = 1$ und $e_j \perp e_k$ erfüllen. Sei $\sphericalangle$ eine Winkelfunktion bezüglich $(\mathbb{R}^n, \|\cdot\|, \perp)$. Dann ist $\sphericalangle$ die eindeutig bestimmte Abbildung mit

$$\cos \sphericalangle(v, w) \quad = \quad \frac{\langle v, w\rangle}{\|v\|\|w\|} \qquad \text{für alle} \quad v, w \in (\mathbb{R}^n)^\times.$$

Beweis: Nach Satz (14.9) gilt unter den angegebenen Voraussetzungen $\|v\| = \sqrt{\langle v, v\rangle}$ und $v \perp w \Leftrightarrow \langle v, w\rangle = 0$ für alle $v, w \in \mathbb{R}^n$. Seien nun $v, w \in (\mathbb{R}^n)^\times$ vorgegeben; zu zeigen ist, dass der Wert $\sphericalangle(v, w) \in [0, \pi]$ die angegebene Gleichung erfüllt. Betrachten wir zunächst den Fall, dass diese linear abhängig sind. Dann gilt $w = \lambda v$ für ein $\lambda \in \mathbb{R}^\times$. Im Fall $\lambda > 0$ erhalten wir auf Grund der Regel (i) für Winkelfunktionen $\sphericalangle(v, w) = \sphericalangle(v, \lambda v) = \sphericalangle(v, v) = 0$, also $\cos \sphericalangle(v, w) = \cos 0 = 1$, und ebenso gilt

$$\frac{\langle v, w\rangle}{\|v\|\|w\|} \quad = \quad \frac{\langle v, \lambda v\rangle}{\|v\|\|\lambda v\|} \quad = \quad \frac{\lambda}{|\lambda|} \quad = \quad 1 \cdot \frac{\langle v, v\rangle}{\|v\|\|v\|} \quad = \quad \frac{\|v\|^2}{\|v\|^2} \quad = \quad 1.$$

Auf Grund der Regel (ii) gilt $\sphericalangle(v, -v) = \sphericalangle(v, v) + \sphericalangle(v, -v) = \pi$. Im Fall $\lambda < 0$ erhalten wir somit $\sphericalangle(v, w) = \sphericalangle(v, (-\lambda)(-v)) = \sphericalangle(v, -v) = \pi$ und $\cos \sphericalangle(v, w) = \cos \pi = -1$; entsprechend gilt

$$\frac{\langle v, w\rangle}{\|v\|\|w\|} \quad = \quad \frac{\langle v, \lambda v\rangle}{\|v\|\|\lambda v\|} \quad = \quad \frac{\lambda}{|\lambda|} \quad = \quad (-1) \cdot \frac{\langle v, v\rangle}{\|v\|\|v\|} \quad = \quad -\frac{\|v\|^2}{\|v\|^2} \quad = \quad -1.$$

Betrachten wir nun den Fall, dass das Paar (v, w) linear unabhängig ist. Im Fall $\langle v, w\rangle = 0$ gilt $v \perp w$ und somit $\sphericalangle(v, w) = \frac{1}{2}\pi$ auf Grund der Regel (iv) für Winkelfunktionen. Es gilt dann also $\cos \sphericalangle(v, w) = \cos \frac{1}{2}\pi = 0 = \frac{\langle v, w\rangle}{\|v\|\|w\|}$. Wir dürfen also von nun an voraussetzen, dass $\langle v, w\rangle$ ungleich null ist. Es gilt dann für alle $\lambda \in \mathbb{R}$ die Äquivalenz

$$(w - \lambda v) \perp v \quad \Leftrightarrow \quad \langle w - \lambda\langle v, v\rangle = 0 \quad \Leftrightarrow \quad \langle w, v\rangle - \lambda\langle v, v\rangle = 0 \quad \Leftrightarrow \quad \lambda\langle v, v\rangle = \langle v, w\rangle \quad \Leftrightarrow \quad \lambda = \frac{\langle v, w\rangle}{\|v\|^2}.$$

Setzen wir also λ auf diesen Wert ungleich null. Außerdem gilt die Äquivalenz dann können wir die Regel (v) für Winkelfunktionen auf λv und w anwenden und erhalten $\cos \sphericalangle(\lambda v, w) = \frac{\|\lambda v\|}{\|w\|} = |\lambda| \frac{\|v\|}{\|w\|}$. Ist nun $\lambda > 0$, dann ist die angegebene Gleichung erfüllt, denn es gilt

$$\cos \sphericalangle(v,w) \quad = \quad \cos \sphericalangle(\lambda v, w) \quad = \quad \lambda \frac{\|v\|}{\|w\|} \quad = \quad \frac{\langle v,w\rangle}{\|v\|^2} \cdot \frac{\|v\|}{\|w\|} \quad = \quad \frac{\langle v,w\rangle}{\|v\|\|w\|}.$$

Auch im Fall $\lambda < 0$ gilt die Gleichung; in diesem Fall ergibt sie sich mit Hilfe der Regel (iii) und der Rechenregeln $\cos(\alpha + \pi) = -\cos(\pi)$ und $\cos(-\alpha) = \cos(\alpha)$ der Kosinusfunktion durch

$$\begin{aligned} \cos \sphericalangle(v,w) \quad &= \quad \cos(\pi - \sphericalangle(-v,w)) \quad = \quad -\cos \sphericalangle(-v,w) \quad = \quad -\cos \sphericalangle((-\lambda)(-v),w) \quad = \quad -\cos \sphericalangle(\lambda v, w) \\ &= \quad -|\lambda| \frac{\|v\|}{\|w\|} \quad = \quad -(-\lambda) \frac{\|v\|}{\|w\|} \quad = \quad \lambda \frac{\|v\|}{\|w\|} \quad = \quad \frac{\langle v,w\rangle}{\|v\|^2} \cdot \frac{\|v\|}{\|w\|} \quad = \quad \frac{\langle v,w\rangle}{\|v\|\|w\|}. \end{aligned}$$

□

Bisher haben wir uns auf die Frage nach der *Eindeutigkeit* einer Norm mit dazu passender Winkelfunktion konzentriert. Als nächstes soll nun gezeigt werden, dass auf jedem euklidischen Vektorraum diese geometrischen Konzepte definiert werden können. Daraus folgt dann, dass auf jedem euklidischen Vektorraum euklidische Geometrie betrieben werden kann, wodurch diese Bezeichnung letztlich motiviert ist. Um dieses Ziel zu erreichen, müssen wir zunächst die Orthogonalität in solchen Vektorräumen genauer untersuchen.

(14.12) Lemma Sei V ein $\mathbb{R}$-Vektorraum und b eine symmetrische Bilinearform auf V. Seien $v, w \in V$ mit $b(v,v) \neq 0$ vorgegeben und $\lambda = \frac{b(v,w)}{b(v,v)}$. Dann gilt $b(v, w - \lambda v) = 0$. Wir bezeichnen den Vektor λv als die ***Orthogonalprojektion*** von w auf den Untervektorraum $\langle v \rangle_{\mathbb{R}}$ von V.

Beweis: Dass man durch den angegebenen Wert von λ einen zu v orthogonalen Vektor $w - \lambda$ erhält, haben wir für den $\mathbb{R}$-Vektorraum $\mathbb{R}^n$ mit dem euklidischen Standard-Skalarprodukt bereits im Beweis von Satz (14.11) gesehen. Die Rechnung ist hier im Wesentlichen dieselbe: Es gilt

$$\begin{aligned} b(v, w - \lambda v) \quad &= \quad b(v,w) - b(v, \lambda v) \quad = \quad b(v,w) - \lambda b(v,v) \quad = \\ b(v,w) - \frac{b(v,w)}{b(v,v)} \cdot b(v,v) \quad &= \quad b(v,w) - b(v,w) \quad = \quad 0. \end{aligned}$$

□

Das Konzept der Orthogonalprojektion, das wir hier für eindimensionale Untervektorräume eingeführt haben, lässt sich auf Untervektorräume beliebiger endlicher Dimension übertragen. Dazu führen wir die folgende Notation ein: Ist V ein $\mathbb{R}$-Vektorraum und b eine symmetrische Bilinearform auf V, dann definieren wir für beliebige Teilmengen $A, B \subseteq V$, dass

$$A \perp_b B \qquad \text{bedeuten soll, dass} \qquad b(v,w) = 0 \ \ \forall\, v \in A, w \in B \quad \text{gilt.}$$

Bei einelementigen Mengen schreiben wir statt $\{v\} \perp_b B$ auch $v \perp_b B$. Damit können wir nun definieren

(14.13) Definition Sei V ein $\mathbb{R}$-Vektorraum, b eine symmetrische Bilinearform auf V und U ein Untervektorraum von V. Eine ***Orthogonalprojektion*** von V auf U ist eine lineare Abbildung $\pi_U : V \to U$ mit der Eigenschaft $\pi_U|_U = \mathrm{id}_U$ und $(v - \pi_U(v)) \perp_b U$ für alle $v \in V$.

Den folgenden Begriff benötigen wir, um die Existenz von Orthogonalprojektionen nachweisen zu können.

(14.14) Definition Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und b eine symmetrische Bilinearform auf V. Eine geordnete Basis $\mathscr{B} = (v_1, ..., v_n)$ von V wird ***Orthonormalbasis*** (kurz *ON*-Basis) genannt, wenn

$$b(v_k, v_\ell) \quad = \quad \delta_{k\ell} \qquad \text{für} \quad 1 \leq k, \ell \leq n \quad \text{erfüllt ist.}$$

Damit kann nun gezeigt werden

(14.15) Proposition Sei (V, b) ein $\mathbb{R}$-Vektorraum mit einer symmetrischen Bilinearform. Sei $U \subseteq V$ ein Untervektorraum der endlichen Dimension n und $(u_1, ..., u_n)$ eine ON-Basis von U. Dann ist durch

$$\pi_U(v) \quad = \quad \sum_{k=1}^{n} b(u_k, v)u_k \qquad \text{eine Orthogonalprojektion auf } U \text{ definiert.}$$

Beweis: Als erstes überprüfen wir, dass π_U linear ist. Seien $v, w \in V$ und $\lambda \in \mathbb{R}$ vorgegeben. Dann gilt

$$\pi_U(v+w) \quad = \quad \sum_{k=1}^{n} b(u_k, v+w)u_k \quad = \quad \sum_{k=1}^{n} (b(u_k, v) + b(u_k, w))u_k$$
$$= \quad \sum_{k=1}^{n} b(u_k, v)u_k + \sum_{k=1}^{n} b(u_k, w)u_k \quad = \quad \pi_U(v) + \pi_U(w)$$

und ebenso $\pi_U(\lambda v) = \sum_{k=1}^{n} b(u_k, \lambda v)u_k = \sum_{k=1}^{n} \lambda b(u_k, v)u_k = \lambda\left(\sum_{k=1}^{n} b(u_k, v)u_k\right) = \lambda\pi_U(v)$. Damit ist die Linearität nachgewiesen. Sei nun $v \in V$ vorgegeben. Zunächst zeigen wir, dass $v - \pi_U(v)$ auf jedem Basisvektor u_ℓ mit $1 \leq \ell \leq n$ senkrecht steht. Es gilt

$$b(u_\ell, v - \pi_U(v)) \quad = \quad b\left(u_\ell, v - \sum_{k=1}^{n} b(u_k, v)u_k\right) \quad = \quad b(u_\ell, v) - \sum_{k=1}^{n} b(u_\ell, b(u_k, v)u_k) \quad =$$
$$b(u_\ell, v) - \sum_{k=1}^{n} b(u_k, v)b(u_\ell, u_k) \quad = \quad b(u_\ell, v) - \sum_{k=1}^{n} b(u_k, v)\delta_{\ell k} \quad = \quad b(u_\ell, v) - b(u_\ell, v) \quad = \quad 0.$$

Ist nun $u \in U$ beliebig, dann gibt es $\lambda_1, ..., \lambda_n \in \mathbb{R}$ mit $u = \sum_{\ell=1}^{n} \lambda_\ell u_\ell$. Wir erhalten

$$b(u, v - \pi_U(v)) \quad = \quad b\left(\sum_{\ell=1}^{n} \lambda_\ell u_\ell, v - \pi_U(v)\right) \quad = \quad \sum_{\ell=1}^{n} \lambda_\ell b(u_\ell, v - \pi_U(v)) \quad = \quad \sum_{\ell=1}^{n} \lambda_\ell \cdot 0 \quad = \quad 0.$$

Es gilt also $(v - \pi_U(v)) \perp U$. Zum Beweis der zweiten Eigenschaft einer Orthogonalprojektion sei $u \in U$ vorgegeben. Dann gibt es $\lambda_1, ..., \lambda_n \in \mathbb{R}$ mit $u = \sum_{k=1}^{n} \lambda_k u_k$. Auf Grund der Linearität von π_U erhalten wir

$$\pi_U(u) \quad = \quad \sum_{k=1}^{n} \lambda_k \pi_U(u_k) \quad = \quad \sum_{k=1}^{n} \lambda_k \left(\sum_{\ell=1}^{n} b(u_\ell, u_k)u_\ell\right) \quad =$$
$$\sum_{k=1}^{n} \lambda_k \left(\sum_{\ell=1}^{n} \delta_{\ell k} u_\ell\right) \quad = \quad \sum_{k=1}^{n} 1 \cdot \lambda_k u_k \quad = \quad u \qquad \text{wie gewünscht.}$$ □

Auf dieser Grundlage können wir nun Längen und Winkel auf beliebigen euklidischen Vektorräumen definieren. Zur Vorbereitung zeigen wir

(14.16) Satz Sei (V,b) ein euklidischer $\mathbb{R}$-Vektorraum, und sei $\|\cdot\|_b : V \to \mathbb{R}_+$ die Funktion definiert durch $\|v\|_b = \sqrt{b(v,v)}$ für $v \in V$. Dann gilt für alle $v,w \in V$

(i) die sog. ***Cauchy-Schwarz'sche Ungleichung*** $|b(v,w)| \leq \|v\|_b \|w\|_b$,
(ii) die Dreiecksungleichung $\|v+w\|_b \leq \|v\|_b + \|w\|_b$.

Dabei ist die Ungleichung (i) genau dann mit Gleichheit erfüllt, wenn v,w linear abhängig sind. Darüber hinaus ist durch $\|\cdot\|_b$ eine Norm auf V definiert. Man nennt sie die von b ***induzierte Norm***.

Beweis: Für den Beweis von (i) unterscheiden wir auch hier zwei Fälle. Ist einer der Vektoren gleich Null, dann sind v,w linear abhängig, und die Ungleichung ist mit Gleichheit erfüllt, da beide Seiten von $|b(v,w)| \leq \|v\|_b\|w\|_b$ gleich Null sind. Also sind in diesem Fall alle Aussagen erfüllt. Nun setzen wir $v,w \neq 0_V$ voraus. Sei $\lambda = \frac{b(v,w)}{b(v,v)} = \frac{b(v,w)}{\|v\|_b^2}$ der Wert aus Lemma (14.12). Weil b positiv definit ist, gilt $b(w-\lambda v, w-\lambda v) \geq 0$. Wir erhalten nun

$$\begin{aligned} b(w-\lambda v, w-\lambda v) &= b(w, w-\lambda v) - \lambda b(v, w-\lambda v) = \\ b(w,w) - \lambda b(w,v) - \lambda b(v,w) + \lambda^2 b(v,v) &= b(w,w) - 2\lambda b(v,w) + \lambda^2 b(v,v). \end{aligned}$$

Setzen wir den Wert von λ in die Ungleichung ein, so ergibt sich

$$b(w,w) - 2\frac{b(v,w)}{\|v\|_b^2} + \frac{b(v,w)^2}{\|v\|_b^4} b(v,v) \geq 0$$

was wegen $\|v\|_b^2 = b(v,v)$ umgeformt werden kann zu

$$b(w,w) - 2\frac{b(v,w)^2}{b(v,v)} b(v,w) + \frac{b(v,w)^2}{b(v,v)} \geq 0.$$

Dies wiederum ist äquivalent zu $b(w,w) \geq \frac{b(v,w)^2}{b(v,v)}$ und $b(v,w)^2 \leq b(v,v)b(w,w)$. Durch Wurzelziehen auf beiden Seiten erhalten wir wegen $\|v\|_b = \sqrt{b(v,v)}$ und $\|w\|_b = \sqrt{b(w,w)}$ die Cauchy-Schwarz'sche Ungleichung.

Als nächstes beweisen wir die Äquivalenzaussage im Zusammenhang mit (i). Für $v = 0_V$ oder $w = 0_V$ besteht offenbar lineare Abhängigkeit, und auf beiden Seiten der Ungleichung steht eine Null, sie ist also mit Gleichheit erfüllt. Wir können deshalb $v,w \neq 0_V$ voraussetzen. Sind v,w linear abhängig, dann gilt $w = \mu v$ für ein $\mu \in \mathbb{R}^\times$. Die linke Seite der Cauchy-Schwarz'schen Ungleichung ist dann gegeben durch $|b(v,\mu v)| = |\mu| b(v,v)$, die rechte durch $\|v\|_b\|\mu v\|_b = \|v\|\sqrt{b(\mu v, \mu v)} = \|v\|_b|\mu|\sqrt{b(v,v)} = |\mu|\|v\|_b^2 = |\mu| b(v,v)$, also stimmen beiden Seiten überein. Setzen wir nun umgekehrt die Gleichung $|b(v,w)| = \|v\|_b\|w\|_b$ voraus, und führen wir die Umformungsschritte von oben in umgekehrter Reihenfolge durch, so erhalten wir $b(w-\lambda v, w-\lambda v) = 0$. Da b positiv definit ist, folgt daraus $w-\lambda v = 0$ und $w = \lambda v$. Dies zeigt, dass v,w linear abhängig sind.

Kommen wir nun zum Beweis von (ii), der Dreiecksungleichung. Diese erhalten wir durch die Rechnung

$$b(v+w,v+w) \quad = \quad b(v,v)+2b(v,w)+b(w,w) \quad \leq \quad \|v\|_b^2+2\|v\|_b\|w\|_b^2+\|w\|_b^2 \quad = \quad (\|v\|_b+\|w\|_b)^2$$

und anschließendes Wurzelziehen auf beiden Seiten. Die Überprüfung der anderen beiden Normeigenschaften von $\|\cdot\|_b$ ist reine Routine: Offenbar gilt $b(0_V,0_V)=0$ und somit $\|0_V\|_b=\sqrt{b(0_V,0_V)}=\sqrt{0}=0$; ist umgekehrt $v\in V$ mit $\|v\|_b=0$, dann folgt $b(v,v)=0$ und somit $v=0_V$, weil b positiv definit ist. Für alle $v\in V$ und $\lambda\in\mathbb{R}$ gilt schließlich

$$\|\lambda v\|_b \quad = \quad \sqrt{b(\lambda v,\lambda v)} \quad = \quad \sqrt{\lambda^2 b(v,v)} \quad = \quad |\lambda|\sqrt{b(v,v)} \quad = \quad |\lambda|\|v\|_b. \qquad \square$$

Wir werden im nächsten Kapitel eine Vielzahl von Normen auf $\mathbb{R}$-Vektorräumen kennenlernen, für verschiedene Fragestellungen aus der Analysis zum Teil besser handhabbar sind. Mit dem folgenden Resultat lässt sich zeigen, dass diese in der Regel aber nicht, wie im letzten Satz durch ein Skalarprodukt zu Stande kommen.

(14.17) Satz Sei V ein $\mathbb{R}$-Vektorraum. Eine Norm $\|\cdot\|$ auf V wird genau dann durch ein Skalarprodukt b induziert, wenn für alle $v,w\in V$ die sog. *Parallelogrammgleichung*

$$\|v+w\|^2+\|v-w\|^2 \quad = \quad 2(\|v\|^2+\|w\|^2) \qquad \text{erfüllt ist.}$$

Beweis: „⇒“ Sei b ein Skalarprodukt mit $\|\cdot\|=\|\cdot\|_b$. Wir müssen überprüfen, dass die Parallelogrammgleichung in diesem Fall gültig ist. Tatsächlich gilt für alle $v,w\in V$ die Gleichung

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

$$b(v,v)+2b(v,w)+b(w,w)+b(v,v)-2b(v,w)+b(w,w) \quad =$$

$$2b(v,v)+2b(w,w) \quad = \quad 2\left(\|v\|^2+\|w\|^2\right).$$

„⇐“ Diese Richtung ist um einiges aufwändiger; aus Gründen der Übersichtlichkeit verschieben wir diesen Beweis ans Ende des Kapitels.

$\square$

(14.18) Satz Sei (V,b) ein euklidischer Vektorraum. Dann ist auf dem normierten $\mathbb{R}$-Vektorraum $(V,\|\cdot\|_b)$ durch $v\perp_b w\iff b(v,w)$ eine Orthogonalität definiert, und die eindeutig bestimmte Funktion $\measuredangle_b : V^\times\times V^\times\to[0,\pi]$ mit

$$\cos\measuredangle_b(v,w) \quad = \quad \frac{b(v,w)}{\|v\|_b\|w\|_b} \qquad \text{für alle} \quad v,w\in V^\times$$

ist eine Winkelfunktion bezüglich $(V,\|\cdot\|_b,\perp_b)$.

Beweis: Zunächst halten wir fest, dass eine Funktion $\sphericalangle_b$ wie angegeben tatsächlich existiert, denn auf Grund der Cauchy-Schwarz'schen Ungleichung (i) aus Satz (14.16) gilt $-1 \leq \frac{b(v,w)}{\|v\|_b\|w\|_b} \leq 1$ für alle $v, w \in V^\times$. Dass sie durch die angegebene Bedingung eindeutig bestimmt ist, liegt an der Bijektivität der Funktion $\cos|_{[0,\pi]} : [0,\pi] \to [-1,1]$. Wir müssen nun die Eigenschaften (i) bis (v) aus Definition (14.10) überprüfen. Die Gleichung $\sphericalangle_b(v,w) = \sphericalangle_b(w,v)$ in Eigenschaft (i) ergibt sich unmittelbar aus $b(v,w) = b(w,v)$. Für alle $v \in V^\times$ ist außerdem $\frac{b(v,v)}{\|v\|_b\|v\|_b} = \frac{\|v\|_b^2}{\|v\|_b^2} = 1$, und wegen $\cos 0 = 1$ erhalten wir $\sphericalangle_b(v,v) = 0$. Eigenschaft (ii) erhalten wir für beliebige $v, w \in V^\times$ und $\lambda \in \mathbb{R}^+$ durch die Rechnung

$$\cos\sphericalangle_b(v,\lambda w) \quad = \quad \frac{b(v,\lambda w)}{\|v\|_b\|\lambda w\|_b} \quad = \quad \frac{\lambda}{|\lambda|}\cdot\frac{b(v,w)}{\|v\|_b\|w\|_b} \quad = \quad \frac{b(v,w)}{\|v\|_b\|w\|_b} \quad = \quad \cos\sphericalangle_b(v,w).$$

Kommen wir nun zur Eigenschaft (iii). Seien $v, w \in V^\times$, $\alpha = \sphericalangle_b(v,w)$ und $\beta = \sphericalangle_b(w,-v)$. Dann gilt

$$\cos(\beta) \quad = \quad \frac{b(w,-v)}{\|w\|_b\|-v\|_b} \quad = \quad -\frac{b(v,w)}{\|v\|_b\|w\|_b} \quad = \quad -\cos(\alpha).$$

Auf Grund der Eigenschaften der Kosinusfunktion folgt $\cos(\beta) = -\cos(\alpha) = -\cos(-\alpha) = \cos(\pi-\alpha)$, und auf Grund der Bijektivität von $\cos|_{[0,\pi]} : [0,\pi] \to [-1,1]$ folgt daraus $\beta = \pi - \alpha$, also $\alpha + \beta = \pi$.

Nun beweisen wir die Eigenschaft (iv). Ist $v \perp_b w$, dann folgt $b(v,w) = 0$ und $\cos\sphericalangle_b(v,w) = \frac{b(v,w)}{\|v\|_b\|w\|_b} = 0 = \cos\frac{1}{2}\pi$ und $\sphericalangle_b(v,w) = \frac{1}{2}\pi$. Für den Beweis der Eigenschaft (v) seien $v, w \in V^\times$ setzen wir $v \perp_b (w-v)$ voraus, was zu $b(v,w) - b(v,v) = b(v,w-v) = 0$ und somit zu $b(v,v) = b(v,w)$ äquivalent ist. Es folgt

$$\cos\sphericalangle_b(v,w) \quad = \quad \frac{b(v,w)}{\|v\|_b\|w\|_b} \quad = \quad \frac{b(v,v)}{\|v\|_b\|w\|_b} \quad = \quad \frac{\|v\|_b^2}{\|v\|_b\|w\|_b} \quad = \quad \frac{\|v\|_b}{\|w\|_b}. \qquad \square$$

Anhang: Beweis der Richtung „⇐" von Satz (14.17)

Entscheidend ist die Beobachtung, dass ein Skalarprodukt b mit der induzierten Norm $\|\cdot\|_b$ für alle $v, w \in V$ durch die Gleichung

$$\|v+w\|_b^2 = \|v\|_b^2 + 2b(v,w) + \|w\|_b^2 \quad \Leftrightarrow \quad b(v,w) = \tfrac{1}{2}(\|v+w\|_b^2 - \|v\|_b^2 - \|w\|_b^2)$$

in Beziehung steht. Es ist daher naheliegend, die Gleichung zu verwenden, um zu einer gegebenen Norm ein „passendes" Skalarprodukt zu definieren. Die Parallelogrammgleichung wird für den Nachweis benötigt, dass die so definierte Abbildung tatsächlich ein Skalarprodukt ist.

Sei also $\|\cdot\|$ eine Norm, für die die Parallelogrammgleichung erfüllt ist. Dann definieren wir die Abbildung $b : V \times V \to \mathbb{R}$ durch

$$b(v,w) \quad = \quad \tfrac{1}{2}(\|v+w\|^2 - \|v\|^2 - \|w\|^2).$$

Wir überprüfen nun, dass durch b ein Skalarprodukt auf V definiert ist. Wegen $b(v,v) = \frac{1}{4}\|v+v\|^2 = \|v\|^2 > 0$ für $v \neq 0_V$ ist b jedenfalls positiv definit. Auch die Symmetrie $b(v,w) = b(w,v)$ für alle $v, w \in V$ erhält man unmittelbar durch Einsetzen. Außerdem gilt offenbar

$$b(v,0_V) \quad = \quad b(0_V,v) \quad = \quad 0 \qquad \text{für alle} \quad v \in V.$$

Auf Grund der Symmetrie brauchen wir für b die Linearität nur in der ersten Komponente überprüfen. Zunächst beweisen wir die Gleichung $b(u+v,w)+b(u-v,w)=2b(u,w)$ für $u,v,w\in V$. Die linke Seite der Gleichung ist in ausgeschriebener Form

$$\tfrac{1}{2}(\|u+v+w\|^2-\|u+v\|^2-\|w\|^2)+\tfrac{1}{2}(\|u-v+w\|^2-\|u-v\|^2-\|w\|^2) \quad ,$$

die rechte Seite

$$2b(u,w) \quad = \quad \|u+w\|^2-\|u\|^2-\|w\|^2.$$

Insgesamt lautet die zu beweisende Gleichung also

$$\tfrac{1}{2}\|u+v+w\|^2+\tfrac{1}{2}\|u-v+w\|^2-\tfrac{1}{2}\|u+v\|^2-\tfrac{1}{2}\|u-v\|^2-\|w\|^2 \quad = \quad \|u+w\|^2-\|u\|^2-\|w\|^2$$

$$\Leftrightarrow \quad (\tfrac{1}{2}\|u+v+w\|^2+\tfrac{1}{2}\|u-v+w\|^2)-(\tfrac{1}{2}\|u+v\|^2+\tfrac{1}{2}\|u-v\|^2) \quad = \quad \|u+w\|^2-\|u\|^2.$$

Die beiden Klammerausdrücke auf der linken Seite können mit Hilfe der Parallelogrammgleichung umgeformt werden. Für den ersten Ausdruck erhalten wir

$$\tfrac{1}{2}\|u+v+w\|^2+\tfrac{1}{2}\|u-v+w\|^2 \quad = \quad \tfrac{1}{2}\|(u+w)+v\|^2+\tfrac{1}{2}\|(u+w)-v\|^2 \quad = \quad \|u+w\|^2+\|v\|^2$$

und für den zweiten

$$\tfrac{1}{2}\|u+v\|^2+\tfrac{1}{2}\|u-v\|^2 \quad = \quad \|u\|^2+\|v\|^2.$$

Setzen wir beides in die zu beweisende Gleichung ein, so erhalten wir

$$(\tfrac{1}{2}\|u+v+w\|^2+\tfrac{1}{2}\|u-v+w\|^2)-(\tfrac{1}{2}\|u+v\|^2+\tfrac{1}{2}\|u-v\|^2) \quad =$$

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

Damit ist der Beweis der Gleichung abgeschlossen. Im Fall $u=v$ erhalten wir insbesondere $b(2u,w)=b(2u,w)+0=b(u+u,w)+b(u-u,w)=2b(u,w)$. Nun können wir die Additivität von b in der linken Komponente nachrechnen: Für alle $v,v',w\in V$ erhalten wir mit Hilfe der bereits bewiesenen Gleichungen

$$b(v,w)+b(v',w) \quad = \quad b(\tfrac{1}{2}(v+v')+\tfrac{1}{2}(v-v'),w)+b(\tfrac{1}{2}(v+v')-\tfrac{1}{2}(v-v'),w)$$

$$= \quad 2b(\tfrac{1}{2}(v+v'),w) \quad = \quad b(v+v',w).$$

Der nächste Schritt besteht im Beweis der Gleichung $b(\lambda v,w)=\lambda b(v,w)$ für $v,w\in V$ und $\lambda\in\mathbb{R}$. Seien also $v,w\in V$ vorgeben. Zunächst beweisen wir die Gleichung für alle $\lambda\in\mathbb{N}_0$ durch vollständige Induktion. Den Fall $\lambda=0$ haben wir oben bereits erledigt. Setzen wir nun die Gleichung für λ voraus, dann erhalten wir mit Hilfe der Additvität

$$b((\lambda+1)v,w) \quad = \quad b(\lambda v+v,w) \quad = \quad b(\lambda v,w)+b(v,w) \quad =$$

$$\lambda b(v,w)+b(v,w) \quad = \quad (\lambda+1)b(v,w).$$

Damit ist die Gleichung für alle $\lambda\in\mathbb{N}_0$ bewiesen. Für beliebiges $\lambda\in\mathbb{N}_0$ gilt auch

$$\lambda b(v,w)+b((-\lambda)v,w) \quad = \quad b(\lambda v,w)+b((-\lambda)v,w) \quad =$$

$$b(\lambda v+(-\lambda)v,w) \quad = \quad b(0_V,w) \quad = \quad 0$$

und somit $b((-\lambda)v,w) = (-\lambda)b(v,w)$. Insgesamt gilt also $b(\lambda v,w) = \lambda b(v,w)$ für alle $\lambda \in \mathbb{Z}$. Sei nun $\lambda \in \mathbb{Q}$, $\lambda = \frac{m}{n}$ mit $m \in \mathbb{Z}$ und $n \in \mathbb{N}$. Es gilt

$$nb(\lambda v,w) \quad = \quad b(n\lambda v,w) \quad = \quad b(mv,w) \quad = \quad mb(v,w)$$

also $b(\lambda v,w) = \frac{m}{n}b(v,w) = \lambda b(v,w)$. Sei schließlich $\lambda \in \mathbb{R}$ eine beliebige reelle Zahl. Dann gibt es eine Folge $(\lambda_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ mit $\lim_n \lambda_n = \lambda$. Für jedes $n \in \mathbb{N}$ gilt

$$\begin{aligned} \|\lambda_n v + w\| \quad &= \quad \|(\lambda_n v + w) - (\lambda v + w) + (\lambda v + w)\| \quad \leq \quad \|(\lambda_n - \lambda)v\| + \|\lambda v + w\| \\ &= \quad |\lambda_n - \lambda|\|v\| + \|\lambda v + w\| \end{aligned}$$

und ebenso

$$\|\lambda v + w\| \quad = \quad \|(\lambda v + w) - (\lambda_n v + w) + (\lambda_n v + w)\| \quad \leq \quad |\lambda_n - \lambda|\|v\| + \|\lambda_n v + w\|$$

insgesamt also

$$|\|\lambda_n v + w\| - \|\lambda v + w\|| \quad \leq \quad |\lambda_n - \lambda|\|v\|.$$

Aus $\lim_n \lambda_n = \lambda$ folgt deshalb $\lim_n \|\lambda_n v + w\| = \|\lambda v + w\|$. Es gilt auch

$$\lim_{n\to\infty} \|\lambda_n v\| \quad = \quad \lim_{n\to\infty} |\lambda_n|\|v\| \quad = \quad |\lambda|\|v\|.$$

Weil die Gleichung $b(\lambda_n v,w) = \lambda_n b(v,w)$ für die $\lambda_n \in \mathbb{Q}$ bereits bewiesen wurde, erhalten wir

$$\begin{aligned} b(\lambda v,w) \quad &= \quad \tfrac{1}{2}(\|\lambda v + w\|^2 - \|\lambda v\|^2 - \|w\|^2) \quad = \quad \lim_{n\to\infty} \tfrac{1}{2}(\|\lambda_n v + w\|^2 - \|\lambda_n v\|^2 - \|w\|^2) \\ &= \quad \lim_{n\to\infty} b(\lambda_n v,w) \quad = \quad \lim_{n\to\infty} \lambda_n b(v,w) \quad = \quad \lambda b(v,w). \end{aligned}$$

Damit ist der Beweis von $b(\lambda v,w) = \lambda b(v,w)$ für alle $\lambda \in \mathbb{R}$ abgeschlossen.

§ 15. *Die Jordansche Normalform*

Inhaltsübersicht

Der Satz von Cayley-Hamilton besagt, dass jeder Endomorphismus ϕ eines endlich-dimensionalen K-Vektorraums V die Beziehung $\chi_\phi(\phi) = 0_{\mathrm{End}_K(V)}$ erfüllt; man erhält also die Nullabbildung, indem man ϕ in sein eigenes charakteristisches Polynom einsetzt. Durch diesen Satz wird die Definition des *Minimalpolynoms* μ_ϕ von ϕ nahegelegt. Es handelt sich dabei um das normierte Polynom minimalen Grades mit derselben Eigenschaft $\mu_\phi(\phi) = 0_{\mathrm{End}_K(V)}$. Dieses kann mit χ_ϕ zusammenfallen, im Allgemeinen ist es aber ein Teiler von χ_ϕ. Neben χ_ϕ erweist sich auch μ_ϕ als wichtiges Werkzeug zur Beschreibung der Endomorphismen eines Vektorraums im endlich-dimensionalen Fall.

In § 13 haben wir gesehen, dass für einen Endomorphismus ϕ eines endlich-dimensionalen K-Vektorraums V unter gewissen Bedingungen eine Basis $\mathscr{B}$ gefunden werden kann, so dass die Darstellungsmatrix von ϕ bezüglich dieser Basis Diagonalgestalt annimmt. Die erste Bedingung, das Zerfallen des charakteristischen Polynoms χ_ϕ, ist isofern unproblematisch, als dass man immer zu einem Erweiterungskörper von K übergehen kann, über dem diese Bedingung erfüllt ist. Wenn die zweite Bedingung, die Übereinstimmung von algebraischer und geometrischer Vielfachheit der Eigenwerte, verletzt ist, gibt es zwar keine Darstellungsmatrix in Diagonalform, man kann aber die Darstellungsmatrix auf eine Form bringen, die von der Diagonalgestalt nur minimal abweicht. Dies ist die *Jordansche Normalform*. Aus den Polynomen μ_ϕ und χ_ϕ lassen sich bereits wesentliche Informationen zur Gestalt der Jordanschen Normalform ablesen.

Ein wichtiges Ziel in diesem Kapitel ist die Beschreibung eines Verfahrens, dass zu einem gegebenen Endomorphismus ϕ eine geordnete Basis $\mathscr{B}$ liefert, so dass $\mathscr{M}_\mathscr{B}(\phi)$ in Jordanscher Normalform vorliegt. An die Stelle der Eigenraumzerlegung aus § 13 tritt die sogenannte *Hauptraumzerlegung*. Für jeden Hauptraum muss dann eine *Jordanbasis* ermittelt werden. Hierzu benötigen wir Informationen über die Eigenschaften *nilpotenter Endomorphismen*. Dies sind Endomorphismen ψ mit der Eigenschaft, dass eine gewissen Potenz ψ^p gleich Null ist.

Wichtige Begriffe und Sätze

- Minimalpolynom μ_ϕ eines Endomorphismus ϕ
- Minimalpolynom μ_A einer Matrix A
- Satz von Caley-Hamilton
- Begleitmatrix A_f eines Polynoms $f \in K[x]$
- Jordanmatrix, Jordanblock, Jordansche Normalform
- nilpotenter Endomorphismus, nilpotente Matrix,
  Nilpotenzgrad einer Matrix bzw. eines Endomorphismus
- Jordankette und Jordanbasis
- Hauptraum einer Matrix bzw. eines Endomorphismus
  zu einem Eigenwert
- Satz von der Hauptraumzerlegung
- Existenz und Eindeutigkeit der Jordanschen Normalform einer Matrix

Sei $n \in \mathbb{N}$, K ein Körper und $A \in \mathscr{M}_{n,K}$. Dann können wir jedem Polynom $f \in K[x]$ der Form $f = a_n x^n + \ldots + a_1 x + a_0$ eine Matrix zuordnen, und zwar durch

$$f(A) \quad = \quad a_n A^n + \ldots + a_1 A + a_0 E^{(n)}.$$

In der Algebra-Vorlesung wird gezeigt, dass durch die Zuordnung $K[x] \to \mathscr{M}_{n,K}$, $f \mapsto f(A)$ ein Ringhomomorphismus gegeben ist, den wir dort als ***Einsetzungshomomorphismus*** bezeichnen. Auf Grund der Homomorphismus-Eigenschaft gilt $(f+g)(A) = f(A) + g(A)$ und $(fg)(A) = f(A) \circ g(A)$ für alle $f, g \in K[x]$.

Ist V ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$, dann können wir ebenso jedem Polynom $f \in K[x]$ der oben angebenen Form einen neuen Endomorphismus

$$f(\phi) \quad = \quad a_n \cdot \phi^n + \ldots + a_1 \cdot \phi + a_0 \cdot \mathrm{id}_V$$

aus $\mathrm{End}_K(V)$ zuordnen, wobei ϕ^ℓ für $\ell \in \mathbb{N}_0$ rekursiv durch $\phi^0 = \mathrm{id}_V$ und $\phi^{\ell+1} = \phi \circ \phi^\ell$ definiert ist. Hier gilt entsprechend $(f+g)(\phi) = f(\phi) + g(\phi)$ und $(fg)(\phi) = f(\phi) \circ g(\phi)$ für alle $f, g \in K[x]$.

Sei $n \in \mathbb{N}$, V ein n-dimensionaler K-Vektorraum und $\mathscr{B}$ eine geordnete Basis von V. In Satz (11.12) wurde gezeigt, dass $\mathscr{M}_{\mathscr{B}}$ die Komposition linearer Abbildungen in das Matrixprodukt überführt, d.h. es gilt $\mathscr{M}_{\mathscr{B}}(\psi \circ \phi) = \mathscr{M}_{\mathscr{B}}(\psi)\mathscr{M}_{\mathscr{B}}(\phi)$ für alle $\phi, \psi \in \mathrm{End}_K(V)$. Unmittelbar daraus ergibt sich, dass $\mathscr{L}_{\mathscr{B}}$ das Matrixprodukt in die Komposition linearer Abbildungen übersetzt. Sind nämlich $A, B \in \mathscr{M}_{n,K}$ vorgegeben, und wenden wir $\mathscr{L}_{\mathscr{B}}$ auf die Gleichung

$$\mathscr{M}_{\mathscr{B}}(\mathscr{L}_{\mathscr{B}}(A) \circ \mathscr{L}_{\mathscr{B}}(B)) \quad = \quad \mathscr{M}_{\mathscr{B}}(\mathscr{L}_{\mathscr{B}}(A))\mathscr{M}_{\mathscr{B}}(\mathscr{L}_{\mathscr{B}}(B)) \quad = \quad AB$$

an, so erhalten wir $\mathscr{L}_{\mathscr{B}}(A) \circ \mathscr{L}_{\mathscr{B}}(B) = \mathscr{L}_{\mathscr{B}}(AB)$.

(15.1) Lemma Sei $f \in K[x]$ ein beliebiges Polynom.

(i) Für alle $\phi \in \mathrm{End}_K(V)$ gilt $\mathscr{M}_{\mathscr{B}}(f(\phi)) = f(\mathscr{M}_{\mathscr{B}}(\phi))$.

(ii) Für alle $A \in \mathscr{M}_{n,K}$ gilt $\mathscr{L}_{\mathscr{B}}(f(A)) = f(\mathscr{L}_{\mathscr{B}}(A))$.

Beweis: Wir beschränken uns auf den Beweis der ersten Gleichung, da der Beweis der zweiten Gleichung weitgehend analog verläuft. Ist $f = a_n x^n + \ldots + a_1 x + a_0$ mit $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in K$ dann gilt

$$\mathscr{M}_{\mathscr{B}}(f(\phi)) \quad = \quad \mathscr{M}_{\mathscr{B}}\left(\sum_{k=0}^{n} a_k \phi^k\right) \quad = \quad \sum_{k=0}^{n} a_k \cdot \mathscr{M}_{\mathscr{B}}(\phi)^k \quad = \quad f(\mathscr{M}_{\mathscr{B}}(\phi)). \qquad \square$$

(15.2) Proposition Sei V ein endlich-dimensionaler K-Vektorraum. Für jedes $\phi \in \mathrm{End}_K(V)$ gibt es ein Polynom $0_K \neq f \in K[x]$ mit $f(\phi) = 0_{\mathrm{End}_K(V)}$.

Beweis: Nach Folgerung (11.10) ist mit V auch $\mathrm{End}_K(V)$ ein endlich-dimensionaler K-Vektorraum. Dies bedeutet, dass das Tupel $(\phi^0, \ldots, \phi^n)$ für hinreichend großes n linear abhängig ist. Es gibt also ein $n \in \mathbb{N}_0$ und Koeffizienten $a_0, a_1, \ldots, a_n \in K$, nicht alle gleich Null, mit $a_0\phi^0 + a_1\phi^1 + \ldots + a_n\phi^n = 0_{\mathrm{End}_K(V)}$. Setzen wir $f = \sum_{k=0}^{n} a_k x^k$, dann gilt $f(\phi) = 0_{\mathrm{End}_K(V)}$ und $f \neq 0_K$. $\square$

(15.3) Definition Sei V ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$. Ist $f \in K[x]$ ein normiertes Polynom minimalen Grades mit der Eigenschaft $f(\phi) = 0_{\mathrm{End}_K(V)}$, so nennt man es ein ***Minimalpolynom*** von ϕ.

(15.4) Satz Sei V ein endlich-dimensionaler K-Vektorraum. Für jedes $\phi \in \mathrm{End}_K(V)$ gibt es genau ein Minimalpolynom, das wir mit μ_ϕ bezeichnen. Ist $f \in K[x]$ ein beliebiges Polynom mit $f(\phi) = 0_{\mathrm{End}_K(V)}$, dann ist μ_ϕ ein Teiler von f.

Beweis: Zunächst beweisen wir die Existenz. Nach Prop. (15.2) gibt es jedenfalls ein Polynom $f \neq 0_K$ mit $f(\phi) = 0_{\mathrm{End}_K(V)}$. Gehen wir davon aus, dass f unter allen Polynomen mit dieser Eigenschaft minimalen Grad besitzt, und ist $c \in K$ der Leitkoeffizient von f, dann ist $c^{-1}f$ ein Minimalpolynom von ϕ.

Nun beweisen wir die Eindeutigkeit. Seien $f, g \in K[x]$ zwei verschiedene Minimalpolynome von ϕ. Dann gilt $\mathrm{grad}(f) = \mathrm{grad}(g)$, und weil f, g beide normiert sind, hat das Polynom $h = f - g \neq 0_K$ einen kleineren Grad als f und g. Sei $c \in K$ der Leitkoeffizient von h und $\tilde{h} = c^{-1}h$. Dann ist $\tilde{h}$ normiert, und es gilt

$$\tilde{h}(\phi) \quad = \quad c^{-1}(f(\phi) - g(\phi)) \quad = \quad c^{-1}\left(0_{\mathrm{End}_K(V)} - 0_{\mathrm{End}_K(V)}\right) \quad = \quad 0_{\mathrm{End}_K(V)}.$$

Aber dies widerspricht der Minimalitätseigenschaft von f und g. Also kann es keine zwei verschiedenen Minimalpolynome geben.

Zum Beweis der letzten Aussage sei $f \in K[x]$ ein Polynom mit $f(\phi) = 0_{\mathrm{End}_K(V)}$. Division mit Rest liefert Polynome $q, r \in K[x]$ mit $f = q\mu_\phi + r$, wobei entweder $r = 0_K$ oder $r \neq 0_K$ und $\mathrm{grad}(r) < \mathrm{grad}(\mu_\phi)$ gilt. Nehmen wir an, dass der zweite Fall vorliegt, und dass $c \in K$ der Leitkoeffizient von r ist. Dann erhalten wir $r(\phi) = (f - q\mu_\phi)(\phi) = f(\phi) - q(\phi) \circ \mu_\phi(\phi) = f(\phi) - q(\phi) \circ 0_{\mathrm{End}_K(V)} = 0_{\mathrm{End}_K(V)} - 0_{\mathrm{End}_K(V)} = 0_{\mathrm{End}_K(V)}$. Setzen wir $\tilde{r} = c^{-1}r$, dann ist $\tilde{r}$ normiert, und es gilt ebenso $\tilde{r}(\phi) = 0_{\mathrm{End}_K(V)}$. Aber dies steht im Widerspruch zur Minimalitätseigenschaft von μ_ϕ, wodurch nur die Möglichkeit $r = 0_K$ übrig bleibt. Es gilt also $f = q\mu_\phi$, damit ist μ_ϕ ein Teiler von f. □

Ebenso können wir für jede Matrix $A \in \mathscr{M}_{n,K}$ das ***Minimalpolynom*** $\mu_A \in K[x]$ definieren als das eindeutig bestimmte normierte Polynom minimalen Grades mit $\mu_A(A) = 0$. Die Eindeutigkeit von μ_A kann fast wörtlich genauso bewiesen werden wie in Satz (15.4), ebenso die Tatsache, dass jedes Polynom $f \in K[x]$ mit $f(A) = 0_{\mathscr{M}_{n,K}}$ von μ_A geteilt wird.

Wie wir im Beweis von Proposition (13.14) gesehen haben, haben ähnliche Matrizen $A, B \in \mathscr{M}_{n,K}$ dasselbe charakteristische Polynom, es gilt also $\chi_A = \chi_B$. Ebenso gilt $\mu_A = \mu_B$. Für den Beweis genügt es zu überprüfen, dass für jedes Polynom $f \in K[x]$ die Äquivalenz $f(A) = 0_{\mathscr{M}_{n,K}} \Leftrightarrow f(B) = 0_{\mathscr{M}_{n,K}}$ erfüllt ist. Denn dann ist das eindeutig bestimmte normierte Polynom minimalen Grades mit A als Nullstelle zugleich das eindeutig bestimmte normierte Polynom minimalen Grades mit B als Nullstelle. Für den Beweis der Äquivalenz sei $f \in K[x]$ mit $f = \sum_{k=0}^{n} a_k x^k$ vorgegeben. Auf Grund der Ähnlichkeit von A und B existiert eine Matrix $T \in \mathrm{GL}_n(K)$ mit $B = TAT^{-1}$. Wie man durch vollständige

Induktion leicht überprüft, gilt $B^k = TA^kT^{-1}$ für alle $k \in \mathbb{N}_0$. Daraus folgt

$$f(B) \quad = \quad \sum_{k=0}^{n} a_k B^k \quad = \quad \sum_{k=0}^{n} a_k TA^kT^{-1} \quad = \quad T\left(\sum_{k=0}^{n} a_k A^k\right)T^{-1} \quad = \quad Tf(A)T^{-1}.$$

Ist nun $f(A) = 0_{\mathscr{M}_{n,K}}$, dann folgt $f(B) = T0_{\mathscr{M}_{n,K}}T^{-1} = 0_{\mathscr{M}_{n,K}}$, und ist $f(B) = 0_{\mathscr{M}_{n,K}}$, dann folgt umgekehrt $f(A) = T^{-1}0_{\mathscr{M}_{n,K}}T$.

Der Satz von Cayley-Hamilton besagt, dass für jeden Endomorphismus ϕ eines endlich-dimensionalen K-Vektorraums V jeweils $\chi_\phi(\phi) = 0_{\mathrm{End}_K(V)}$ gilt, wobei χ_ϕ wie in § 13 das charakteristische Polynom von ϕ bezeichnet. Aus Satz (15.4) ergibt sich dann unmittelbar, dass μ_ϕ stets ein Teiler von χ_ϕ ist. Zum Beweis dieses Satzes sind einige Vorbereitungen erforderlich.

(15.5) Satz Für jedes normierte, nicht-konstante Polynom $f = x^n + \sum_{k=0}^{n-1} a_k x_k \in K[x]$ bezeichnet man die Matrix $A_f \in \mathscr{M}_{n,K}$ gegeben durch

$$A_f \quad = \quad \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

als ***Begleitmatrix*** von f. Diese erfüllt die Beziehung $\chi_{A_f} = f$.

Beweis: Nach Definition des charakteristischen Polynoms gilt

$$\chi_{A_f} \quad = \quad \det \begin{pmatrix} x & & & & a_0 \\ -1 & x & & & a_1 \\ & -1 & \ddots & & \vdots \\ & & \ddots & x & a_{n-2} \\ & & & -1 & x + a_{n-1} \end{pmatrix}.$$

Wir berechnen diese Determinante durch Entwicklung zur n-ten Spalte. Sei $k \in \{2, \ldots, n-1\}$. Streichen wir in der Matrix die k-te Zeile und die n-te Spalte, dann hat die Restmatrix die Blockgestalt

$$\begin{pmatrix} B_k & 0 \\ 0 & C_k \end{pmatrix} \qquad \text{mit} \qquad B_k = \begin{pmatrix} x & & & \\ -1 & x & & \\ & \ddots & \ddots & \\ & & -1 & x \end{pmatrix} \quad \text{und} \quad C_k = \begin{pmatrix} -1 & x & & \\ & -1 & \ddots & \\ & & \ddots & x \\ & & & -1 \end{pmatrix}$$

wobei $B_k \in \mathscr{M}_{k-1,K}$ und $C_k \in \mathscr{M}_{n-k,K}$ ist. Für die Determinante der oberen Dreiecksmatrix C_k erhalten wir mit Satz (12.18) den Wert $\det C_k = (-1)^{n-k}$, und mit Satz (12.19) erhalten wir $\det B_k = \det {}^{\mathrm{t}}B_k = x^{k-1}$. Die Formel für die Determinaten von Blockmatrizen aus Satz (12.23) liefert ingesamt den Wert $(\det B_k)(\det C_k) = (-1)^{n-k}x^{k-1}$ für die Restmatrix. Der entsprechende Summand im Laplace'schen Entwicklungssatz, Satz (12.28), ist dann $(-1)^{n+k}a_{k-1}(-1)^{n-k}x^{k-1} =$

$a_{k-1}x^{k-1}$. Ebenso sieht man, dass für $k = 1$ der Summand $(-1)^{n+1}a_0(-1)^{n-1} = a_0$ und für $k = n$ der Summand $(-1)^{2n}(x + a_{n-1})x^{n-1} = x^n + a_{n-1}x^{n-1}$ herauskommt; in diesen beiden Fällen gibt es jeweils nur einen Block. Insgesamt erhalten wir also die Determinante

$$x^n + a_{n-1}x^{n-1} + \sum_{k=2}^{n-1} a_{k-1}x^{k-1} + a_0 \quad = \quad x^n + a_{n-1}x^{n-1} + \sum_{k=1}^{n-2} a_k x^k + a_0 \quad = \quad f. \qquad \square$$

Als weitere Vorbereitung müssen wir eine weitere Klassen von Minimalpolynomen einführen, die für ein $\phi \in \mathrm{End}_K(V)$ den einzelnen Elementen $v \in V$ zugeordnet sind.

> **(15.6) Proposition** Sei V ein endlich-dimensionaler K-Vektorraum. Für jedes $\phi \in \mathrm{End}_K(V)$ und jeden Vektor $0_V \neq v \in V$ gibt es ein eindeutig bestimmtes, normiertes Polynom $\mu_{\phi,v}$ minimalen Grades mit $\mu_{\phi,v}(\phi)(v) = 0_V$. Wir nennen es das Minimalpolynom von ϕ bezüglich v. Jedes $f \in K[x]$ mit $f(\phi)(v) = 0_V$ ist ein Vielfaches von $\mu_{\phi,v}$.

Beweis: Der Beweis verläuft weitgehend parallel zum Beweis von Prop. (15.2) und von Satz (15.4). Zunächst zeigen wir, dass es zumindest ein Polynom $f \in K[x]$ ungleich 0 mit $f(\phi)(v) = 0$ gibt. Weil V endlich-dimensional ist, muss das Tupel $(\phi^0(v), ..., \phi^n(v))$ für hinreichend großes n linear abhängig sein. Es gibt also ein $n \in \mathbb{N}_0$ und Koeffizienten $a_0, a_1, ..., a_n \in K$, nicht alle gleich Null, mit

$$a_0\phi^0(v) + a_1\phi^1(v) + ... + a_n\phi^n(v) \quad = \quad 0_{\mathrm{End}_K(V)}.$$

Nach eventueller Verkleinerung von n können wir $a_n \neq 0$ annehmen. Setzen wir $f = \sum_{k=0}^{n} a_k x^k$, dann gilt $f(\phi)(v) = 0_V$ und $f \neq 0_K$ wie gewünscht. Ersetzen wir f durch $a_n^{-1}f$, so erhalten wir ein normiertes Polynom f mit $f(\phi)(v) = 0_V$. Wir wählen unter allen normierten Polynomen mit dieser Eigenschaft eines von minimalem Grad und bezeichnen es mit $\mu_{\phi,v}$.

Zum Nachweis der Eindeutigkeit von $\mu_{\phi,v}$ nehmen wir an, dass $g \in K[x]$ ein weiteres normiertes Polynom mit $g(\phi)(v) = 0_V$ ist, das denselben Grad besitzt wie $\mu_{\phi,v}$. Dann gilt $(g - \mu_{\phi,v})(\phi)(v) = (g(\phi) - \mu_{\phi,v}(\phi))(v) = g(\phi)(v) - \mu_{\phi,v}(\phi)(v) = 0_V - 0_V = 0_V$. Ist $g \neq \mu_{\phi,v}$, dann erhalten wir durch Normierung von $g - \mu_{\phi,v}$ ein normiertes Polynom $h \in K[x]$ kleineren Grades als $\mu_{\phi,v}$ mit $h(\phi)(v) = 0_V$, was aber der Minimalitätseigenschaft von $\mu_{\phi,v}$ widerspricht. Damit ist die Eindeutigkeit von $\mu_{\phi,v}$ nachgewiesen.

Sei nun $f \in K[x]$ ein beliebiges Polynom mit $f(\phi)(v) = 0_V$. Durch Division mit Rest erhalten wir Polynome $q, r \in K[x]$ mit $f = q\mu_{\phi,v} + r$, wobei $r = 0_K$ oder $r \neq 0_K$ und $\mathrm{grad}(r) < \mathrm{grad}(\mu_{\phi,v})$ gilt. Im ersten Fall ist $\mu_{\phi,v}$ ein Teiler von f. Im zweiten Fall gilt $r(\phi)(v) = f(\phi)(v) - (q\mu_{\phi,v})(\phi)(v) = f(\phi)(v) - (q(\phi) \circ \mu_{\phi,v}(\phi))(v) = 0_V - q(\phi)(0_V) = 0_V$, und durch Normierung von r erhalten wir ein normiertes Polynom mit derselben Eigenschaft. Dies würde erneut einen Widerspruch zur Minimalitätseigenschaft von $\mu_{\phi,v}$ bedeuten, weshalb der zweite Fall ausgeschlossen ist. $\square$

Aus Proposition (15.6) ergibt sich unmittelbar, dass $\mu_{\phi,v}$ für jedes $v \in V$ mit $v \neq 0_V$ ein Teiler von μ_ϕ ist, denn es gilt $\mu_\phi(\phi)(v) = 0_{\mathrm{End}_K(V)}(v) = 0_V$.

(15.7) Satz *(Satz von Cayley-Hamilton)*

Sei V ein endlich-dimensionaler K-Vektorraum, $\phi \in \mathrm{End}_K(V)$ und χ_ϕ sein charakteristisches Polynom. Dann gilt $\chi_\phi(\phi) = 0_{\mathrm{End}_K(V)}$.

Beweis: Offenbar genügt es, $\chi_\phi(\phi)(v) = 0_V$ für jedes Vektor $v \in V$ mit $v \neq 0_V$ nachzuweisen. Sei also ein solcher Vektor v vorgegeben. Wenn wir zeigen können, dass χ_ϕ ein Vielfaches von $f = \mu_{\phi,v}$ ist, also $\chi_\phi = gf$ für ein $g \in K[x]$ gilt, dann folgt wegen $\chi_\phi(\phi) = g(\phi) \circ f(\phi)$ und $f(\phi)(v) = 0_V$ die Gleichung

$$\chi_\phi(\phi)(v) \quad = \quad (g(\phi) \circ f(\phi))(v) \quad = \quad g(\phi)(0_V) \quad = \quad 0_V.$$

Wir zeigen nun, dass χ_ϕ tatsächlich ein Vielfaches von f ist, indem wir die Darstellungsmatrix von χ_ϕ bezüglich einer geeigneten Basis berechnen. Sei dazu $v_k = \phi^{k-1}(v)$ für $1 \leq k \leq n$, wobei $n = \mathrm{grad}(f)$ ist. Zunächst überprüfen wir, dass das Tupel $\mathscr{A} = (v_1, ..., v_n)$ linear unabhängig ist. Wäre es linear abhängig, dann gäbe es Koeffizienten $b_0, ..., b_{n-1} \in K$, nicht alle gleich Null, mit

$$\sum_{k=0}^{n-1} b_k \phi^k(v) \quad = \quad \sum_{k=0}^{n-1} b_k v_{k+1} \quad = \quad 0_V.$$

Für das Polynom $g = \sum_{k=0}^{n-1} b_k x^k$ würde dann $g(\phi)(v) = 0_V$ gelten, was wegen $\mathrm{grad}(g) < \mathrm{grad}(f)$ im Widerspruch zur Minimalitätseigenschaft des Polynoms f steht. Damit ist die lineare Unabhängigkeit bewiesen. Wir ergänzen nun $\mathscr{A}$ durch Vektoren $w_1, ..., w_r$ zu einer Basis $\mathscr{B}$ von V und bestimmen die Darstellungsmatrix $A = \mathscr{M}_{\mathscr{B}}(\phi)$. Dazu schreiben wir das Polynom f in der Form $f = x^n + \sum_{k=0}^{n-1} a_k x^k$ und definieren den Untervektorraum $U = \langle v_1, ..., v_n \rangle_K$ von V. Für $1 \leq k < n$ gilt $\phi(v_k) = \phi(\phi^{k-1}(v)) = \phi^k(v) = v_{k+1} \in U$, und aus

$$\phi(v_n) + \sum_{k=1}^{n} a_{k-1} v_k \quad = \quad \phi^n(v) + \sum_{k=0}^{n-1} a_k \phi^k(v) \quad = \quad \left(\phi^n + \sum_{k=0}^{n-1} a_k \phi^k\right)(v) \quad = \quad f(\phi)(v) \quad = \quad 0_V$$

folgt $\phi(v_n) = -\sum_{k=1}^{n} a_{k-1} v_k \in U$. Die Rechnung zeigt, dass $\phi(U) \subseteq U$ gilt, und dass die Darstellungsmatrix von $\phi|_U$ bezüglich der Basis $\mathscr{A}$ genau mit der Begleitmatrix $A_f \in \mathscr{M}_{n,K}$ von f übereinstimmt. Daraus folgt, dass A eine Blockgestalt der Form

$$A \quad = \quad \begin{pmatrix} A_f & B \\ 0 & C \end{pmatrix}$$

besitzt, mit geeigneten Matrizen $B \in \mathscr{M}_{n \times r,K}$ und $C \in \mathscr{M}_{r,K}$. Mit der Formel für die Determinante von Blockmatrizen aus Satz (12.23) und mit Satz (15.5) erhalten wir

$$\begin{aligned} \chi_\phi \quad = \quad \chi_A \quad = \quad \det(xE^{(n+r)} - A) \quad = \quad \det\begin{pmatrix} xE^{(n)} - A_f & B \\ 0 & xE^{(r)} - C \end{pmatrix} \\ = \quad \det(xE^{(n)} - A_f) \cdot \det(xE^{(r)} - C) \quad = \quad \chi_{A_f} \cdot \chi_C \quad = \quad f \cdot \chi_C. \end{aligned}$$

Dies zeigt, dass χ_ϕ tatsächlich ein Vielfaches von f ist. □

(15.8) Folgerung Für alle $A \in \mathscr{M}_{n,K}$ gilt $\chi_A(A) = 0_{\mathscr{M}_{n,K}}$.

Beweis: Nach Satz (15.7) gilt $\chi_{\phi_A}(\phi_A) = 0_{\mathrm{End}_K(V)}$ für den Endomorphismus ϕ_A des Vektorraums $V = K^n$. Nach Proposition (11.8) gilt $A = \mathscr{M}_{\mathscr{E}}(\phi_A)$, außerdem gilt $\chi_{\phi_A} = \chi_A$, nach Definition des charakteristischen Polynoms eines Endomorphismus. Es folgt $\chi_A(A) = \chi_{\phi_A}(A) = \chi_{\phi_A}(\mathscr{M}_{\mathscr{E}}(\phi_A)) = \mathscr{M}_{\mathscr{E}}(\chi_{\phi_A}(\phi_A)) = \mathscr{M}_{\mathscr{E}}(0_{\mathrm{End}_K(V)}) = 0_{\mathscr{M}_{n,K}}$. □

Neben der Eigenschaft, ein Teiler des charakteristischen Polynoms χ_ϕ zu seien, besitzt μ_ϕ mit χ_ϕ noch die folgende Gemeinsamkeit.

(15.9) Proposition Für jeden endlich-dimensionalen K-Vektorraum V und jedes $\phi \in \mathrm{End}_K(V)$ sind die Nullstellen von μ_ϕ genau die Eigenwerte von ϕ.

Beweis: Sei λ ein Eigenwert von ϕ und $v \in V$ ein Eigenvektor zum Eigenwert λ. Dann gilt $(\phi - \lambda \mathrm{id}_V)(v) = 0_V$. Also ist $\mu_{\phi,v}$ ein Teiler von $x - \lambda$, und weil der Grad von $x - \lambda$ bereits minimal ist, muss $\mu_{\phi,v} = x - \lambda$ gelten. Wegen $\mu_{\phi,v} | \mu_\phi$ ist λ damit eine Nullstelle von μ_ϕ. Sei umgekehrt λ eine Nullstelle von μ_ϕ. Dann gibt es ein $f \in K[x]$ mit $\mu_\phi = (x - \lambda) f$. Es muss einen Vektor v mit $f(\phi)(v) \neq 0_V$ geben, weil ansonsten $f(\phi) = 0_{\mathrm{End}_K(V)}$ im Widerspruch zur Minimalität von μ_ϕ stehen würde. Setzen wir $w = f(\phi)(v)$, dann folgt

$$(\phi - \lambda \mathrm{id}_V)(w) \quad = \quad ((\phi - \lambda \mathrm{id}_V) \circ f(\phi))(v) \quad = \quad \mu_\phi(\phi)(v) \quad = \quad 0_{\mathrm{End}_K(V)}(v) \quad = \quad 0_V$$

und somit $\phi(w) = \lambda \mathrm{id}_V(w) = \lambda w$. Also ist w ein Eigenvektor von ϕ zum Eigenwert λ. □

(15.10) Definition Eine Matrix $J \in \mathscr{M}_{n,K}$ heißt ***Jordanmatrix*** zum Eigenwert $\lambda \in K$, wenn sie die Form

$$J \quad = \quad \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix} \qquad \text{besitzt.}$$

In kleiner Dimension sind die Jordanmatrizen zum Eigenwert λ also gegeben durch

$$\begin{pmatrix} \lambda \end{pmatrix} \quad , \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad , \quad \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} \quad , \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Eine Matrix $A \in \mathscr{M}_{n,K}$ befindet sich in ***Jordanscher Normalform***, wenn sie als Blockmatrix in der Form

$$A \quad = \quad \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_r \end{pmatrix} \qquad \text{mit Jordanmatrizen} \quad J_1, \ldots, J_r \quad \text{schreiben lässt.}$$

Man bezeichnet die $J_1, \ldots, J_r$ dann als ***Jordanblöcke*** der Matrix A. Zum Beispiel setzt sich die Matrix

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

aus den Jordanblöcken

$$J_1 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \quad , \quad J_2 = \begin{pmatrix} 2 \end{pmatrix} \quad \text{und} \quad J_3 = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \quad \text{zusammen.}$$

(15.11) Proposition Sei V ein n-dimensionaler K-Vektorraum, $\psi \in \mathrm{End}_K(V)$ und $\mathscr{B}$ eine geordnete Basis mit der Eigenschaft, dass $J = \mathscr{M}_{\mathscr{B}}(\psi)$ eine Jordanmatrix zum Eigenwert $\lambda \in K$ ist. Dann gilt

(i) Der einzige Eigenwert von ψ ist λ. Die algebraische und die geometrische Vielfachheit dieses Eigenwerts sind durch $\mu_a(\psi, \lambda) = n$ und $\mu_g(\psi, \lambda) = 1$ gegeben.

(ii) Es gilt $\mu_\psi = \chi_\psi = (x - \lambda)^n$.

Beweis: Die Jordanmatrix $J \in \mathscr{M}_{n,K}$ ist eine obere Dreiecksmatrix, deren sämtliche Hauptdiagonaleinträge mit λ übereinstimmen. Daraus folgt $\chi_\psi = \chi_J = \det(xE^{(n)} - J) = (x-\lambda)^n$. Da die Eigenwerte von ψ genau die Nullstellen von χ_ψ sind, ist λ der einzige Eigenwert von ψ, und weil λ eine Nullstelle der Vielfachheit n von χ_ψ ist, gilt $\mu_a(\psi, \lambda) = n$. Die Darstellungsmatrix von $\psi - \lambda \cdot \mathrm{id}_V$ ist gegeben durch

$$\mathscr{M}_{\mathscr{B}}(\psi - \lambda \cdot \mathrm{id}_V) = J - \lambda E^{(n)} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Seien $v_1, \ldots, v_n$ die Elemente der geordneten Basis $\mathscr{B}$. An den Spalten der Matrix $\mathscr{M}_{\mathscr{B}}(\psi - \lambda \cdot \mathrm{id}_V)$ kann abgelesen werden, dass $(\psi - \lambda \cdot \mathrm{id}_V)(v_1) = 0_V$ und $(\psi - \lambda \cdot \mathrm{id}_V)(v_k) = v_{k-1}$ für $2 \leq k \leq n$ gilt. Es gilt also insbesondere $(\psi - \lambda \cdot \mathrm{id}_V)^{n-1}(v_n) = v_1 \neq 0_V$. Das Minimalpolynom μ_ψ ist, wie wir im Anschluss an Satz (15.4) festgestellt haben, ein Teiler von $\chi_\psi = (x-\lambda)^n$, aber wegen $(\psi - \lambda \cdot \mathrm{id}_V)^{n-1} \neq 0_{\mathrm{End}_K(V)}$ ist ψ keine Nullstelle von $(x-\lambda)^{n-1}$, und folglich kann μ_ψ kein echter Teiler von $(x-\lambda)^n$ sein. Damit ist die Gleichung $\mu_\psi = (x-\lambda)^n$ nachgewiesen. Schließlich zeigen die Gleichungen $(\psi - \lambda \cdot \mathrm{id}_V)(v_1) = 0_V$ und $(\psi - \lambda \cdot \mathrm{id}_V)(v_k) = v_{k-1}$ für $2 \leq k \leq n$ auch, dass $\dim \mathrm{im}(\psi - \lambda \cdot \mathrm{id}_V) = n-1$ gilt, denn das Bild von $\psi - \lambda \cdot \mathrm{id}_V$ stimmt mit $\mathrm{lin}\{v_2, \ldots, v_n\}$ überein. Der Dimensionssatz für lineare Abbildungen liefert $\mu_g(\psi, \lambda) = \dim \mathrm{Eig}(\psi, \lambda) = \dim \ker(\psi - \lambda \cdot \mathrm{id}_V) = n - \dim \mathrm{im}(\psi - \lambda \cdot \mathrm{id}_V) = n - (n-1) = 1$. □

(15.12) Lemma Sei V ein K-Vektorraum mit einer Zerlegung $V = U_1 \oplus ... \oplus U_r$ als direkte Summe von Untervektorräumen $U_i \leq V$, und sei $\psi \in \mathrm{End}_K(V)$ mit $\psi(U_i) \subseteq U_i$ für $1 \leq i \leq r$. Dann gilt für jedes $\lambda \in K$ jeweils

$$\mathrm{Eig}(\psi, \lambda) \quad = \quad \mathrm{Eig}(\psi|_{U_1}, \lambda) \oplus ... \oplus \mathrm{Eig}(\psi|_{U_r}, \lambda).$$

Beweis: Zunächst bemerken wir, dass die Summe auf der rechten Seite der Gleichung tatsächlich eine direkte Summe ist. Denn nach Voraussetzung gilt $U_j \cap (\sum_{k \neq j} U_k) = \{0_V\}$ für alle j, wegen $\mathrm{Eig}(\psi|_{U_j}, \lambda) \subseteq U_j$ für $1 \leq j \leq r$ also erst recht $\mathrm{Eig}(\psi|_{U_j}, \lambda) \cap (\sum_{k \neq j} \mathrm{Eig}(\psi|_{U_k}, \lambda)) = \{0_V\}$. Die Inklusion „$\supseteq$“ ist offensichtlich erfüllt, denn für jeden Vektor $v \in \mathrm{Eig}(\psi|_{U_j}, \lambda)$ mit $j \in \{1, ..., r\}$ gilt insbesondere $v \in U_j$ und somit $\psi(v) = (\psi|_{U_j})(v) = \lambda v$. Zum Nachweis von „$\subseteq$“ sei $v \in V$ vorgegeben. Auf Grund der direkten Summenzerlegung von V gibt es Elemente $u_j \in U_j$ für $1 \leq j \leq r$, so dass $v = u_1 + ... + v_r$ erfüllt ist. Es gilt nun

$$\sum_{j=1}^{r} \psi(u_j) \quad = \quad \psi\left(\sum_{j=1}^{r} u_j\right) \quad = \quad \psi(v) \quad = \quad \lambda v \quad = \quad \lambda \cdot \left(\sum_{j=1}^{r} u_j\right) \quad = \quad \sum_{j=1}^{r} \lambda u_j.$$

Auf Grund der Eindeutigkeit der Darstellung von Elementen in direkten Summen (siehe Satz (10.4), Teil (ii)) folgt $\psi(u_j) = \lambda u_j$ und somit $u_j \in \mathrm{Eig}(\psi|_{U_j}, \lambda)$ für $1 \leq j \leq r$. Damit ist v in der direkten Summe auf der rechten Seite der Gleichung enthalten. □

(15.13) Satz Sei V ein n-dimensionaler K-Vektorraum, $\psi \in \mathrm{End}_K(V)$ und $\mathscr{B}$ eine geordnete Basis mit der Eigenschaft, dass $A = \mathscr{M}_{\mathscr{B}}(\psi)$ in Jordanscher Normalform vorliegt. Sei $\lambda \in K$ ein Eigenwert von ψ. Dann gilt

(i) Sowohl χ_ψ als auch μ_ψ zerfallen in Linearfaktoren.

(ii) Die geometrische Vielfachheit $\mu_g(\psi, \lambda)$ ist gleich der Anzahl aller Jordanblöcke von A zum Eigenwert λ.

(iii) Die algebraische Vielfachheit $\mu_a(\psi, \lambda)$ ist gleich der Summe der Größen aller Jordanblöcke von A zum Eigenwert λ.

(iv) Die Vielfachheit von λ als Nullstelle von μ_ψ ist gleich der Größe des größten Jordanblocks zum Eigenwert λ.

Beweis: Seien $J_1, ..., J_r$ die Jordanblöcke von A. Für $1 \leq i \leq r$ sei $\lambda_i \in K$ der Eigenwert und $s_i \in \mathbb{N}$ die Größe von J_i. Wir setzen $n_0 = 0$ und $n_i = \sum_{k=1}^{i} s_k$ für $1 \leq i \leq r$; dann gilt insbesondere $n_r = \sum_{k=1}^{r} s_k = n$, und außerdem $s_i = n_i - n_{i-1}$ für $1 \leq i \leq r$. Ist $\mathscr{B} = (v_1, ..., v_n)$ die geordnete Basis von V, dann setzen wir $\mathscr{B}_i = (v_{n_{i-1}+1}, ..., v_{n_i-1}, v_i)$ und $U_i = \langle \mathscr{B}_i \rangle_k$ für $1 \leq i \leq r$. Der i-te Jordanblock J_i befindet sich dann jeweils in den Zeilen und Spalten der Matrix A mit den Nummern $n_{i-1} + 1, n_{i-1} + 2, ..., n_i$. Für jedes $j \in \{n_{i-1} + 1, ..., n_i\}$ hat die j-te Spalte Einträge ungleich Null also nur in den Zeilen $n_{i-1} + 1$ bis n_i. Daraus folgt $\psi(v_j) \in U_i$ für $n_{i-1} + 1 \leq j \leq n_i$, insgesamt also $\psi(U_i) \subseteq U_i$, und nach Konstruktion ist $J_i = \mathscr{M}_{\mathscr{B}_i}(\psi_i|_{U_i})$.

zu (i) Jede Jordanmatrix ist eine obere Dreiecksmatrix, und weil A aus Jordanmatrizen J_i entlang der Hauptdiagonalen besteht, handelt es sich auch bei A um eine obere Dreiecksmatrix. Daraus folgt, dass $\chi_\psi = \chi_A$ in Linearfaktoren zerfällt. Wie wir im Anschluss an Satz (15.4) festgestellt haben, ist μ_ψ ein Teiler von χ_ψ. Daraus folgt, dass auch μ_ψ ein Produkt von Polynomen vom Grad 1 ist, also ebenfalls in Linearfaktoren zerfällt.

zu (ii) Für jeden Eigenwert α von ψ sei $S(\alpha) = \{i \mid \lambda_i = \alpha\}$, und es sei $i \in S(\lambda)$. Weil $J_i = \mathscr{M}_{\mathscr{B}_i}(\psi_i|_{U_i})$ eine Jordanmatrix zum Eigenwert λ ist, gilt jeweils $\dim \mathrm{Eig}(\psi|_{U_i}, \lambda) = \mu_g(\psi|_{U_i}, \lambda) = 1$ nach Prop. (15.11). Für alle $i \in \{1, ..., r\}$ mit $i \notin S(\lambda)$ gilt $\mathrm{Eig}(\psi|_{U_i}, \lambda) = \{0_V\}$ und somit $\dim \mathrm{Eig}(\psi|_{U_i}, \lambda) = 0$, denn ebenfalls nach Prop. (15.11) ist λ kein Eigenwert von $\psi|_{U_i}$. Mit Lemma (15.12) und Folgerung (10.7) erhalten wir

$$\begin{aligned}\mu_g(\psi,\lambda) &= \dim \mathrm{Eig}(\psi,\lambda) = \sum_{i=1}^{r} \dim \mathrm{Eig}(\psi|_{U_i},\lambda) = \sum_{i\in S(\lambda)} \dim \mathrm{Eig}(\psi|_{U_i},\lambda) + \sum_{i\notin S(\lambda)} \dim \mathrm{Eig}(\psi|_{U_i},\lambda) \\ &= \sum_{i\in S(\lambda)} 1 + \sum_{i\notin S(\lambda)} 0 = |S(\lambda)|.\end{aligned}$$

Aber dies ist genau die Anzahl der Jordanblöcke von A zum Eigenwert λ.

zu (iii) Nach Prop. (15.11) ist für $1 \le i \le r$ das charakteristische Polynom von $\psi|_{U_i}$ jeweils durch $(x-\lambda_i)^{s_i}$ gegeben. Weil A aus den Jordanblöcken $J_1, ..., J_r$ entlang der Hauptdiagonalen besteht, erhalten wir

$$\chi_\psi = \chi_A = \det(xE^{(n)} - A) = \prod_{i=1}^{r} \det(xE^{(s_i)} - J_i) = \prod_{i=1}^{r} \chi_{J_i} = \prod_{i=1}^{r} \chi_{\psi|_{U_i}} = \prod_{i=1}^{r} (x-\lambda_i)^{s_i}.$$

Die Vielfachheit von λ als Nullstelle von χ_ψ ist somit gegeben durch $\sum_{i\in S(\lambda)} s_i$. Dies ist die Summe der Größen s_i aller Jordanblöcke J_i mit $\lambda_i = \lambda$.

zu (iv) Für $1 \le i \le r$ gilt jeweils $\mu_{\psi|_{U_i}} = (x-\lambda_i)^{s_i}$, nach Proposition (15.11). Nach Definition des Minimalpolynoms folgt daraus folgt $(J_i - \lambda_i E^{(s_i)})^j \neq 0_{\mathscr{M}_{s_i,K}}$ für $1 \le j < s_i$ und $(J_i - \lambda_i E^{(s_i)})^j = 0_{\mathscr{M}_{s_i,K}}$ für alle $j \ge s_i$. Nach Proposition (15.9) sind die Nullstellen des Minimalpolynoms $\mu_\psi = \mu_A$ genau die Eigenwerte von A (oder ψ). Das Minimalpolynom hat also die Form $\mu_A = \prod_\alpha (x-\alpha)^{m(\alpha)}$, wobei α die Eigenwerte von ψ durchläuft und jeweils $m(\alpha) \in \mathbb{N}$ gilt. Definieren wir jeweils $m'(\alpha) = \max\{s_i \mid i \in S(\alpha)\}$, so ist das Ziel unserer Beweisführung die Übereinstimmung $m(\alpha) = m'(\alpha)$ für jeden Eigenwert α.

Die Produktmatrix $\mu_A(A) = \prod_\alpha (A - \alpha E^{(n)})^{m(\alpha)}$ besteht aus Blöcken der Größen $s_1, ..., s_r$ entlang der Hauptdiagonalen. Diese sind gegeben durch die Produkte

$$\prod_\alpha (J_i - \alpha E^{(s_i)})^{m(\alpha)} \quad \text{für } 1 \le i \le r.$$

Sei $i \in \{1, ..., r\}$. Ist $\alpha \neq \lambda_i$, dann hat die Matrix $J_i - \alpha E^{(s_i)}$ auf der Hauptdiagonalen die Einträge $\lambda_i - \alpha \neq 0$, somit ist $(J_i - \alpha E^{(s_i)})^{m(\alpha)}$ invertierbar. Das Produkt $\prod_\alpha (J_i - \alpha E^{(s_i)})^{m(\alpha)}$ ist also genau dann gleich Null, wenn der Faktor $(J_i - \lambda_i E^{(s_i)})^{m(\lambda_i)}$ gleich Null ist. Wie oben bemerkt, ist dies genau dann der Fall, wenn $m(\lambda_i) \ge s_i$ gilt.

Auf Grund der Gleichung $\mu_A(A) = 0_{\mathscr{M}_{n,K}}$ (die sich aus der Definition des Minimalpolynoms μ_A ergibt) sind nun aber *alle* Blöcke der Matrix $\mu_A(A)$ entlang der Hauptdiagonalen gleich Null. Es gilt also $m(\lambda_i) \ge s_i$ für $1 \le i \le r$, was zu $m(\alpha) \ge s_i$ für alle Eigenwerte α und alle $i \in S(\alpha)$ äquivalent ist. Daraus folgt $m(\alpha) \ge m'(\alpha)$. Aus $m'(\lambda_i) \ge s_i$ folgt

andererseits $(J_i-\lambda_i E^{(s_i)})^{m'(\lambda_i)}=0_{\mathscr{M}_{s_i,K}}$, für $1\le i\le r$. Für jedes i ist also das Produkt $\prod_\alpha (J_i-\alpha E^{(s_i)})^{m'(\alpha)}$ gleich Null, und insgesamt ist A somit eine Nullstelle des Polynoms $\prod_\alpha (x-\alpha)^{m'(\alpha)}$. Nach Satz (15.4), bzw. seinem Analogon für Matrizen, muss dieses Polynom also ein Vielfaches des Minimalpolynoms μ_A sein. Es folgt $m(\alpha)\le m'(\alpha)$, insgesamt also $m(\alpha)=m'(\alpha)$ für alle Eigenwerte α. □

Für eine 5×5-Matrix in Jordanscher Normalform mit einem einzigen Eigenwert $\lambda\in K$ gibt es somit bis auf Reihenfolge der Jordanblöcke die folgenden sechs Möglichkeiten.

$$J_1=\begin{pmatrix}\lambda&1&0&0&0\\0&\lambda&1&0&0\\0&0&\lambda&1&0\\0&0&0&\lambda&1\\0&0&0&0&\lambda\end{pmatrix}\qquad J_2=\begin{pmatrix}\lambda&1&0&0&0\\0&\lambda&1&0&0\\0&0&\lambda&1&0\\0&0&0&\lambda&0\\0&0&0&0&\lambda\end{pmatrix}\qquad J_3=\begin{pmatrix}\lambda&1&0&0&0\\0&\lambda&1&0&0\\0&0&\lambda&0&0\\0&0&0&\lambda&1\\0&0&0&0&\lambda\end{pmatrix}$$

$$\chi_{J_1}=\mu_{J_1}=(x-\lambda)^5 \qquad \chi_{J_2}=(x-\lambda)^5,\mu_{J_2}=(x-\lambda)^4 \qquad \chi_{J_3}=(x-\lambda)^5,\mu_{J_3}=(x-\lambda)^3$$
$$\mu_a(J_1,\lambda)=5,\mu_g(J_1,\lambda)=1 \qquad \mu_a(J_2,\lambda)=5,\mu_g(J_2,\lambda)=2 \qquad \mu_a(J_3,\lambda)=5,\mu_g(J_3,\lambda)=2$$

$$J_4=\begin{pmatrix}\lambda&1&0&0&0\\0&\lambda&0&0&0\\0&0&\lambda&1&0\\0&0&0&\lambda&0\\0&0&0&0&\lambda\end{pmatrix}\qquad J_5=\begin{pmatrix}\lambda&1&0&0&0\\0&\lambda&0&0&0\\0&0&\lambda&0&0\\0&0&0&\lambda&0\\0&0&0&0&\lambda\end{pmatrix}\qquad J_6=\begin{pmatrix}\lambda&0&0&0&0\\0&\lambda&0&0&0\\0&0&\lambda&0&0\\0&0&0&\lambda&0\\0&0&0&0&\lambda\end{pmatrix}$$

$$\chi_{J_4}=(x-\lambda)^5,\mu_{J_4}=(x-\lambda)^2 \qquad \chi_{J_5}=(x-\lambda)^5,\mu_{J_5}=(x-\lambda)^2 \qquad \chi_{J_6}=(x-\lambda)^5,\mu_{J_6}=x-\lambda$$
$$\mu_a(J_4,\lambda)=5,\mu_g(J_4,\lambda)=3 \qquad \mu_a(J_5,\lambda)=5,\mu_g(J_5,\lambda)=4 \qquad \mu_a(J_6,\lambda)=\mu_g(J_6,\lambda)=5$$

(15.14) Definition

(i) Sei V ein endlich-dimensionaler K-Vektorraum. Ein Endomorphismus $\psi\in \mathrm{End}_K(V)$ wird als ***nilpotent*** bezeichnet, wenn ein $p\in\mathbb{N}$ mit $\psi^p=0_{\mathrm{End}_K(V)}$ existiert. Das kleinste p mit dieser Eigenschaft nennt man den ***Nilpotenzgrad*** von ψ.

(ii) Ebenso bezeichnet man eine Matrix $A\in\mathscr{M}_{n,K}$ als nilpotent, wenn $A^p=0_{\mathscr{M}_{n,K}}$ für ein $p\in\mathbb{N}$ gilt; entsprechend ist der Nilpotenzgrad einer solchen Matrix definiert.

Beispielsweise ist $A=\begin{pmatrix}0&1\\0&0\end{pmatrix}\in\mathscr{M}_{2,\mathbb{R}}$ eine nilpotente Matrix vom Nilpotenzgrad 2.

(15.15) Lemma Sei V ein endlich-dimensionaler K-Vektorraum und $\psi \in \mathrm{End}_K(V)$ ein nilpotenter Endomorphismus vom Nilpotenzgrad p. Dann haben die Untervektorräume von $V_0, ..., V_p$ von V gegeben durch $V_k = \ker(\psi^k)$ für $0 \leq k \leq p$ die folgenden Eigenschaften.

(i) Es gilt $\{0_V\} = V_0 \subsetneq V_1 \subsetneq ... \subsetneq V_{p-1} \subsetneq V_p = V$.

(ii) Für $1 \leq k \leq p$ gilt $\psi^{-1}(V_{k-1}) = V_k$.

Beweis: zu (i) Wegen $\psi^0 = \mathrm{id}_V$ gilt $V_0 = \ker(\mathrm{id}_V) = \{0_V\}$, und aus $\psi^p = 0_{\mathrm{End}_K(V)}$ folgt $\psi^p(v) = 0_V$ für alle $v \in V$ und somit $V_p = V$. Sei nun $k \in \{1, ..., p\}$; zum Nachweis von $V_{k-1} \subseteq V_k$ sei $v \in V_{k-1}$ vorgegeben. Dann gilt $\psi^{k-1}(v) = 0_V$, und es folgt $\psi^k(v) = \psi(\psi^{k-1}(v)) = \psi(0_V) = 0_V$, also $v \in V_k$. Nehmen wir nun an, dass $V_{k-1} = V_k$ gilt. Wir zeigen, dass daraus $V_{p-1} = V_p$ folgen würde. Die Inklusion $V_{p-1} \subseteq V_p$ haben wir bereits gezeigt. Ist umgekehrt $v \in V_p$, dann gilt $\psi^k(\psi^{p-k}(v)) = \psi^p(v) = 0_V$, also $\psi^{p-k}(v) \in V_k = V_{k-1}$. Daraus wiederum folgt $\psi^{p-1}(v) = \psi^{k-1}(\psi^{p-k}(v)) = 0_V$, also $v \in V_{p-1}$. Aber aus $V_{p-1} = V_p = V$ folgt $\psi^{p-1} = 0_{\mathrm{End}_K(V)}$, was der Minimalität von p widerspricht. Also muss $V_{k-1} \subsetneq V_k$ für $1 \leq k \leq p$ gelten.

zu (ii) Für jeden Vektor $v \in V$ gilt die Äquivalenz

$$v \in \psi^{-1}(V_{k-1}) \qu\Leftrightarrow \quad \psi(v) \in V_{k-1} \quad \Leftrightarrow \quad \psi^k(v) = \psi^{k-1}(\psi(v)) = 0_V \quad \Leftrightarrow \quad v \in V_k. \qquad \square$$

(15.16) Satz Sei V ein endlich-dimensionaler K-Vektorraum und $\psi \in \mathrm{End}_K(V)$ ein nilpotenter Endomorphismus vom Nilpotenzgrad p. Sei $V_k = \ker(\psi^k)$ für $0 \leq k \leq p$. Dann gibt es in V Untervektorräume $U_1, ..., U_p$ und $W_1, ..., W_{p-1}$, so dass folgende Bedingungen erfüllt sind.

(i) Es gilt $\psi(U_k) \subseteq U_{k-1}$ für $2 \leq k \leq p$, und die Einschränkung $\psi|_{U_k}$ ist jeweils injektiv.

(ii) Es gilt $V_k = V_{k-1} \oplus U_k$ für $1 \leq k \leq p$ und $U_k = \psi(U_{k+1}) \oplus W_k$ für $1 \leq k \leq p-1$.

Beweis: Zunächst bestimmen wir einen Untervektorraum $U_p \leq V$, so dass $V = V_p = V_{p-1} \oplus U_p$ erfüllt ist. Dazu wählen wir eine Basis $\mathscr{B}$ von V_{p-1}, ergänzen diese durch eine geeignete Teilmenge $\mathscr{C} \subseteq V$ zu einer Basis von V zu setzen $U_p = \langle \mathscr{C} \rangle$. Sei nun $k \in \{2, ..., p\}$, und nehmen wir an, die Untervektorräume U_j für $k \leq j \leq p$ und W_j für $k \leq j \leq p-1$ mit den angegebenen Eigenschaften wurden bereits konstruiert. Ziel ist nun die Konstruktion von Untervektorräumen U_{k-1} und W_{k-1} mit $V_{k-1} = V_{k-2} \oplus U_{k-1}$ und $U_{k-1} = \psi(U_k) \oplus W_{k-1}$. Eine naheliegende Vorgehensweise besteht darin, eine Basis von $V_{k-2} \oplus \psi(U_k)$ zu einer Basis von V_{k-1} zu ergänzen. Wir müssen lediglich vorher sicherstellen, dass sich V_{k-2} und $\psi(U_k)$ tatsächlich nur in $\{0_V\}$ schneiden.

Sei dazu $v \in V_{k-2} \cap \psi(U_k)$ vorgegeben und $u \in U_k$ mit $\psi(u) = v$. Dann gilt $u \in \psi^{-1}(V_{k-2})$, was nach Lemma (15.15) (ii) mit V_{k-1} übereinstimmt. Wegen $k \geq 1$ liegt u also insbesondere in $V_1 = \ker(\psi)$. Daraus folgt $v = \psi(u) = 0_V$. Wir können nun unser Vorhaben umsetzen und eine Basis von $V_{k-2} \oplus \psi(U_k)$ durch Vektoren $v_1, ..., v_r$ (mit $r \in \mathbb{N}_0$) zu einer Basis von V_{k-1} ergänzen. Setzen wir nun $W_{k-1} = \langle v_1, ..., v_r \rangle_K$ und $U_{k-1} = \psi(U_k) \oplus W_{k-1}$, dann gilt offenbar $V_{k-1} = V_{k-2} \oplus U_{k-1}$.

Da die Aussagen aus Teil (ii) nach Konstruktion erfüllt sind, müssen nur noch die Aussagen aus Teil (i) überprüft werden. Wegen $U_k = \psi(U_{k+1}) \oplus W_k$ für $1 \leq k \leq p-1$ gilt offenbar $\psi(U_k) \subseteq U_{k-1}$ für $2 \leq k \leq p$. Es gilt jeweils $U_k \cap V_{k-1} = \{0_V\}$, wegen $k-1 \geq 1$ damit erst recht $U_k \cap \ker(\psi) = U_k \cap V_1 = \{0_V\}$. Daraus folgt, dass $\psi|_{U_k}$ injektiv ist. □

Um eine Verbindung zwischen diesem Satz und der Jordanschen Normalform herzustellen, benötigen wir zwei neue Begriffe.

(15.17) Definition Sei V ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$.

(i) Wir bezeichnen ein Tupel $(w_1, ..., w_p)$ von Vektoren mit $p \in \mathbb{N}$ als ***Jordankette*** bezüglich ϕ, wenn $\phi(w_k) = w_{k-1}$ für $2 \leq k \leq p$ und $\phi(w_1) = 0_V$ gilt.

(ii) Eine geordnete Basis $\mathscr{B}$ von V ist eine ***Jordanbasis*** bezüglich ϕ, wenn die Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}(\phi)$ in Jordanscher Normalform vorliegt.

Ist eine geordnete Basis $\mathscr{B} = (w_1, ..., w_p)$ von V zugleich eine Jordankette bezüglich ϕ, dann ist die Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}(\phi)$ eine Jordanmatrix zum Eigenwert 0. Denn aus der Gleichung $\phi(w_1) = 0_V$ folgt, dass die erste Spalte dieser Matrix der Nullvektor ist, und aus den Gleichungen $\phi(w_k) = w_{k-1}$ für $2 \leq k \leq p$ folgt, dass die zweite bis p-te Spalte durch die Einheitsvektoren $e_1, ..., e_{p-1}$ gegeben sind. Ist die geordnete Basis $\mathscr{B}$ aus mehreren Jordanketten zusammengesetzt, dann ist $\mathscr{M}_{\mathscr{B}}(\phi)$ entsprechend eine Matrix in Jordanscher Normalform (wiederum mit 0 als einzigem Eigenwert).

(15.18) Folgerung Seien die Bezeichnungen wie in Satz (15.16) gewählt, und sei außerdem $W_p = U_p$. Dann gilt

$$V = \bigoplus_{j=1}^{p} \bigoplus_{\ell=0}^{j-1} \psi^\ell(W_j).$$

Beweis: Für $1 \leq k \leq p$ gilt jeweils

$$\begin{aligned} U_k &= \psi(U_{k+1}) \oplus W_k = \psi(\psi(U_{k+2}) \oplus W_{k+1}) \oplus W_k = \psi^2(U_{k+2}) \oplus \psi(W_{k+1}) \oplus W_k = \\ &= \psi^2(\psi(U_{k+3}) \oplus W_{k+2}) \oplus \psi(W_{k+1}) \oplus W_k = \psi^3(U_{k+3}) \oplus \psi^2(W_{k+2}) \oplus \psi(W_{k+1}) \oplus W_k = \ldots \\ &= \psi^{p-k}(U_p) \oplus \ldots \oplus \psi(W_{k+1}) \oplus W_k = \psi^{p-k}(W_p) \oplus \ldots \oplus \psi(W_{k+1}) \oplus W_k = \bigoplus_{\ell=0}^{p-k} \psi^\ell(W_{k+\ell}). \end{aligned}$$

Setzen wir dies ein, so erhalten wir

$$\begin{aligned} V &= V_p = V_{p-1} \oplus U_p = V_{p-2} \oplus U_{p-1} \oplus U_p = \ldots = V_0 \oplus U_1 \oplus \ldots \oplus U_p \\ &= \{0_V\} \oplus U_1 \oplus \ldots \oplus U_p = \bigoplus_{k=1}^{p} U_k = \bigoplus_{k=1}^{p} \bigoplus_{\ell=0}^{p-k} \psi^\ell(W_{k+\ell}) = \bigoplus_{j=1}^{p} \bigoplus_{\ell=0}^{j-1} \psi^\ell(W_j) \quad , \end{aligned}$$

wobei im letzten Schritt die Gleichung $\{(\ell, k+\ell) \mid 1 \le k \le p, 0 \le \ell \le p-k\} = \{(\ell, j) \mid 1 \le j \le p, 0 \le \ell \le j-1\}$ verwendet wurde. □

(15.19) Folgerung Seien die Bezeichnungen wie in Satz (15.16) gewählt, und außerdem $W_p = U_p$. Dann existiert eine Jordanbasis $\mathscr{B}$ von V bezüglich ψ derart, dass die Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}(\psi)$ für $1 \le j \le p$ jeweils genau $\dim W_j$ Jordanblöcke der Größe j enthält, und darüber hinaus keine weiteren.

Beweis: Sei $j \in \{1, \ldots, p\}$, $m_j = \dim W_j$, und sei $(v_1, \ldots, v_{m_j})$ eine Basis von W_j. Für $0 \le \ell \le j-2$ ist nach Teil (i) von Satz (15.16) die Abbildung $\psi|_{U_{j-\ell}}$ injektiv, es gilt $\psi(U_{j-\ell}) \subseteq U_{j-\ell-1}$, und außerdem $W_j \subseteq U_j$. Daraus folgt, dass $(\psi^\ell(v_1), \ldots, \psi^\ell(v_{m_j}))$ für $0 \le \ell \le j-1$ jeweils eine Basis von $\psi^\ell(W_j)$ ist. Für $1 \le i \le m_j$ ist das Tupel

$$(\, \psi^{j-1}(v_i),\, \psi^{j-2}(v_i),\, \ldots,\, \psi(v_i),\, v_i\,)$$

eine Jordankette, denn jeder Vektor in dem Tupel mit Ausnahme des ersten wird auf seinen Vorgänger abgebildet; darüber hinaus liegt der Vektor $\psi^{j-1}(v_i)$ nach Konstruktion in U_1, und wegen $U_1 \subseteq V_1 = \ker(\psi)$ folgt daraus $\psi(\psi^{j-1}(v_i)) = 0_V$. Insgesamt erhalten wir auf diese Weise m_j Jordanketten der Länge j. Fassen wir all diese Jordanketten zusammen, so erhalten wir eine geordnete Basis der direkten Summe $\bigoplus_{\ell=0}^{j-1} \psi^\ell(W_j)$. Führen wir dies nun für $1 \le j \le p$ aus und fassen alle geordneten Basen abermals zusammen, so erhalten wir auf Grund der Folgerung (15.18) insgesamt eine geordnete Basis $\mathscr{B}$ von V. Die entsprechende Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}(\psi)$ enthält für $1 \le j \le p$ jeweils genau m_j Jordanblöcke der Größe j. □

Aus den bisherigen Ergebnissen können nun eine Formel für die Anzahl der Jordanblöcke einer bestimmen Größe ableiten.

(15.20) Satz Sei V ein endlich-dimensionaler K-Vektorraum, $\psi \in \mathrm{End}_K(V)$ ein nilpotenter Endomorphismus und $V_k = \ker(\psi^k)$, $d_k = \dim V_k$ für alle $k \ge 0$. Desweiteren sei $\mathscr{B}$ eine Jordanbasis wie in Folgerung (15.19) und $J = \mathscr{M}_{\mathscr{B}}(\psi)$. Für jedes $k \in \mathbb{N}$ sei a_k jeweils die Anzahl der Jordanblöcke der Größe k in J zum Eigenwert 0. Dann gilt

$$a_k = 2d_k - d_{k-1} - d_{k+1} \qquad \text{für alle } k \ge 1.$$

Beweis: Sei $p \in \mathbb{N}$ der Nilpotenzgrad von ψ. Wir überprüfen die Formel zunächst für $k \in \{1, \ldots, p-1\}$ und verwenden dazu die Bezeichnungen aus Satz (15.16). Nach Folgerung (15.19) gilt $a_k = \dim W_k$. Auf Grund der Injektivität von

$\psi|_{U_{k+1}}$ gilt außerdem $\dim \psi(U_{k+1}) = \dim U_{k+1}$. Die direkten Summenzerlegungen in Teil (ii) von Satz (15.16) liefern die Gleichungen $\dim U_k = \dim \psi(U_{k+1}) + \dim W_k = \dim U_{k+1} + \dim W_k$ und

$$d_k \quad = \quad \dim V_k \quad = \quad \dim V_{k-1} + \dim U_k \quad = \quad d_{k-1} + \dim U_k \quad ,$$

was zu $\dim U_k = d_k - d_{k-1}$ umgestellt werden kann. Ebenso gilt $\dim U_{k+1} = d_{k+1} - d_k$. Ingesamt erhalten wir auf diese Weise

$$a_k \quad = \quad \dim W_k \quad = \quad \dim U_k - \dim U_{k+1} \quad = \quad (d_k - d_{k-1}) - (d_{k+1} - d_k) \quad = \quad 2d_k - d_{k-1} - d_{k+1}.$$

Wegen $V_p = V_{p-1} \oplus U_p$ und $V_p = V_{p+1}$ gilt außerdem $d_p = d_{p+1}$ und $a_p = \dim U_p = d_p - d_{p-1} = 2d_p - d_{p-1} - d_{p+1}$. Für alle $k \geq p+1$ ist die Gleichung ebenfalls erfüllt, denn für diese k gilt $a_k = 0$ und wegen $d_k = d_{k-1} + d_{k+1}$ ebenso $2d_k - d_{k-1} - d_{k+1} = 0$. □

Wir zeige nun anhand zweier Beispiele, wie diese Formel angewendet werden kann, um für eine gegebene Matrix A eine zu A ähnliche Matrix in Jordanscher Normalform zu bestimmen. Zunächst betrachten wir eine Matrix mit einem einzigen Eigenwert, nämlich

$$A \quad = \quad \begin{pmatrix} 1 & 2 & 0 & 1 & 0 \\ -1 & 4 & -2 & 2 & 1 \\ 0 & -2 & 8 & -4 & -3 \\ 1 & -2 & 4 & -1 & -2 \\ -1 & -2 & 8 & -5 & -2 \end{pmatrix}.$$

Die Berechnung des charakteristischen Polynoms dieser Matrix ergibt

$$\chi_A \quad = \quad x^5 - 10x^4 + 40x^3 - 80x^2 + 80x - 32 \quad = \quad (x-2)^5 \quad ;$$

dies zeigt, dass 2 der einzige Eigenwert von A ist. Setzen wir

$$N \quad = \quad A - 2E \quad = \quad \begin{pmatrix} -1 & 2 & 0 & 1 & 0 \\ -1 & 2 & -2 & 2 & 1 \\ 0 & -2 & 6 & -4 & -3 \\ 1 & -2 & 4 & -3 & -2 \\ -1 & -2 & 8 & -5 & -4 \end{pmatrix} \quad ,$$

dann ist

$$N^2 \quad = \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 2 & -4 & 0 & -2 & 0 \end{pmatrix} \quad ,$$

und N^3 ist die Nullmatrix. Die Matrix N ist also nilpotent mit dem Nilpotenzgrad 3. Für alle $k \in \mathbb{N}_0$ sei $d_k = \dim \ker(N^k)$. Dann ist $d_0 = \dim \ker(E) = 0$ und $d_k = \dim \ker(N^k) = \dim \ker(0_{\mathcal{M}_{5,\mathbb{R}}}) = 5$ für alle $k \geq 3$. Mit Hilfe des Gauß-Algorithmus berechnen wir $\mathrm{rg}(N) = 3$, und an der Matrix N^2 kann $\mathrm{rg}(N^2) = 1$ unmittelbar abgelesen werden.

Mit dem Dimensionssatz folgt $d_1 = 5-3 = 2$ und $d_2 = 5-1 = 4$. Bezeichnet nun a_k für jedes $k \in \mathbb{N}$ die Anzahl der Jordanblöcke wie in Satz (15.20), dann erhalten wir

$$\begin{aligned} a_1 &= 2d_1 - d_0 - d_2 = 2\cdot 2 - 0 - 4 = 0 \\ a_2 &= 2d_2 - d_1 - d_3 = 2\cdot 4 - 2 - 5 = 1 \\ a_3 &= 2d_3 - d_2 - d_4 = 2\cdot 5 - 4 - 5 = 1 \\ a_k &= 2d_k - d_{k-1} - d_{k+1} = 2\cdot 5 - 5 - 5 = 0 \quad \text{für alle } k \geq 4. \end{aligned}$$

Die Matrix N ist somit ähnlich zur Jordanmatrix

$$J_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

und die Matrix $A = 2E + N$ ist ähnlich zur Jordanmatrix

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

Nun betrachten wir noch ein Beispiel, bei dem zwei verschiedene Eigenwerte vorkommen. Diesmal sei

$$A = \begin{pmatrix} -4 & -13 & 7 & 5 & 4 \\ 1 & 5 & -1 & 0 & -1 \\ -4 & -7 & 7 & 4 & 2 \\ 0 & -1 & 0 & 1 & 1 \\ 1 & 1 & -1 & -2 & 3 \end{pmatrix}.$$

Das charakteristische Polynom dieser Matrix ist gegeben durch

$$\chi_A = x^5 - 12x^4 + 57x^3 - 134x^2 + 156x - 72 = (x-2)^3(x-3)^2.$$

Also sind 2 und 3 die beiden Eigenwerte der Matrix. Wir setzen $N = A - 2E$ und $N' = A - 3E$ und berechnen $d_k = \dim\ker(N^k)$ sowie $d'_k = \dim\ker((N')^k)$ für $k \geq 1$. Die Rechnung ergibt $d_1 = 1$, $d_2 = 2$, $d_3 = 3$ sowie $d'_1 = 1$, $d'_2 = 2$. Eine weitere Rechnung ergibt, dass die Vektorräume $V = \ker(N^3)$ und $V' = \ker((N')^2)$ sich in $\{0_{\mathbb{R}^5}\}$ schneiden und wegen $\dim V + \dim V' = d_3 + d'_2 = 3 + 2 = 5$ somit $\mathbb{R}^5 = V \oplus V'$ gilt. Aus der Definition von V und V' folgt unmittelbar $\phi_N(V) \subseteq V$ und $\phi_{N'}(V') \subseteq V'$. Definieren wir $\psi = \phi_N|_V$ und $\psi' = \phi_{N'}|_{V'}$, dann ist $\psi \in \mathrm{End}_{\mathbb{R}}(V)$ nilpotent vom Nilpotenzgrad 3, und $\psi' \in \mathrm{End}_{\mathbb{R}}(V')$ ist nilpotent vom Nilpotenzgrad 2.

Wenden wir Satz (15.20) auf den Endomorphismus ψ an, so erhalten wir eine Jordanbasis $\mathscr{B}$ von V. Die Anzahl a_k der Jordanblöcke der Größe k in der Darstellungmatrix $\mathscr{M}_{\mathscr{B}}(\psi)$ ist gegeben durch

$$\begin{aligned} a_1 &= 2d_1 - d_0 - d_2 = 2\cdot 1 - 0 - 2 = 0 \\ a_2 &= 2d_2 - d_1 - d_3 = 2\cdot 2 - 1 - 3 = 0 \\ a_3 &= 2d_3 - d_2 - d_4 = 2\cdot 3 - 2 - 3 = 1 \\ a_k &= 2d_k - d_{k-1} - d_{k+1} = 2\cdot 3 - 3 - 3 = 0 \quad \text{für alle } k \geq 4. \end{aligned}$$

Die Darstellungsmatrix besteht also aus einer einzelnen Jordanmatrix und hat die Form

$$\mathscr{M}_{\mathscr{B}}(\psi) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Wegen $A = N + 2E$ gilt $\phi_A|_V = \phi_N|_V + 2\cdot \mathrm{id}_V = \psi + 2\cdot \mathrm{id}_V$ und somit

$$\mathscr{M}_{\mathscr{B}}(\phi_A|_V) = \mathscr{M}_{\mathscr{B}}(\psi) + \mathscr{M}_{\mathscr{B}}(2\cdot \mathrm{id}_V) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Wenden wir Satz (15.20) auf den Endomorphismus ψ' an, so erhalten wir eine Jordanbasis $\mathscr{B}'$ von V'. Die Anzahl a'_k der Jordanblöcke der Größe k in der Darstellungmatrix $\mathscr{M}_{\mathscr{B}}(\psi')$ ist gegeben durch

$$\begin{aligned} a'_1 &= 2d'_1 - d'_0 - d'_2 = 2\cdot 1 - 0 - 2 = 0 \\ a'_2 &= 2d'_2 - d'_1 - d'_3 = 2\cdot 2 - 1 - 2 = 1 \\ a'_k &= 2d'_k - d'_{k-1} - d'_{k+1} = 2\cdot 2 - 2 - 2 = 0 \quad \text{für alle } k \geq 3. \end{aligned}$$

Auch diesmal erhalten wir als Darstellungsmatrix eine Jordanmatrix, nämlich

$$\mathscr{M}_{\mathscr{B}'}(\psi') = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Wegen $A = N' + 3E$ gilt $\phi_A|_{V'} = \phi_{N'}|_{V'} + 3\cdot \mathrm{id}_{V'} = \psi' + 3\cdot \mathrm{id}_{V'}$ und somit

$$\mathscr{M}_{\mathscr{B}'}(\phi_A|_{V'}) = \mathscr{M}_{\mathscr{B}'}(\psi') + \mathscr{M}_{\mathscr{B}'}(3\cdot \mathrm{id}_{V'}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}.$$

Wegen $\mathbb{R}^5 = V \oplus V'$ können wir $\mathscr{B}$ und $\mathscr{B}'$ zu einer Basis $\mathscr{B}''$ von $\mathbb{R}^5$ zusammenfügen. Wir erhalten dann für ϕ_A die Darstellungsmatrix

$$J = \mathscr{M}_{\mathscr{B}''}(\phi_A) = \begin{pmatrix} \mathscr{M}_{\mathscr{B}}(\phi_A|_V) & 0 \\ 0 & \mathscr{M}_{\mathscr{B}'}(\phi_A|_{V'}) \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

Setzen wir $T = \mathcal{T}_{\mathcal{E}}^{\mathcal{B}''}$, dann gilt auf Grund der Transformationsformel $J = \mathcal{M}_{\mathcal{B}''}(\phi_A) = T^{-1} \cdot \mathcal{M}_{\mathcal{E}}(\phi_A) \cdot T = T^{-1}AT$. Dies zeigt, dass A zu der Matrix J in Jordanscher Normalform ähnlich ist.

Als nächstes befassen wir uns mit der Frage, wie man zu einem gegebenen nilpotenten Endomorphismus ψ auf einem endlich-dimensionalen K-Vektorraum V eine geordnete Basis $\mathcal{B}$ bestimmt, so dass $\mathcal{M}_{\mathcal{B}}(\psi)$ in Jordanscher Normalform vorliegt. Sei p der Nilpotenzgrad von ψ. Dann führt man die folgenden Schritte aus.

- Sei $V_k = \ker(\psi^k)$ für $0 \leq k \leq p$. Bestimme eine Basis $\mathcal{C}_k$ von V_k für $1 \leq k \leq p$, und setze $\mathcal{C}_0 = \emptyset$.
- Nun orientieren wir uns an den Gleichungen $V_p = V_{p-1} \oplus U_p$ und $W_p = U_p$. Sei $\mathcal{B}_p \subseteq \mathcal{C}_p$ so gewählt, dass $\mathcal{C}_{p-1} \cup \mathcal{B}_p$ eine Basis von V_p ist. Setze $\mathcal{D}_p = \mathcal{B}_p$.
- Für $k = p-1, p-2, ..., 1$ betrachten wir die Gleichungen $V_k = V_{k-1} \oplus \psi(U_{k+1}) \oplus W_k$ und $U_k = \psi(U_{k+1}) \oplus W_k$. Wähle eine Teilmenge $\mathcal{D}_k \subseteq \mathcal{C}_k$ so, dass $\mathcal{C}_{k-1} \cup \psi(\mathcal{B}_{k+1}) \cup \mathcal{D}_k$ eine Basis von V_k ist. Setze $\mathcal{B}_k = \psi(\mathcal{B}_{k+1}) \cup \mathcal{D}_k$.
- Für $1 \leq k \leq p$ sei $m_k = |\mathcal{D}_k|$, und es seien $w_1^{(k)}, w_2^{(k)}, ..., w_{m_k}^{(k)}$ die Elemente von $\mathcal{D}_k$. Definiere das Tupel $\hat{\mathcal{B}}_k$ bestehend aus den Elementen

$$\begin{pmatrix} \psi^{k-1}(w_1^{(k)}), \psi^{k-2}(w_1^{(k)}), ..., \psi(w_1^{(k)}), w_1^{(k)}, \\ \psi^{k-1}(w_2^{(k)}), \psi^{k-2}(w_2^{(k)}), ..., \psi(w_2^{(k)}), w_2^{(k)}, \\ ... \\ \psi^{k-1}(w_{m_k}^{(k)}), \psi^{k-2}(w_{m_k}^{(k)}), ..., \psi(m_k{}^{(k)}), w_{m_k}^{(k)} \end{pmatrix}.$$

  Dann ist $\mathcal{B} = \hat{\mathcal{B}}_1 \cup \hat{\mathcal{B}}_2 \cup ... \cup \hat{\mathcal{B}}_p$ eine geordnete Basis mit der gewünschten Eigenschaft. Die Matrix $\mathcal{M}_{\mathcal{B}}(\psi)$ enthält die Jordanblöcke der Größe nach aufsteigend geordnet.

Mit Hilfe des soeben formulierten Algorithmus kann nun auch das folgende, mit der vorherigen Aufgabenstellung eng verwandte Problem, gelöst werden: Gegeben sei eine nilpotente Matrix $N \in \mathcal{M}_{n,K}$. Gesucht ist eine Matrix $T \in \mathrm{GL}_n(K)$ mit der Eigenschaft, dass $T^{-1}NT$ in Jordanscher Normalform vorliegt. Dazu wendet man den oben angebenen Algorithmus auf den Endomorphismus $\phi_N \in \mathrm{End}_K(K^n)$ an und erhält eine geordnete Basis $\mathcal{B}$ des K^n mit der Eigenschaft, dass $J = \mathcal{M}_{\mathcal{B}}(\phi_N)$ eine Matrix in Jordanscher Normalform ist. Trägt man die Elemente von $\mathcal{B}$ als Spalten in eine Matrix T ein, dann ist $T = \mathcal{T}_{\mathcal{E}}^{\mathcal{B}}$, und auf Grund der Transformationsformel, Satz (11.16), gilt

$$T^{-1}NT \quad = \quad \mathcal{T}_{\mathcal{B}}^{\mathcal{E}} \mathcal{M}_{\mathcal{E}}(\phi_N) \mathcal{T}_{\mathcal{E}}^{\mathcal{B}} \quad = \quad \mathcal{M}_{\mathcal{B}}(\phi_N) \quad = \quad J.$$

Also ist $T^{-1}NT$ eine Matrix in Jordanscher Normalform.

Wir demonstrieren die Funktionsweise des Verfahrens nochmals mit Hilfe der Matrix

$$N \quad = \quad A - 2E \quad = \quad \begin{pmatrix} -1 & 2 & 0 & 1 & 0 \\ -1 & 2 & -2 & 2 & 1 \\ 0 & -2 & 6 & -4 & -3 \\ 1 & -2 & 4 & -3 & -2 \\ -1 & -2 & 8 & -5 & -4 \end{pmatrix}$$

von oben. Wie oben bereits festgestellt wurde, ist $p = 3$ der Nilpotenzgrad von N. Mit dem Gauß-Algorithmus bestimmt man für $V_1 = \ker(N^1)$ und $V^2 = \ker(N^2)$ die Basen

$$\mathscr{C}_1 = \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \\ -2 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 2 \end{pmatrix} \right\} \qquad \text{und} \qquad \mathscr{C}_2 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Außerdem ist $\mathscr{C}_0 = \varnothing$ eine Basis von $V_0 = \ker(N^0) = \ker(E) = \{0_{\mathbb{R}^5}\}$, und $\mathscr{C}_3 = \{e_1, e_2, e_3, e_4, e_5\}$ ist eine Basis von $V_3 = \ker(N^3) = \ker(0_{\mathscr{M}_{5,\mathbb{R}}}) = \mathbb{R}^5$.

Dem Algorithmus folgend ergänzen wir nun $\mathscr{C}_2$ durch das Element $w_1^{(3)} = e_1$ aus $\mathscr{C}_3$ zu einer Basis von V_3, wir setzen also $\mathscr{B}_3 = \mathscr{D}_3 = \{e_1\}$. Dass $\mathscr{C}_2 \cup \mathscr{B}_3$ tatsächlich eine Basis von V_3 ist, stellen wir dadurch sicher, dass wir mit dem Gauß-Algorithmus die lineare Unabhängigkeit der 5-elementigen Mengen $\mathscr{C}_2 \cup \mathscr{B}_3$ überprüfen: Die Elemente werden als Zeilen in eine 5×5-Matrix eingetragen, und der Gauß-Algorithmus zeigt an, dass sich um eine Matrix vom Rang 5 handelt.

Im nächsten Schritt (für $k = 2$) ergänzen wir die dreielementige Menge $\mathscr{C}_1 \cup \psi(\mathscr{B}_3)$ bestehend aus $(0,1,0,-2,2)$, $(0,0,1,0,2)$ und $\phi_N(e_1) = (-1,-1,0,1,-1)$ durch $w_1^{(2)} = (1,0,0,1,0)$ zu einer Basis von V_2, wir setzen also $\mathscr{D}_2 = \{w_1^{(2)}\}$. Dass tatsächlich eine Basis vorliegt, wird wiederum mit dem Gauß-Algorithmus überprüft. Wie im Algorithmus setzen wir außerdem $\mathscr{B}_2 = \psi(\mathscr{B}_3) \cup \mathscr{D}_2$.

Im letzten Schritt (für $k = 1$) bemerken wir, dass $\mathscr{C}_0 \cup \psi(\mathscr{B}_2)$ bereits $d_1 = 2$ Elementen besteht, also bereits eine Basis von V_1 liefert. Es kann also $\mathscr{D}_1 = \varnothing$ und $\mathscr{B}_1 = \psi(\mathscr{B}_2)$ gesetzt werden.

Der Algorithmus hat für $m_k = |\mathscr{D}_k|$ die Werte $m_1 = 0$ und $m_2 = m_3 = 1$ ergeben. Das Tupel $\hat{\mathscr{B}}_1$ ist damit leer, außerdem ist $\hat{\mathscr{B}}_2 = (Nw_1^{(2)}, w_1^{(2)})$ und $\hat{\mathscr{B}}_3 = (N^2w_1^{(3)}, Nw_1^{(3)}, w_1^{(3)})$. Setzen wir $\mathscr{B} = \hat{\mathscr{B}}_1 \cup \hat{\mathscr{B}}_2 \cup \hat{\mathscr{B}}_3$, dann erhalten wir für $T = \mathscr{T}_{\mathscr{E}}^{\mathscr{B}}$ die Matrix

$$T = \begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ -4 & 0 & 1 & 0 & 0 \\ -2 & 1 & 0 & 1 & 0 \\ -6 & 0 & 2 & -1 & 0 \end{pmatrix} \quad \text{mit der Inversen} \quad T^{-1} = \begin{pmatrix} 0 & -1 & -2 & 0 & 1 \\ 0 & 0 & -2 & 1 & 1 \\ 0 & -4 & -7 & 0 & 4 \\ 0 & -2 & -2 & 0 & 1 \\ 1 & -2 & 0 & -1 & 0 \end{pmatrix}.$$

Es ist

$$T^{-1}NT = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

und wegen $A = N + 2E$ ist $T^{-1}AT = T^{-1}NT + 2E$ die bereits oben ermittelte Matrix in Jordanscher Normalform, mit zwei Jordanblöcken zum Eigenwert 2.

Oben hatten wir bereits die Matrix

$$A = \begin{pmatrix} -4 & -13 & 7 & 5 & 4 \\ 1 & 5 & -1 & 0 & -1 \\ -4 & -7 & 7 & 4 & 2 \\ 0 & -1 & 0 & 1 & 1 \\ 1 & 1 & -1 & -2 & 3 \end{pmatrix}$$

mit den beiden Eigenwerten 2 und 3 betrachtet. Wir schauen uns nun an, wie man auch hier eine Transformationsmatrix findet, die A in Jordansche Normalform überführt. Hier besteht der Ansatz darin, das soeben behandelte Verfahren auf die nilpotenten Endomorphismen $\psi = \phi_N|_V$ und $\psi' = \phi_{N'}|_{V'}$ anwendet, wobei wie oben $N = A-2E$, $N' = A-3E$, $V = \ker(N^3)$ und $V' = \ker((N')^2)$ ist. Wie wir unten feststellen werden, ist V der Hauptraum $\mathrm{Hau}(A,2)$ zum Eigenwert 2, V' der Hauptraum $\mathrm{Hau}(A,3)$ zum Eigenwert 3. Für jede Matrix $A \in \mathscr{M}_{n,K}$ mit zerfallendem charakteristischem Polynom $\chi_A \in K[x]$ existiert eine Zerlegung des K-Vektorraums K^n in eine direkte Summe von Haupträumen, analog zur bereits oben gefundenen Zerlegung $\mathbb{R}^5 = \mathrm{Hau}(A,2) \oplus \mathrm{Hau}(A,3)$.

Der nilpotente Endomorphismus ψ hat den Nilpotenzgrad $p = 3$. Der Gauß-Algorithmus liefert für die Vektorräume $V_k = \ker(\psi^k)$ mit $0 \le k \le 3$ die Basen $\mathscr{C}_k$ gegeben durch

$$\mathscr{C}_0 = \varnothing\ ,\ \mathscr{C}_1 = \left\{ \begin{pmatrix} 5 \\ -1 \\ 3 \\ 0 \\ -1 \end{pmatrix} \right\}\ ,\ \mathscr{C}_2 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ -1 \\ 0 \\ 2 \end{pmatrix} \right\}\ ,\ \mathscr{C}_3 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \\ -1 \end{pmatrix} \right\}.$$

Sei $d_k = |\mathscr{C}_k| = \dim V_k$ für $0 \le k \le 3$. Entsprechend dem Algorithmus ergänzen wir $\mathscr{C}_2$ durch das Element $w_1^{(3)} = (2,0,0,1,1)$ aus $\mathscr{C}_3$ zu einer Basis von V_3; wir setzen also $\mathscr{B}_3 = \mathscr{D}_3 = \{w_1^{(3)}\}$. Die Menge $\mathscr{C}_1 \cup \psi(\mathscr{D}_3)$ besteht bereits aus $d_2 = 2$ Elementen. Wir können deshalb $\mathscr{D}_2 = \varnothing$ und $\mathscr{B}_2 = \psi(\mathscr{D}_3)$ setzen. Ebenso enthält $\mathscr{C}_0 \cup \psi(\mathscr{B}_2)$ bereits $d_1 = 1$ Element; deshalb setzen wir $\mathscr{D}_1 = \varnothing$ und $\mathscr{B}_1 = \psi(\mathscr{B}_2)$. Mit der Notation von oben ist nun $\hat{\mathscr{B}}_1 = \hat{\mathscr{B}}_2 = ()$ und $\hat{\mathscr{B}}_3 = (\psi^2(w_1^{(3)}), \psi(w_1^{(3)}), w_1^{(3)})$, und insgesamt

$$\mathscr{B} = \hat{\mathscr{B}}_1 \cup \hat{\mathscr{B}}_2 \cup \hat{\mathscr{B}}_3 = (\psi^2(w_1^{(3)}), \psi(w_1^{(3)}), w_1^{(3)}) = (N^2 w_1^{(3)}, N w_1^{(3)}, w_1^{(3)}) = \left(\begin{pmatrix} -5 \\ 1 \\ -3 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -3 \\ 1 \\ -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right).$$

Der nilpotente Endomorphismus ψ' hat den Nilpotenzgrad $p' = 2$. Der Gauß-Algorithmus liefert für die Vektorräume $V_k' = \ker((\psi')^k)$ mit $0 \le k \le 2$ die Basen $\mathscr{C}_k'$ gegeben durch

$$\mathscr{C}_0 = \varnothing\ ,\ \mathscr{C}_1 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\}\ ,\ \mathscr{C}_2 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \\ -1 \\ -1 \end{pmatrix} \right\}.$$

Sei $d'_k = |\mathscr{C}'_k| = \dim V'_k$ für $0 \le k \le 2$. Auch hier gehen wir wie im Algorithmus vor und ergänzen zunächst $\mathscr{C}'_1$ durch das Element $w_1^{(2)} = (0,1,3,-1,-1)$ zu einer Basis von V'_2. Wir setzen also $\mathscr{B}'_2 = \mathscr{D}'_2 = \{w_1^{(2)}\}$. Die Menge $\mathscr{C}'_0 \cup \psi'(\mathscr{D}'_2)$ enthält bereits $d'_1 = 1$ Element. Wir setzen deshalb $\mathscr{D}'_1 = \varnothing$ und $\mathscr{B}'_1 = \psi(\mathscr{D}'_2)$. Mit der Notation von oben ist nun $\hat{\mathscr{B}}'_1 = ()$ und $\hat{\mathscr{B}}'_2 = (\psi'(w_1^{(2)}), w_1^{(2)})$. Wir erhalten wir V' die geordnete Basis

$$\mathscr{B}' \quad = \quad (\psi'(w_1^{(2)}), w_1^{(2)}) \quad = \quad (N' w_1^{(2)}, w_1^{(2)}) \quad = \quad \left(\begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \\ -1 \\ -1 \end{pmatrix} \right).$$

Tragen wir nun $\mathscr{B} \cup \mathscr{B}'$ als Spalten in einer Matrix ein, so erhalten wir

$$T = \begin{pmatrix} -5 & -3 & 2 & -1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ -3 & -2 & 0 & -1 & 3 \\ 0 & 0 & 1 & 0 & -1 \\ 1 & 1 & 1 & 0 & -1 \end{pmatrix} \quad \text{mit der Inversen} \quad T' = \begin{pmatrix} -1 & -1 & 1 & 2 & 0 \\ 1 & 1 & -1 & -3 & 1 \\ 0 & 1 & 0 & 2 & -1 \\ 1 & 4 & -2 & 3 & -5 \\ 0 & 1 & 0 & 1 & -1 \end{pmatrix}.$$

Man kann sich nun davon überzeugen, dass $T^{-1}AT$ mit der oben angegebenen Jordanschen Normalform, mit den beiden Jordanblöcken zu den Eigenwerten 2 und 3, übereinstimmt.

Um nachzuweisen, dass dieses Verfahren für jeden Endomorphismus $\phi \in \mathrm{End}_K(V)$ eines endlich-dimensionalen K-Vektorraums mit zerfallendem charakterisischen Polynom $\chi_\phi \in K[x]$ (oder jeder Matrix $A \in \mathscr{M}_{n,K}$ mit zerfallendem charakterisischen Polynom $\chi_A \in K[x]$) funktioniert, muss nun noch gezeigt werden, dass der Vektorraum V (bzw. K^n) eine direkte Summenzerlegung in Analogie zu der Zerlegung $\mathbb{R}^5 = V \oplus V'$ von oben besitzt.

Zwei Polynome $f, g \in K[x]$ werden ***teilerfremd*** genannt, wenn es kein Polynom $h \in K[x]$ vom Grad ≥ 1 gibt, dass sowohl f als auch g teilt.

(15.21) Satz *(Zerlegungssatz)*

Sei V ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$. Seien $f, g \in K[x]$ teilerfremde Polynome mit $\mu_\phi = f\,g$. Dann gilt $\ker f(\phi) = \mathrm{im}\, g(\phi)$, $\mathrm{im}\, f(\phi) = \ker g(\phi)$ und

$$V \quad = \quad \mathrm{im}\, f(\phi) \oplus \mathrm{im}\, g(\phi) \quad = \quad \ker f(\phi) \oplus \ker g(\phi).$$

Beweis: Wir unterteilen den Beweis der Übersichtlichkeit halber in eine Reihe von Einzelschritten und zeigen nacheinander die Aussagen

(i) $\ker f(\phi) \cap \ker g(\phi) = \{0_V\}$
(ii) $\mathrm{im}\, f(\phi) \subseteq \ker g(\phi)$ und $\mathrm{im}\, g(\phi) \subseteq \ker f(\phi)$

(iii) $V = \ker f(\phi) \oplus \operatorname{im} f(\phi) = \ker g(\phi) \oplus \operatorname{im} g(\phi)$
(iv) $\ker f(\phi) = \operatorname{im} g(\phi)$ und $\ker g(\phi) = \operatorname{im} f(\phi)$
(v) $V = \operatorname{im} f(\phi) \oplus \operatorname{im} g(\phi)$

zu (i) Angenommen, es gibt einen Vektor $v \neq 0_V$ in $\ker f(\phi) \cap \ker g(\phi)$. Dann gilt $f(\phi)(v) = g(\phi)(v) = 0_V$, und damit ist $\mu_{\phi,v}$ nach Proposition (15.6) ein gemeinsamer Teiler von f und g. Aber dies widerspricht der Teilerfremdheit von f und g.

zu (ii) Sei $w \in \operatorname{im} f(\phi)$. Dann gibt es ein $v \in V$ mit $f(\phi)(v) = w$. Es folgt

$$g(\phi)(w) \quad = \quad g(\phi)(f(\phi)(v)) \quad = \quad (g(\phi) \circ f(\phi))(v) \quad = \quad (gf)(\phi)(v) \quad =$$

$$\mu_\phi(\phi)(v) \quad = \quad 0_{\mathrm{End}_K(V)}(v) \quad = \quad 0_V \quad ,$$

und damit liegt w im Kern von $g(\phi)$. Die Inklusion $\operatorname{im} g(\phi) \subseteq \ker f(\phi)$ beweist man nach genau demselben Schema, lediglich die Rollen von f und g sind hier vertauscht.

zu (iii) Aus $\ker f(\phi) \cap \ker g(\phi) = \{0_V\}$ und $\operatorname{im} f(\phi) \subseteq \ker g(\phi)$ folgt $\ker f(\phi) \cap \operatorname{im} f(\phi) = \{0_V\}$. Die direkte Summe $\ker f(\phi) \oplus \operatorname{im} f(\phi)$ ist jedenfalls ein Untervektorraum von V. Nach dem Schnittdimensionssatz (10.5) und dem Dimensionssatz für lineare Abbildungen (10.8) gilt außerdem

$$\dim \ker f(\phi) \oplus \operatorname{im} f(\phi) \quad = \quad \dim \ker f(\phi) + \dim \operatorname{im} f(\phi) \quad = \quad \dim V.$$

Aus $\ker f(\phi) \oplus \operatorname{im} f(\phi) \subseteq V$ und der Gleichheit der Dimension folgt $\ker f(\phi) \oplus \operatorname{im} f(\phi) = V$. Der Beweis der Gleichung $\ker g(\phi) \oplus \operatorname{im} g(\phi) = V$ läuft wiederum genauso ab.

zu (iv) Nach (ii) gilt jedenfalls $\operatorname{im} f(\phi) \subseteq \ker g(\phi)$, und daraus folgt $\dim \operatorname{im} f(\phi) \leq \dim \ker g(\phi)$. Wegen (i) bilden die Untervektorräume $\ker f(\phi)$ und $\ker g(\phi)$ eine direkte Summe, damit ist $\dim \ker f(\phi) + ker\ g(\phi) \leq \dim V$. Insgesamt erhalten wir die Ungleichungskette

$$\dim V \quad = \quad \dim \operatorname{im} f(\phi) + \dim \ker f(\phi) \quad \leq \quad \dim \ker g(\phi) + \dim \ker f(\phi) \quad \leq \quad \dim V.$$

Weil Anfang und Ende der Kette übereinstimmen, muss $\dim \operatorname{im} f(\phi) = \dim \ker g(\phi)$ gelten, und zusammen mit $\operatorname{im} f(\phi) \subseteq \ker g(\phi)$ folgt daraus die Gleichheit $\operatorname{im} f(\phi) = \ker g(\phi)$. Der Beweis der anderen Gleichung läuft genauso.

zu (v) Dies folgt unmittelbar aus (iii) und (iv). □

(15.22) Definition Sei V ein endlich-dimensionaler K-Vektorraum, $\phi \in \mathrm{End}_K(V)$ und $\lambda \in K$. Dann wird

$$\mathrm{Hau}(\phi, \lambda) \quad = \quad \bigcup_{r=0}^{\infty} \ker((\phi - \lambda \mathrm{id}_V)^r)$$

der ***Hauptraum*** zum Wert λ genannt.

Wie in Lemma (15.15) überprüft man leicht, dass für alle $r,s \in \mathbb{N}_0$ mit $r \leq s$ jeweils die Teilmengenbeziehung $\ker((\phi - \lambda \mathrm{id}_V)^r) \subseteq \ker((\phi - \lambda \mathrm{id}_V)^s)$ gilt. Mit Hilfe dieser Feststellung ist wiederum leicht zu sehen, dass $\mathrm{Hau}(\phi, \lambda)$ ein Untervektorraum von V ist. Zunächst ist 0_V im Hauptraum enthalten, wegen $\{0_V\} = \ker(\mathrm{id}_V) = \ker((\phi - \lambda \mathrm{id}_V)^0) \subseteq \mathrm{Hau}(\phi, \lambda)$. Sind nun $v, w \in \mathrm{Hau}(\phi, \lambda)$ und $\alpha \in K$ vorgegeben, dann gibt es $r,s \in \mathbb{N}_0$ mit $v \in \ker((\phi - \lambda \mathrm{id}_V)^r)$ und $w \in \ker((\phi - \lambda \mathrm{id}_V)^s)$. Nach eventueller Vertauschung von v und w können wir $r \leq s$ annehmen, und auf Grund der soeben festgestellten Inklusion sind dann $v, w \in \ker((\phi - \lambda \mathrm{id}_V)^s)$. Weil dies ein Untervektorraum von V ist, folgt $v + w \in \ker((\phi - \lambda \mathrm{id}_V)^s)$ und $\alpha v \in \ker((\phi - \lambda \mathrm{id}_V)^s)$, und damit erst recht $v + w, \alpha v \in \mathrm{Hau}(\phi, \lambda)$.

(15.23) Proposition Seien die Bezeichnungen wie in Definiton (15.22) gewählt, und sei r die Vielfachheit von λ als Nullstelle von μ_ϕ. Dann gilt $\mathrm{Hau}(\phi, \lambda) = \ker((\phi - \lambda \mathrm{id}_V)^r)$.

Beweis: Die Inklusion „$\supseteq$“ ist nach Definition des Hauptraums offensichtlich. Zum Beweis von „$\subseteq$“ sei $v \in \mathrm{Hau}(\phi, \lambda)$ vorgegeben. Dann gibt es ein $s \in \mathbb{N}_0$ mit $v \in \ker((\phi - \lambda \mathrm{id}_V)^s)$, es gilt also $f(\phi)(v) = 0_V$ für das Polynom $f = (x - \lambda)^s$. Daraus folgt, dass $\mu_{\phi,v}$ ein Teiler von f ist. Es gibt also ein $r_1 \leq s$ mit $\mu_{\phi,v} = (x - \lambda)^{r_1}$. Andererseits ist das Polynom $\mu_{\phi,v}$ wegen $\mu_\phi(\phi)(v) = 0_{\mathrm{End}_K(V)}(v) = 0_V$ nach Proposition (15.6) auch ein Teiler von μ_ϕ. Auf Grund dieser Teilerbeziehung gilt $r_1 \leq r$. Nach Definition des Polynoms $\mu_{\phi,v}$ gilt darüber hinaus $(\phi - \lambda \mathrm{id}_V)^{r_1}(v) = \mu_{\phi,v}(v) = 0_V$, damit erst recht $(\phi - \lambda \mathrm{id}_V)^r(v) = 0_V$ und folglich $v \in \ker((\phi - \lambda \mathrm{id}_V)^r)$. □

(15.24) Lemma Sei V ein endlich-dimensionaler K-Vektorraum, $\phi \in \mathrm{End}_K(V)$, $f \in K[x]$ und $U = \ker f(\phi)$. Dann gilt $\phi(U) \subseteq U$.

Beweis: Setzen wir $g = xf$, dann gilt $g(\phi) = \phi \circ f(\phi) = f(\phi) \circ \phi$. Sei nun $v \in U$ vorgegeben. Dann gilt $f(\phi)(v) = 0_V$. Es folgt $f(\phi)(\phi(v)) = (f(\phi) \circ \phi)(v) = (\phi \circ f(\phi))(v) = \phi(0_V) = 0_V$ und somit auch $\phi(v) \in U$. □

(15.25) Satz Sei V ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$ ein Endomorphismus mit der Eigenschaft, dass das charakteristische Polynom $\chi_\phi \in K[x]$ oder das Minimalpolynom μ_ϕ in Linearfaktoren zerfällt. Dann gilt

$$V \quad = \quad \mathrm{Hau}(\phi, \lambda_1) \oplus \ldots \oplus \mathrm{Hau}(\phi, \lambda_r) \quad ,$$

wobei $\lambda_1, \ldots, \lambda_r$ die verschiedenen Eigenwerte von ϕ bezeichnen.

Beweis: Wir führen den Beweis durch vollständige Induktion über die Dimension von V. Im Fall $V = \{0_V\}$ ist nichts zu zeigen. Sei nun $\dim V \geq 1$, und setzen wir die Aussage für alle Vektorräume kleinerer Dimension voraus. Mit χ_ϕ zerfällt als Teiler auch das Polynom μ_ϕ in Linearfaktoren, es gilt also

$$\mu_\phi \quad = \quad \prod_{k=1}^{r} (x - \lambda_k)^{e_k} \quad ,$$

wobei $\lambda_1, \ldots, \lambda_r \in K$ die verschiedenen Eigenwerte von ϕ sind. Wir betrachten nun die Zerlegung $\mu_\phi = fg$ mit $f = (x - \lambda_1)^{e_1}$ und $g = \prod_{k=2}^{r} (x - \lambda_k)^{e_k}$. Die Faktoren f und g sind offenbar teilerfremd. Wir können also Satz

(15.21) anwenden und erhalten eine direkte Summenzerlegung $V = U \oplus W$ mit $U = \ker f(\phi) = \mathrm{Hau}(\phi, \lambda_1)$ und $W = \ker g(\phi)$. Nach Lemma (15.24) gilt $\phi(U) \subseteq U$ und $\phi(W) \subseteq W$.

Unser Ziel besteht nun darin, die Induktionsvoraussetzung auf den Endomorphismus $\psi = \phi|_W$ in $\mathrm{End}_K(W)$ anzuwenden. Wegen

$$\mu_\phi(\psi) \quad = \quad \mu_\phi(\phi)|_W \quad = \quad 0_{\mathrm{End}_K(V)}|_W \quad = \quad 0_{\mathrm{End}_K(W)}$$

ist μ_ψ nach Satz (15.4) ein Teiler von μ_ϕ. Also zerfällt auch das Polynom μ_ψ in Linearfaktoren. Wegen $\mathrm{Eig}(\phi, \lambda_1) \neq \{0_V\}$ und $\mathrm{Hau}(\phi, \lambda_1) \supseteq \mathrm{Eig}(\phi, \lambda_1)$ ist auch $U \neq \{0_V\}$ und somit $\dim W < \dim V$. Wenden wir die Induktionsvoraussetzung auf $\psi = \phi|_W \in \mathrm{End}_K(W)$ an, so erhalten wir eine Zerlegung

$$W \quad = \quad \bigoplus_{k=2}^{r} \mathrm{Hau}(\psi, \lambda_k).$$

Wir zeigen, dass die Haupträume von ψ mit entsprechenden Haupträumen von ϕ übereinstimmen. Sei dazu $k \in \{2, ..., r\}$ vorgegeben. Aus $(\psi - \lambda_k \mathrm{id}_W)^{e_k} = (\phi - \lambda_k \mathrm{id}_V)^{e_k}|_W$ folgt mit Proposition (15.23)

$$\mathrm{Hau}(\psi, \lambda_k) \quad = \quad \ker((\psi - \lambda_k \mathrm{id}_W)^{e_k}) \quad = \quad \ker((\phi - \lambda_k \mathrm{id}_V)^{e_k}) \cap W \quad = \quad \mathrm{Hau}(\phi, \lambda_k) \cap W.$$

Weil $f_k = (x - \lambda_k)^{e_k}$ ein Teiler von g ist, ist $\mathrm{Hau}(\phi, \lambda_k) = \ker f_k(\phi)$ darüber hinaus in $W = \ker g(\phi)$ enthalten. Wir erhalten $\mathrm{Hau}(\psi, \lambda_k) = \mathrm{Hau}(\phi, \lambda_k)$ für $2 \leq k \leq r$ und damit insgesamt die gewünschte Zerlegung. □

Wir fassen das wichtigste Ergebnis über die Jordansche Normalform von Matrizen nochmals in einem Satz zusammen.

(15.26) Folgerung *(Existenz und Eindeutigkeit der Jordanschen Normalform)*

Sei $n \in \mathbb{N}$ und K ein Körper.

(i) Sei $A \in \mathcal{M}_{n,K}$ eine Matrix, deren charakteristisches Polynom χ_A in $K[x]$ in Linearfaktoren zerfällt. Dann ist A ähnlich zu einer Matrix in Jordanscher Normalform.

(ii) Zwei Matrizen $J, J' \in \mathcal{M}_{n,K}$ in Jordanscher Normalform sind genau dann ähnlich zueinander, wenn sie bis auf Reihenfolge dieselben Jordanblöcke enthalten.

Beweis: zu (i) Sei $V = K^n$ und $\phi = \phi_A$. Dann stimmt das charakteristische Polynom χ_A mit χ_ϕ überein. Da χ_ϕ in Linearfaktoren zerfällt, können wir Satz (15.25) anwenden und erhalten eine direkte Summenzerlegung von V in Haupträume $U_i = \mathrm{Hau}(\phi, \lambda_i)$, mit $1 \leq i \leq r$. Setzen wir $\psi_i = \phi|_{U_i} - \lambda_i \cdot \mathrm{id}_{U_i}$, dann gilt nach Proposition (15.23) jeweils $\psi_i^{e_i} = \mathrm{id}_{U_i}$ für ein $e_i \in \mathbb{N}$, der Endomorphismus $\psi_i \in \mathrm{End}_K(U_i)$ ist also nilpotent. Nach Folgerung (15.19) existiert jeweils eine Jordanbasis $\mathcal{B}_i$ von U_i bezüglich ψ_i. Es ist dann $J_i = \mathcal{M}_{\mathcal{B}_i}(\psi_i)$ jeweils eine Matrix in Jordanscher Normalform, mit null als einzigem Eigenwert. Auf Grund der direkten Summenzerlegung ist $\mathcal{B} = \mathcal{B}_1 \cup ... \cup \mathcal{B}_r$ eine geordnete Basis von V. Die Darstellungsmatrix J_i' von $\phi|_{U_i}$ bezüglich $\mathcal{B}_i$ ist gegeben durch

$$J_i' \quad = \quad \mathcal{M}_{\mathcal{B}_i}(\phi|_{U_i}) \quad = \quad \mathcal{M}_{\mathcal{B}_i}(\psi_i + \lambda_i \cdot \mathrm{id}_{U_i}) \quad = \quad \mathcal{M}_{\mathcal{B}_i}(\psi_i) + \lambda_i \cdot \mathcal{M}_{\mathcal{B}_i}(\mathrm{id}_{U_i}) \quad = \quad \mathcal{M}_{\mathcal{B}_i}(\psi_i) + \lambda_i \cdot E_{n_i} \quad ,$$

wobei E_{n_i} die Einheitsmatrix der Größe $n_i = \dim U_i$ bezeichnet. Dabei handelt es sich um eine Matrix in Jordanscher Normalform, mit λ_i als einzigem Eigenwert. Wegen $\mathscr{B} = \mathscr{B}_1 \cup ... \cup \mathscr{B}_r$ und $\phi(U_i) \subseteq U_i$ für $1 \leq i \leq r$ ist dann die Matrix $J = \mathscr{M}_{\mathscr{B}}(\phi)$ eine Blockmatrix, mit den Blöcken $J'_1, ..., J'_r$ entlang der Hauptdiagonalen. Dies ist eine Matrix in Jordanscher Normalform. Setzen wir $T = \mathscr{T}_{\mathscr{E}}^{\mathscr{B}}$, wobei $\mathscr{E}$ die Einheitsmatrix des K^n bezeichnet, dann gilt auf Grund der Transformationsformel (11.16) die Gleichung

$$J \quad = \quad \mathscr{M}_{\mathscr{B}}(\phi) \quad = \quad \mathscr{T}_{\mathscr{B}}^{\mathscr{E}} \cdot \mathscr{M}_{\mathscr{E}}(\phi_A) \cdot \mathscr{T}_{\mathscr{E}}^{\mathscr{B}} \quad = \quad T^{-1}AT.$$

Dies zeigt, dass A und J ähnlich zueinander sind.

zu (ii) „⇒“ Seien $J, J' \in \mathscr{M}_{n,K}$ zwei Matrizen in Jordanscher Normalform, und nehmen wir an, dass J und J' ähnlich zueinander sind. Dann existiert eine Matrix $T \in \mathrm{GL}_n(K)$ mit $J' = T^{-1}JT$. Sei $\mathscr{B}$ die Basis von $V = K^n$ bestehend aus den Spaltenvektoren von T; dann gilt $T = \mathscr{T}_{\mathscr{E}}^{\mathscr{B}}$. Definieren wir nun $\phi \in \mathrm{End}_K(V)$ durch $\phi = \phi_J$, dann gilt auf Grund der Transformationsformel $J' = \mathscr{M}_{\mathscr{B}}(\phi)$; außerdem ist offenbar $J = \mathscr{M}_{\mathscr{E}}(\phi)$. Die Matrizen J und J' sind also Darstellungsmatrizen desselben Endomorphismus ϕ von V.

Sei nun λ ein Eigenwert von ϕ, und es sei a_k bzw. a'_k die Anzahl der Jordanblöcke der Größe k in J bzw. J' zum Eigenwert λ, für $1 \leq k \leq n$. Ist allgemein J'' eine Jordanmatrix zum Eigenwert λ der Größe k, dann ist $J'' - \lambda E$ nach Proposition (15.11) eine nilpotente Matrix vom Nilpotenzgrad k. Setzen wir nun $\psi = \phi - \lambda \mathrm{id}_V$ und $d_k = \dim \ker(\psi^k)$ für jedes k, so kann mit Hilfe dieser Feststellung an den Darstellungsmatrizen direkt abgelesen werden, dass jeweils $d_k = a_1 + ... + a_k$ gilt, und ebenso $d_k = a'_1 + ... + a'_k$. Weil die d_k's nur vom Endomorphismus abhängen, nicht aber von den Darstellungsmatrizen, leitet man daraus sukzessive $a_1 = a'_1$, $a_2 = a'_2$, ..., $a_n = a'_n$ ab. Dies zeigt, dass in J und J' dieselben Jordanblöcke zum Eigenwert λ vorkommen.

„⇐“ Seien $J, J' \in \mathscr{M}_{n,K}$ zwei Jordanmatrizen, die bis auf Reihenfolge dieselben Jordanblöcke enthalten. Es seien $J_1, ..., J_r$ die Jordanblöcke der Matrix J in der Reihenfolge ihres Auftretens, und es sei n_i jeweils die Größe von J_i, für $1 \leq i \leq r$. Für $0 \leq j \leq r$ sei jeweils $m_j = \sum_{i=1}^{j} n_i$, und für $1 \leq j \leq r$ sei $\mathscr{E}_j = (e_{m_{j-1}+1}, ..., e_{m_j})$. Dann ist $\mathscr{E} = \mathscr{E}_1 \cup ... \cup \mathscr{E}_r$ offenbar die Einheitsbasis. Definieren wir $U_j = \langle \mathscr{E}_j \rangle_K$, dann gilt auf Grund der Form der Matrix J jeweils $\phi_J(U_j) \subseteq U_j$ und $J_j = \mathscr{M}_{\mathscr{E}_j}(\phi_J|_{U_j})$. Da J' dieselben Jordanblöcke wie J enthält, gibt es eine Permutation $\sigma \in S_r$, so dass J' der Reihe nach die Jordanblöcke $J_{\sigma(1)}, ..., J_{\sigma(r)}$ enthält. Es ist $J_{\sigma(j)} = \mathscr{M}_{\mathscr{E}_{\sigma(j)}}(\phi_J|_{U_{\sigma(j)}})$ für $1 \leq j \leq r$. Daraus folgt, dass J' die Darstellungsmatrix von ϕ_J bezüglich der geordneten Basis $\mathscr{B} = \mathscr{E}_{\sigma(1)} \cup ... \cup \mathscr{E}_{\sigma(r)}$ ist. Setzen wir $T = \mathscr{T}_{\mathscr{E}}^{\mathscr{B}}$, dann gilt

$$J' \quad = \quad \mathscr{M}_{\mathscr{B}}(\phi_J) \quad = \quad \mathscr{T}_{\mathscr{B}}^{\mathscr{E}} \cdot \mathscr{M}_{\mathscr{E}}(\phi_J) \cdot \mathscr{T}_{\mathscr{E}}^{\mathscr{B}} \quad = \quad T^{-1}JT$$

auf Grund der Transformationsformel (11.16). Dies zeigt, dass J und J' zueinander ähnlich sind. □

Zum Schluss können wir noch das Verfahren zur Bestimmung einer Darstellungsmatrix in Jordanscher Normalform und einer zugehörigen geordneten Basis vervollständigen. Sei V ein endlich-dimensionaler K-Vektorraum und $\phi \in \mathrm{End}_K(V)$ ein Endomorphismus, dessen Minimalpolynom als Produkt von Linearfaktoren

$$\mu_\phi \quad = \quad \prod_{k=1}^{r} (x - \lambda_k)^{e_k} \quad \text{vorliegt.}$$

Ist an Stelle des Endomorphismus ϕ eine Matrix $A \in \mathscr{M}_{n,K}$ vorgegeben, dann setzt man $\phi = \phi_A$ und $V = K^n$.
Nun führt man die folgenden Schritte aus.

(1) Sei $U_k = \mathrm{Hau}(\phi, \lambda_k)$ für $1 \leq k \leq r$. Dann ist $\psi_k = (\phi - \lambda_k \mathrm{id}_V)|_{U_k}$ ein nilpotenter Endomorphismus, vom Nilpotenzgrad e_k.

(2) Wende nun das oben beschriebene Verfahren an, um für $1 \leq k \leq r$ eine Jordanbasis $\mathscr{B}_k$ von U_k zu erhalten. Dann ist $J_k = \mathscr{M}_{\mathscr{B}_k}(\psi_k)$ also eine Matrix in Jordanscher Normalform, mit null als einzigem Eigenwert.

(3) Auf Grund der direkten Summenzerlegung in Satz (15.25) ist $\mathscr{B} = \mathscr{B}_1 \cup \ldots \cup \mathscr{B}_r$ eine geordnete Basis von V.

(4) Setze $n_k = \dim U_k$ und $J_k' = J_k + \lambda_k E_{n_k}$ für $1 \leq k \leq r$. Dann ist $J = \mathscr{M}_{\mathscr{B}}(\phi)$ die Matrix bestehend aus den Blöcken J_k', also ebenfalls eine Matrix in Jordanscher Normalform.

(5) War zu Beginn des Verfahrens an Stelle eines Endomorphismus eine Matrix A vorgegeben, dann setzt man $T = \mathscr{T}_{\mathscr{E}}^{\mathscr{B}}$. Auf Grund der Transformationsformel (11.16) gilt dann $J = T^{-1}AT$, insbesondere sind A und J ähnlich.

§ 16. *Hurwitz-Kriterium und Hauptachsentransformation*

Inhaltsübersicht

Den Begriff der Bilinearform haben wir bereits in § 14 kennengelernt. Dort haben wir uns auf die Untersuchung der *Skalarprodukte* konzentriert, da sich diese für geometrische Anwendungen als besonders nützlich herausgestellt haben. In diesem Kapitel beschäftigen wir uns nun mit allgemeinen Bilinearformen, da auch diese wichtige Anwendungen inner- und außerhalb der Mathematik besitzen.

Genau wie den linearen Abbildungen kann auch einer Bilinearform auf einem endlich-dimensionalen Vektorraum V eine Darstellungsmatrix bezüglich einer geordneten Basis $\mathscr{B}$ zugeordnet werden. Ebenso gibt es auch hier eine Transformationsformel, mit der man Darstellungsmatrizen bezüglich unterschiedlicher Basen ineinander umrechnen kann. Häufig ist man daran interessiert, anhand der Darstellungsmatrix zu erkennen, ob die zu Grunde liegende Bilinearform positiv definit ist. Dies ist mit Hilfe des *Hurwitz-Kriteriums* möglich. Um den Beweis dieses Kriteriums vorzubereiten, behandeln wir zuvor ein Verfahren, mit dem für Räume mit einer positiv definiten Bilinearform eine Orthonormalbasis bestimmt werden kann. Am Ende des Kapitels befassen wir uns noch mit zwei wichtigen Klassen linearer Abbildungen, den orthogonalen und den selbstadjungierten Endomorphismen, und wir beweisen den Satz über die *Hauptachsentransformation*, der die Diagonalisierbarkeit der selbstadjungierte Endomorphismen sicherstellt.

Wichtige Begriffe und Sätze

- Darstellungsmatrix einer Bilinearform bezüglich einer geordneten Basis
- Transformationsformel für Bilinearformen
- positiv und negativ (semi-)definite Bilinearform
- positiv und negativ (semi-)definite Matrix
- Hurwitz-Kriterium für positiv definite Matrizen
- orientierungserhaltende und -umkehrende Bewegung
- orthogonale Matrix, orthogonaler Endomorphismus
- selbstadjungierter Endomorphismus
- Korrektheit des Gram-Schmidt-Verfahrens
- Satz von der Hauptachsentransformation

Sei V ein endlich-dimensionaler K-Vektorraum und $\mathscr{B} = (v_1, ..., v_n)$ eine geordnete Basis von V. Sei b eine Bilinearform auf V. Um $b(v, w)$ für beliebige Vektoren $v, w \in V$ auszurechnen, genügt es, die Werte $b(v_i, v_j)$ zu kennen. Sind nämlich $v = \sum_{k=1}^{n} \lambda_k v_k$ und $w = \sum_{\ell=1}^{n} \mu_\ell v_\ell$ Darstellungen von v und w als Linearkombinationen der Basis, dann gilt auf Grund der Linearität der Bilinearform in beiden Komponenten

$$b(v,w) \quad = \quad b\left(\sum_{k=1}^{n} \lambda_k v_k, \sum_{\ell=1}^{n} \mu_\ell v_\ell\right) \quad = \quad \sum_{k=1}^{n} \lambda_k b\left(v_k, \sum_{\ell=1}^{n} \mu_\ell v_\ell\right) \quad = \quad \sum_{k=1}^{n}\sum_{\ell=1}^{n} \lambda_k \mu_\ell b(v_k, v_\ell).$$

Dies liefert uns die Möglichkeit, eine Bilinearform auf einem endlich-dimensionalen $\mathbb{R}$-Vektorraum auf kompakte Art und Weise durch Angabe einer Matrix zu definieren.

(16.1) Definition Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorrau, $\mathscr{B} = (v_1, ..., v_n)$ eine geordnete Basis und b eine Bilinearform auf V. Dann nennt man die reelle $n \times n$-Matrix $A = (a_{ij})$ mit den Einträgen

$$a_{ij} \quad = \quad b(v_i, v_j) \qquad \text{für} \quad 1 \leq i, j \leq n$$

die ***Darstellungsmatrix*** $M_{\mathscr{B}}(b)$ von b bezüglich $\mathscr{B}$.

Wir illustrieren den Begriff der Darstellungsmatrix an einer Reihe von Beispielen.

(i) Sei $V = \mathbb{R}^n$ und $\mathscr{E}$ die Basis bestehend aus den Einheitsvektoren $e_1, ..., e_n$. Dann ist die Darstellungsmatrix des euklidischen Skalarprodukts $\langle \cdot, \cdot \rangle$ bezüglich $\mathscr{E}$ die Einheitsmatrix. Denn für alle k, ℓ mit $1 \leq k, \ell \leq n$ gilt $\langle e_k, e_\ell \rangle = \delta_{k\ell}$, und dies sind genau die Einträge der Einheitsmatrix E_n.

(ii) Sei $V = \mathbb{R}^3$. Diesmal betrachten wir das euklidische Skalarprodukt bezüglich einer anderen Basis, nämlich $\mathscr{B} = (v_1, v_2, v_3)$ bestehend aus den Vektoren $v_1 = (1, 0, 2)$, $v_2 = (3, 3, -1)$ und $v_3 = (5, -1, 2)$. Die erste Zeile der Darstellungsmatrix $M_{\mathscr{B}}(b) = (a_{ij})$ erhält man durch die Berechung der Skalarprodukte

$$a_{11} = \langle v_1, v_1 \rangle \quad , \quad a_{12} = \langle v_1, v_2 \rangle \quad \text{und} \quad a_{13} = \langle v_1, v_3 \rangle = 9.$$

Berechnet man nach demselben Schema auch die zweite und dritte Zeile, so erhält man insgesamt die Matrix

$$M_{\mathscr{B}}(b) \quad = \quad \begin{pmatrix} 5 & 1 & 9 \\ 1 & 19 & 10 \\ 9 & 10 & 30 \end{pmatrix}.$$

(iii) Sei V der Vektorraum der Polynomfunktionen vom Grad ≤ 1 und die Bilinearform $b : V \times V \to \mathbb{R}$ definiert durch

$$b(f, g) \quad = \quad \int_0^1 f(x)g(x)\, dx \qquad \text{für} \quad f, g \in V.$$

Seien nun $f_1, f_2 \in V$ definiert durch $f_1(x) = x$ und $f_2(x) = x + 1$. Dann ist $\mathscr{B} = (f_1, f_2)$ eine geordnete Basis von V. Es gilt

$$b(f_1, f_1) \quad = \quad \int_0^1 f_1(x)^2\, dx = \int_0^1 x^2\, dx \quad = \quad \left[\tfrac{1}{3}x^3\right]_0^1 \quad = \quad \tfrac{1}{3} \qquad ,$$

$$b(f_1, f_2) \quad = \quad b(f_2, f_1) \quad = \quad \int_0^1 f_1(x)f_2(x)\, dx \quad = \quad \int_0^1 (x^2 + x)\, dx \quad = \quad \left[\tfrac{1}{3}x^3 + \tfrac{1}{2}x^2\right]_0^1$$

$$= \quad \tfrac{1}{3} + \tfrac{1}{2} \quad = \quad \tfrac{5}{6}$$

und

$$b(f_2, f_2) \quad = \quad \int_0^1 f_2(x)^2\, dx \quad = \quad \int_0^1 (x^2 + 2x + 1)\, dx \quad =$$

$$\left[\tfrac{1}{3}x^3 + x^2 + x\right]_0^1 \quad = \quad \tfrac{1}{3} + 1 + 1 \quad = \quad \tfrac{8}{3}.$$

Wir erhalten somit die Darstellungsmatrix

$$M_{\mathscr{B}}(b) \quad = \quad \tfrac{1}{6}\begin{pmatrix} 2 & 5 \\ 5 & 16 \end{pmatrix}.$$

Jeder Bilinearform auf einem endlich-dimensionalen $\mathbb{R}$-Vektorraum kann also (nach Wahl einer geordneten Basis) eine Matrix zugeordnet werden. Umgekehrt existiert zu jeder Matrix eine entsprechende Bilinearform.

(16.2) Satz Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und $\mathscr{B} = (v_1, ..., v_n)$ eine geordnete Basis von V. Dann existiert für jede Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ eine eindeutig bestimmte Bilinearform b auf V mit $M_{\mathscr{B}}(b) = A$.

Beweis: Existenz: Zu einer vorgegebenen $n \times n$-Matrix $A = (a_{ij})$ definieren wir eine Abbildung $b : V \times V \to \mathbb{R}$, indem wir einem Paar von Vektoren $(v, w) \in V \times V$ mit den (eindeutig bestimmten) Basisdarstellungen $v = \sum_{i=1}^n \lambda_i v_i$ und $w = \sum_{j=1}^n \mu_j v_j$, $\lambda_i, \mu_j \in \mathbb{R}$ für $1 \leq i, j \leq n$ das Bild

$$b(v, w) \quad = \quad \sum_{i=1}^n \sum_{j=1}^n \lambda_i \mu_j a_{ij} \qquad \text{zuordnen.}$$

Dann gilt insbesondere $b(v_i, v_j) = a_{ij}$ für $1 \leq i, j \leq n$. Es muss nun überprüft werden, dass auf diese Weise tatsächlich eine Bilinearform auf V definiert ist. Wir beschränken uns auf den Nachweis der Gleichung $b(v + v', w) = b(v, w) + b(v', w)$ für alle $v, v', w \in V$. Seien also $v, v', w \in V$ mit den Basisdarstellungen $v = \sum_{i=1}^n \lambda_i v_i$, $v' = \sum_{i=1}^n \lambda_i' v_i$, $w = \sum_{j=1}^n \mu_j v_j$. Dann besitzt der Vektor $v + v'$ die Basisdarstellung $\sum_{i=1}^n (\lambda_i + \lambda_i') v_i$, und es folgt

$$b(v + v', w) \quad = \quad \sum_{i=1}^n \sum_{j=1}^n (\lambda_i + \lambda_i') \mu_j a_{ij} \quad = \quad \sum_{i=1}^n \sum_{j=1}^n \lambda_i \mu_j a_{ij} + \sum_{i=1}^n \sum_{j=1}^n \lambda_i' \mu_j a_{ij}$$

$$= \quad b(v, w) + b(v', w).$$

Der Beweis der Gleichungen $b(v, w + w') = b(v, w) + b(v, w')$ und $b(\lambda v, w) = b(v, \lambda w) = \lambda b(v, w)$ für $v, v', w \in V$ und $\lambda \in \mathbb{R}$ funktioniert nach demselben Schema.

Eindeutigkeit: Seien b, b' zwei Bilinearformen mit $b(v_i, v_j) = b'(v_i, v_j) = a_{ij}$ für $1 \leq i, j \leq n$. Seien $v, w \in V$ mit Basisdarstellungen $v = \sum_{i=1}^n \lambda_i v_i$ und $w = \sum_{j=1}^n \mu_j v_j$. Durch Anwendung der der Bilinearität der Abbildung b erhalten wir

$$b(v, w) \quad = \quad b\left(\sum_{i=1}^n \lambda_i v_i, w\right) \quad = \quad \sum_{i=1}^n \lambda_i b(v_i, w) \quad = \quad \sum_{i=1}^n \lambda_i b\left(v_i, \sum_{j=1}^n \mu_j v_j\right)$$

$$= \quad \sum_{i=1}^n \sum_{j=1}^n \lambda_i \mu_j b(v_i, v_j) \quad = \quad \sum_{i=1}^n \sum_{j=1}^n \lambda_i \mu_j a_{ij}.$$

Durch eine analoge Rechnung überprüft man auch die Gleichung $b'(v, w) = \sum_{i=1}^n \sum_{j=1}^n \lambda_i \mu_j a_{ij}$. □

Für viele Anwendungen ist es wichtig, Darstellungsmatrizen von Bilinearformen bezüglich verschiedener Basen ineinander umrechnen zu können, auf ähnliche Weisen, wie wir bereits in § 7 Darstellungsmatrizen von linearen Abbildungen umgerechnet haben.

Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum, b eine Bilinearform auf V und $\mathscr{B} = (v_1, ..., v_n)$ eine geordnete Basis von V. In § 11 haben wir jedem $v \in V$ einen ***Koordinatenvektor*** $\Phi_{\mathscr{B}}(v) = {}^{\mathrm{t}}(\lambda_1, ..., \lambda_n) \in \mathbb{R}^n$ zugeordnet, dessen Einträge $\lambda_k \in \mathbb{R}$ jeweils die Gleichung $v = \sum_{k=1}^{n} \lambda_k v_k$ erfüllen. Es zeigt sich nun, dass die Bilinearform für vorgegebene Vektoren auch mit Hilfe der Koordinatenvektoren und der Darstellungsmatrix ausgedrückt werden kann.

(16.3) Proposition Unter den angegebenen Voraussetzungen gilt für alle $v, w \in V$ jeweils

$$b(v,w) \quad = \quad {}^{\mathrm{t}}\Phi_{\mathscr{B}}(v)\mathscr{M}_{\mathscr{B}}(b)\Phi_{\mathscr{B}}(w).$$

Beweis: Diese Gleichung kann direkt nachgerechnet werden. Seien die Koordinatenvektoren von v und w bezüglich $\mathscr{B}$ gegeben durch $\Phi_{\mathscr{B}}(v) = {}^{\mathrm{t}}(\lambda_1, ..., \lambda_n)$ und $\Phi_{\mathscr{B}}(w) = {}^{\mathrm{t}}(\mu_1, ..., \mu_n)$. Dann gilt $v = \sum_{k=1}^{n} \lambda_k v_k$ und $w = \sum_{\ell=1}^{n} \mu_\ell v_\ell$, und die Einträge $a_{k\ell}$ der Darstellungsmatrix $\mathscr{M}_{\mathscr{B}}(b)$ sind durch $b(v_k, v_\ell)$ gegeben, für $1 \le k, \ell \le n$. Das Produkt ${}^{\mathrm{t}}\Phi_{\mathscr{B}}(v)\mathscr{M}_{\mathscr{B}}(b)$ ist ein Zeilenvektor der Länge n. Bezeichnen wir dessen Einträge mit $\tilde{\lambda}_1, ..., \tilde{\lambda}_n$, dann gilt nach Definition des Matrix-Vektor-Produkts jeweils

$$\tilde{\lambda}_\ell \quad = \quad \sum_{k=1}^{n} \lambda_k b(v_k, v_\ell) \qquad \text{für} \quad 1 \le \ell \le n.$$

Für die rechte Seite der Gleichung erhalten wir damit insgesamt den Wert

$$\sum_{\ell=1}^{n} \tilde{\lambda}_\ell \mu_\ell \quad = \quad \sum_{\ell=1}^{n} \left(\sum_{k=1}^{n} \lambda_k b(v_k, v_\ell) \right) \mu_\ell \quad = \quad \sum_{k=1}^{n} \sum_{\ell=1}^{n} \lambda_k \mu_\ell b(v_k, v_\ell).$$

Auf der linken Seite der Gleichung gilt

$$b(v,w) \quad = \quad b\left(\sum_{k=1}^{n} \lambda_k v_k, \sum_{\ell=1}^{n} \mu_\ell w_\ell \right) \quad = \quad \sum_{k=1}^{n} \sum_{\ell=1}^{n} \lambda_k \mu_\ell b(v_k, v_\ell).$$

Also stimmen die beiden Seiten überein. □

Im Beispiel von oben hat der Vektor $v = 1 \cdot v_1 + 1 \cdot v_2 + 1 \cdot v_3$ bezüglich der Basis $\mathscr{B} = (v_1, v_2, v_3)$ den Koordinatenvektor $\Phi_{\mathscr{B}}(v) = {}^{\mathrm{t}}(1,1,1)$. Mit Hilfe der Darstellungsmatrix des euklidischen Standard-Skalarprodukts bezüglich $\mathscr{B}$ können wir den Wert $\langle v, v \rangle$ ausrechnen. Es gilt

$$\langle v, v \rangle \quad = \quad {}^{\mathrm{t}}\Phi_{\mathscr{B}}(v)\mathscr{M}_{\mathscr{B}}(b)\Phi_{\mathscr{B}}(v) \quad = \quad \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 5 & 1 & 9 \\ 1 & 19 & 10 \\ 9 & 10 & 30 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 15 & 30 & 49 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad = \quad 94.$$

Andererseits können wir $\langle v, v \rangle$ natürlich auch direkt ausrechnen. Es gilt $v = v_1 + v_2 + v_3 = (9, 2, 3)$ und somit $\langle v, v \rangle = 9^2 + 2^2 + 3^2 = 94$.

(16.4) Satz *(Transformationsformel für Bilinearformen)*

Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und b eine Bilinearform auf V. Seien $\mathscr{A}$ und $\mathscr{B}$ zwei geordnete Basen von V und $A = M_{\mathscr{A}}(b)$, $B = M_{\mathscr{B}}(b)$ die Darstellungsmatrizen von b bezüglich dieser Basen. Sei $T = \mathscr{T}_{\mathscr{B}}^{\mathscr{A}}$ die Matrix des Basiswechsels von $\mathscr{A}$ nach $\mathscr{B}$. Dann gilt $A = {}^tTBT$.

Beweis: Sei $A = (a_{ij})$, $B = (b_{ij})$ und $T = (t_{ij})$. Wir überprüfen, dass ${}^tTBT$ die Darstellungsmatrix von b bezüglich $\mathscr{A}$ ist und beweisen auf diesem Weg die Gleichung $A = {}^tTBT$. Der Eintrag der Matrix $C = BT$ an der Stelle (k,ℓ) ist $c_{k\ell} = \sum_{j=1}^{n} b_{kj}t_{j\ell}$. Der Eintrag von ${}^tTC = {}^tTBT$ an der Stelle (k,ℓ) ist folglich durch die Summe

$$\sum_{i=1}^{n} t_{ik}c_{i\ell} \quad = \quad \sum_{i=1}^{n}\sum_{j=1}^{n} t_{ik}b_{ij}t_{j\ell} \quad = \quad \sum_{i=1}^{n}\sum_{j=1}^{n} t_{ik}t_{j\ell}b_{ij} \qquad \text{gegeben.}$$

Sei $\mathscr{A} = (v_1, ..., v_n)$ und $\mathscr{B} = (w_1, ..., w_n)$. Weil T die Matrix des Basiswechsels von $\mathscr{A}$ nach $\mathscr{B}$ ist, gilt $v_k = \sum_{i=1}^{n} t_{ik}w_i$ für $1 \le k \le n$. Für $1 \le k, \ell \le n$ ist somit

$$b(v_k, v_\ell) \quad = \quad b\left(\sum_{i=1}^{n} t_{ik}w_i, \sum_{j=1}^{n} t_{j\ell}w_j\right) \quad = \quad \sum_{k=1}^{n}\sum_{\ell=1}^{n} t_{ik}t_{j\ell}\,b(w_i, w_j) \quad = \quad \sum_{k=1}^{n}\sum_{\ell=1}^{n} t_{ik}t_{j\ell}b_{ij}.$$

Also ist ${}^tTBT$ tatsächlich die Darstellungsmatrix von b bezüglich der Basis $\mathscr{A}$. □

Man beachte hierbei die Analogie zur Transformationsformel aus § 11: Ist $\phi : V \to V$ ein Endomorphismus von V, dann besteht zwischen den Darstellungsmatrizen von ϕ bezüglich der beiden geordneten Basen $\mathscr{A}$ und $\mathscr{B}$ der Zusammenhang $M_{\mathscr{A}}(\phi) = T^{-1}M_{\mathscr{B}}(\phi)T$, wobei $T = T_{\mathscr{B}}^{\mathscr{A}}$ wieder die Matrix des Basiswechsels bezeichnet. Bei Bilinearformen muss also lediglich die inverse Matrix T^{-1} durch die transponierte Matrix ${}^tT$ ersetzt werden!

Für die weitere Entwicklung benötigen wir ein Verfahren zur Berechnung von Orthonormalbasen auf Untervektorräumen des $\mathbb{R}^n$. Dazu erinnern wir an den Begriff der ***Orthogonalprojektion*** aus § 14. Sei U ein Untervektorraum des $\mathbb{R}^n$. Dann existiert eine eindeutig bestimmte lineare Abbildung $\pi_U : \mathbb{R}^n \to U$ mit der Eigenschaft, dass für alle $v \in \mathbb{R}^n$ jeweils $(v - \pi_U(v)) \perp U$ gilt. Wir hatten π_U als Orthogonalprojektion auf den Untervektorraum U bezeichnet.

(16.5) Satz *(Gram-Schmidt-Orthonormalisierung)*

(i) Sei $U \subseteq \mathbb{R}^n$ ein Untervektorraum der Dimension $m \in \mathbb{N}_0$ von V, $(u_1, ..., u_m)$ eine ON-Basis und $U' \supseteq U$ ein $(m+1)$-dimensionaler Untervektorraum. Dann existiert ein Vektor $u_{m+1} \in U'$, so dass $(u_1, ..., u_m, u_{m+1})$ eine ON-Basis von U' ist.

(ii) Jeder Untervektorraum des $\mathbb{R}^n$ besitzt eine ON-Basis.

Beweis: zu (i) Sei $v \in U' \setminus U$ beliebig gewählt und $w = v - \pi_U(v)$. Dann gilt $w \perp U$ nach. Setzen wir $u_{m+1} = \frac{1}{\|w\|}w$, dann gilt $\langle u_{m+1}, u_{m+1}\rangle = 1 = \delta_{m+1,m+1}$. Weil mit w auch u_{m+1} auf U senkrecht steht, gilt außerdem $\langle u_k, u_{n+1}\rangle =$

$\langle u_{n+1}, u_k\rangle = 0 = \delta_{k,m+1}$ für $1 \le k \le m$. Für alle k, ℓ mit $1 \le k, \ell \le m$ ist $\langle u_k, u_\ell\rangle = \delta_{k\ell}$ erfüllt, weil $(u_1, ..., v_m)$ eine ON-Basis von U ist. Insgesamt ist $(u_1, ..., u_{m+1})$ also eine ON-Basis von U'.

zu (ii) Wir beweisen die Aussage durch vollständige Induktion über die Dimension. Der null-dimensionale Untervektorraum $\{0_{\mathbb{R}^n}\}$ besitzen das leere Tupel $\varnothing$ als ON-Basis. Sei nun $m \in \mathbb{N}_0$, und setzen wir die Aussage für m voraus. Sei U' ein $(m+1)$-dimensionaler Untervektorraum des $\mathbb{R}^n$ und darin wiederum $U \subseteq U'$ ein beliebiger m-dimensionaler Untervektorraum. Dann existiert nach Induktionsvoraussetzung eine ON-Basis von U, und nach Teil (i) können wir diese zu einer ON-Basis von U' erweitern. □

Aus dem letzten Satz können wir das folgende Verfahren zur Bestimmung einer ON-Basis ableiten. Sei U ein m-dimensionaler Untervektorraum des $\mathbb{R}^n$.

(1) Wähle eine beliebige Basis $\mathscr{B} = (v_1, ..., v_m)$ von U und und setze $k = 0$, $\mathscr{B}' = \varnothing$.

(2) Im Fall $k = m$ ist das Verfahren beendet. Ansonsten nehmen wir an, dass $\mathscr{B}' = (u_1, ..., u_k)$ bereits eine *ON*-Basis von $U_k = \langle v_1, ..., v_k\rangle_{\mathbb{R}}$ ist.

(3) Berechne gemäß Proposition(14.15) die Orthogonalprojektion $w_{k+1} = \pi_{U_k}(v_{k+1})$ von v_{k+1} auf U_k durch

$$w_{k+1} \quad = \quad \sum_{\ell=1}^{k} \langle u_\ell, v_{k+1}\rangle u_\ell .$$

(4) Definiere den Vektor $\tilde{u}_{k+1} = v_{k+1} - w_{k+1}$ und normiere ihn zu $u_{k+1} = \|\tilde{u}_{k+1}\|^{-1}\tilde{u}_{k+1}$.

(5) Erweitere $\mathscr{B}'$ um den Vektor u_{k+1}, ersetze k durch $k+1$, und gehe zurück zu Schritt (2).

Wenn man bereits über eine ON-Basis $\mathscr{B}'$ für einen Untervektorraum von U verfügt, kann das Verfahren auch genutzt werden, um diese zu einer ON-Basis von ganz U zu erweitern. Als konkretes Beispiel betrachten wir $U = \mathbb{R}^3$ und den Vektor $u_1 = (\frac{1}{3}, \frac{2}{3}, \frac{2}{3})$. Unser Ziel besteht darin, die ON-Basis $\mathscr{B}' = (u_1)$ dieses Untervektorraums zu einer ON-Basis von $\mathbb{R}^3$ zu erweitern. Dafür müssen wir den oben angegebenen Algorithmus über zwei „Runden“ laufen lassen. Mit den dort verwendeten Bezeichnungen gilt

k = 1

$\langle u_1, e_2\rangle = \frac{2}{3}$

$w_2 = \langle u_1, e_2\rangle u_1 = \frac{2}{3}u_1 = \frac{2}{3}(\frac{1}{3}, \frac{2}{3}, \frac{2}{3}) = (\frac{2}{9}, \frac{4}{9}, \frac{4}{9})$

$\tilde{u}_2 = e_2 - w_2 = (0,1,0) - (\frac{2}{9}, \frac{4}{9}, \frac{4}{9}) = (-\frac{2}{9}, \frac{5}{9}, -\frac{4}{9})$

$\|\tilde{u}_2\| = \sqrt{(-\frac{2}{9})^2 + (\frac{5}{9})^2 + (-\frac{4}{9})^2} = \sqrt{\frac{45}{81}} = \frac{1}{3}\sqrt{5}$

$u_2 = \|\tilde{u}_2\|^{-1}\tilde{u}_2 = \frac{3}{\sqrt{5}}(-\frac{2}{9}, \frac{5}{9}, -\frac{4}{9}) = (-\frac{2}{3\sqrt{5}}, \frac{1}{3}\sqrt{5}, -\frac{4}{3\sqrt{5}})$

k = 2

$\langle u_1, e_3\rangle = \frac{2}{3}$, $\langle u_2, e_3\rangle = -\frac{4}{3\sqrt{5}}$

$w_3 = \langle u_1, e_3\rangle u_1 + \langle u_2, e_3\rangle u_2 = \frac{2}{3}(\frac{1}{3}, \frac{2}{3}, \frac{2}{3}) - \frac{4}{3\sqrt{5}}(-\frac{2}{3\sqrt{5}}, \frac{1}{3}\sqrt{5}, -\frac{4}{3\sqrt{5}})$
$= (\frac{2}{9}, \frac{4}{9}, \frac{4}{9}) + (\frac{8}{45}, -\frac{4}{9}, \frac{16}{45}) = (\frac{2}{5}, 0, \frac{4}{5})$

$\tilde{u}_3 = e_3 - w_3 = (0,0,1) - (\frac{2}{5}, 0, \frac{4}{5}) = (-\frac{2}{5}, 0, \frac{1}{5})$

$\|\tilde{u}_3\| = \sqrt{(-\frac{2}{5})^2 + 0^2 + (\frac{1}{5})^2} = \sqrt{\frac{1}{5}} = \frac{1}{\sqrt{5}}$

$u_3 = \|\tilde{u}_3\|^{-1}\tilde{u}_3 = \sqrt{5}(-\frac{2}{5}, 0, \frac{1}{5}) = (-\frac{2}{\sqrt{5}}, 0, \frac{1}{\sqrt{5}})$

Also ist (u_1, u_2, u_3) bestehend aus den Vektoren $u_1 = (\frac{1}{3}, \frac{2}{3}, \frac{2}{3})$, $u_2 = (-\frac{2}{3\sqrt{5}}, \frac{1}{3}\sqrt{5}, -\frac{4}{3\sqrt{5}})$, $u_3 = (-\frac{2}{\sqrt{5}}, 0, \frac{1}{\sqrt{5}})$ eine ON-Basis von $\mathbb{R}^3$. Es empfiehlt sich, zur Sicherheit die Gleichungen $\langle u_k, u_\ell \rangle = \delta_{k\ell}$ für $1 \leq k, \ell \leq 3$ zu überprüfen.

Wir bemerken noch, dass Satz (16.5) nicht nur für den $\mathbb{R}^n$ mit dem Standard-Skalarprodukt, sondern für beliebige endlich-dimensionale euklidische Vektorräume, also endlich-dimensionale $\mathbb{R}$-Vektorräume mit einem Skalarprodukt, gültig ist. Dementsprechend funktioniert auch das Gram-Schmidt-Verfahren für Vektorräume dieser Art.

Wir fahren nun fort mit der allgemeinen Theorie der Bilinearformen. Eine Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ wird symmetrisch genannt, wenn $A = {}^tA$ gilt. Der folgende Satz stellt einen Zusammenhang mit den symmetrischen Bilinearformen her.

> **(16.6) Proposition** Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und b eine Bilinearform auf V. Sei $\mathscr{B}$ eine beliebige Basis von V und $A = M_{\mathscr{B}}(b)$. Unter diesen Voraussetzungen ist b genau dann symmetrisch, wenn A symmetrisch ist.

Beweis: Sei $A = (a_{ij})$ und $\mathscr{B} = (v_1, ..., v_n)$. Nach Definition der Darstellungsmatrix gilt $b(v_i, v_j) = a_{ij}$ für $1 \leq i, j \leq n$. Sei die Abbildung $\tilde{b} : V \times V \to \mathbb{R}$ gegeben durch

$$\tilde{b}(v, w) \quad = \quad b(w, v) \qquad \text{für alle} \quad v, w \in V.$$

Man überprüft unmittelbar, dass auch $\tilde{b}$ eine Bilinearform ist. Offenbar ist b genau dann symmetrisch, wenn $b = \tilde{b}$ gilt. Wegen $\tilde{b}(v_i, v_j) = b(v_j, v_i) = a_{ji}$ für $1 \leq i, j \leq n$ gilt $\mathscr{M}_{\mathscr{B}}(\tilde{b}) = {}^tA$. Nach Satz (16.2) stimmen zwei Bilinearformen genau dann überein, wenn ihre Darstellungsmatrizen gleich sind. Also ist die Gleichheit $b = \tilde{b}$ äquivalent zur Übereinstimmung $A = {}^tA$ der Matrizen. □

Bereits in § 10 haben wir die Eigenschaft „positiv definit“ für eine symmetrische Bilinearform definiert. Wir führen nun noch weitere Klassen von Bilinearformen ein.

> **(16.7) Definition** Sei V ein $\mathbb{R}$-Vektorraum und b eine symmetrische Bilinearform auf V. Man bezeichnet b als
>
> (i) ***positiv semidefinit***, wenn $b(v, v) \geq 0$
>
> (ii) ***negativ semidefinit***, wenn $b(v, v) \leq 0$
>
> (iii) ***negativ definit***, wenn $b(v, v) < 0$
>
> jeweils für alle $v \in V \setminus \{0_V\}$ gilt. Eine Bilinearform die weder positiv noch negativ semidefinit ist, bezeichnet man als ***indefinit***.

Es erweist sich als praktisch, diese Begriffe auch für symmetrische quadratische Matrizen zur Verfügung zu haben. Bezeichnet $\mathscr{E}$ die Einheitsbasis des $\mathbb{R}^n$, so existiert für jede symmetrische Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ nach Satz (16.2) eine eindeutig bestimmte Bilinearform b mit $\mathscr{M}_{\mathscr{E}}(b) = A$. Diese ist gegeben durch $b(v, w) = {}^tvAw$ für alle $v, w \in \mathbb{R}^n$.

(16.8) Definition Eine symmetrische Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ wird als ***positiv definit*** (bzw. positiv semidefinit, negativ (semi-)definit, indefinit) bezeichnet, wenn die Bilinearform b_A gegeben durch $b_A(v,w) = {}^t vAw$ diese Eigenschaft besitzt.

Beispielsweise ist die Einheitsmatrix positiv definit, denn dies ist die Darstellungsmatrix des euklidischen Standard-Skalarprodukts bezüglich der Einheitsbasis. Es ist leicht zu sehen, dass jede Diagonalmatrix mit lauter positiven Einträgen positiv definit ist.

(16.9) Satz *(Hurwitz-Kriterium)*

Sei $A \in \mathscr{M}_{n,\mathbb{R}}$ eine symmetrische Matrix und A_k jeweils die linke obere $k \times k$-Teilmatrix, für $1 \leq k \leq n$. Genau dann ist A positiv definit, wenn $\det(A_k) > 0$ für $1 \leq k \leq n$ erfüllt ist.

Beweis: Wir führen folgende Bezeichnungen ein: Für $k \in \{1,...,n\}$ sei $\mathscr{E}_k = (e_1,...,e_k)$ jeweils das k-Tupel bestehend aus den ersten k Einheitsvektoren im $\mathbb{R}^n$. Dann spannt $\mathscr{E}_k$ jeweils den Untervektorraum $U_k = \langle \mathscr{E}_k \rangle_{\mathbb{R}} = \mathbb{R}^k \times \{0\}^{n-k}$ von $\mathbb{R}^n$ auf. Wir bezeichnen mit b die eindeutig bestimmte Bilinearform auf $\mathbb{R}^n$ mit der Darstellungsmatrix A und mit b_k jeweils die Einschränkung von b auf den Untervektorraum U_k. Nach Definition der Darstellungsmatrix gilt $A_k = M_{\mathscr{E}_k}(b_k)$ für $1 \leq k \leq n$.

„⇒“ Ist A positiv definit, dann gibt es auf Grund des Gram-Schmidt-Verfahrens eine Basis $\mathscr{B} = (v_1,...,v_n)$, so dass $\mathscr{B}_k = (v_1,...,v_k)$ jeweils eine ON-Basis von U_k ist, für $1 \leq k \leq n$. Nach Definition gilt $E_k = \mathscr{M}_{\mathscr{B}_k}(b_k)$ für $1 \leq k \leq n$, die Darstellungsmatrizen bezüglich $\mathscr{B}_k$ sind also die Einheitsmatrizen. Setzen wir nun $T_k = T^{\mathscr{E}_k}_{\mathscr{B}_k}$ für jedes k, dann erhalten wir nach Satz (16.4) jeweils

$$A_k \quad = \quad \mathscr{M}_{\mathscr{E}_k}(b_k) \quad = \quad {}^t T^{\mathscr{E}_k}_{\mathscr{B}_k} M_{\mathscr{B}_k}(b_k) T^{\mathscr{E}_k}_{\mathscr{B}_k} \quad = \quad {}^t T_k E_k T_k \quad = \quad {}^t T_k T_k$$

und folglich $\det(A_k) = \det(T_k)^2 > 0$. Denn als Transformationsmatrix ist T_k invertierbar, d. h. es gilt $\det(T_k) \neq 0$.

„⇐“ Hier zeigen wir durch vollständige Induktion über k, dass die Bilinearform b_k auf U_k positiv definit ist. Setzen wir $A = (a_{k\ell})$, dann gilt $A_1 = (a_{11})$, und aus $\det(A_1) > 0$ folgt $a_{11} > 0$. Dies wiederum bedeutet, dass b_1 positiv definit ist. Für jeden Vektor $v \in U_1$ mit $v \neq 0$ gibt es nämlich ein $\lambda \in \mathbb{R}^\times$ mit $v = \lambda e_1$, und es folgt $b(v,v) = \lambda^2 b(e_1,e_1) = \lambda^2 a_{11} > 0$. Damit ist der Induktionsanfang abgeschlossen.

Sei nun $k \in \mathbb{N}$ mit $1 \leq k < n$ und setzen wir voraus, dass b_k positiv definit ist. Auf Grund des Gram-Schmidt-Verfahrens existiert eine ON-Basis $(u_1,...,u_k)$ von U_k bezüglich b_k. Setzen wir nun $w = e_{k+1} - \pi_{U_k}(e_{k+1})$, dann gilt $w \perp_{b_k} U_k$ nach Definition der Orthogonalprojektion π_{U_k}. Mit e_{k+1} ist außerdem auch w in $U_{k+1} \setminus U_k$ enthalten. Dies zeigt, dass durch $\mathscr{B} = (u_1,...,u_k,w)$ eine Basis von U_{k+1} gegeben ist. Auf Grund der ON-Eigenschaft von $(u_1,...,u_k)$ und wegen $w \perp_{b_k} U_k$ hat b_{k+1} bezüglich $\mathscr{B}$ die Darstellungsmatrix

$$\mathscr{M}_{\mathscr{B}}(b_{k+1}) \quad = \quad \begin{pmatrix} E^{(k)} & 0 \\ 0 & a \end{pmatrix},$$

mit einem geeigneten $a \in \mathbb{R}$. Setzen wir nun $T = T_{\mathscr{B}}^{\mathscr{E}_{k+1}}$, dann gilt wegen Satz (16.4) die Gleichung

$$A_{k+1} \quad = \quad \mathscr{M}_{\mathscr{E}_{k+1}}(b_{k+1}) \quad = \quad {}^{\mathrm{t}}T_{\mathscr{B}}^{\mathscr{E}_{k+1}} \mathscr{M}_{\mathscr{B}}(b_{k+1}) T_{\mathscr{B}}^{\mathscr{E}_{k+1}} \quad = \quad {}^{\mathrm{t}}T \begin{pmatrix} E^{(k)} & 0 \\ 0 & a \end{pmatrix} T.$$

Es folgt $\det(A_{k+1}) = \det(T)^2 a$. Nach Voraussetzung ist $\det(A_{k+1}) > 0$, daraus folgt $a > 0$. Damit können wir nun zeigen, dass b_{k+1} positiv definit ist. Sei $v \in U_{k+1}$ mit $v \neq 0$. Setzen wir ${}^{\mathrm{t}}(\lambda_1, \ldots, \lambda_{k+1}) = \Phi_{\mathscr{B}}(v)$, dann ist mindestens ein λ_ℓ ungleich Null, und folglich gilt nach Prop. (16.3) dann

$$b_{k+1}(v,v) \quad = \quad \begin{pmatrix} \lambda_1 & \cdots & \lambda_k & \lambda_{k+1} \end{pmatrix} \begin{pmatrix} E^{(k)} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \\ \lambda_{k+1} \end{pmatrix} \quad = \quad \begin{pmatrix} \lambda_1 & \cdots & \lambda_k & a\lambda_{k+1} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \\ \lambda_{k+1} \end{pmatrix}$$

$$= \quad \sum_{\ell=1}^{k} \lambda_\ell^2 + a\lambda_{k+1}^2 \quad > \quad 0. \qquad \square$$

Als Anwendungsbeispiel zum Hurwitz-Kriterium zeigen, dass die Matrix $A \in \mathscr{M}_{3,\mathbb{R}}$ gegeben durch

$$A \quad = \quad \begin{pmatrix} 5 & 1 & 9 \\ 1 & 19 & 10 \\ 9 & 10 & 30 \end{pmatrix}$$

positiv definit ist. Auf Grund des Kriteriums müssen wir überprüfen, dass die Matrizen $\det(A_1)$, $\det(A_2)$ und $\det(A_3)$ alle positiv sind. Tatsächlich gilt

$$\det(A_1) = \det((5)) = 5 > 0 \quad , \quad \det(A_2) = \det \begin{pmatrix} 5 & 1 \\ 1 & 19 \end{pmatrix} = 94 > 0 \quad \text{und} \quad \det(A_3) = \det(A) = 961 > 0.$$

(16.10) Folgerung Eine Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ ist genau dann negativ definit, wenn $(-1)^k \det(A_k) > 0$ für $1 \leq k \leq n$ erfüllt ist.

Beweis: Die Matrix A ist genau dann negativ definit, wenn $-A$ positiv definit ist, denn für jedes $v \in V \setminus \{0_V\}$ ist ${}^{\mathrm{t}}vAv < 0$ äquivalent zu ${}^{\mathrm{t}}v(-A)v > 0$. Aus § 12 wissen wir, dass sich das Vorzeichen der Determinante ändert, wenn eine Zeile durch ihr Negatives ersetzt wird. Weil A_k aus k Zeilen besteht, gilt jeweils $\det(-A_k) = (-1)^k \det(A_k)$, für $1 \leq k \leq n$. Nach dem Hurwitz-Kriterium ist $-A$ genau dann positiv definit, wenn $\det(-A_k) > 0$ für $1 \leq k \leq n$ gilt, und auf Grund der Gleichung ist dies äquivalent zu $(-1)^k \det(A_k) > 0$ für $1 \leq k \leq n$. $\square$

In Verbindung mit der folgenden Aussage kann mit dem Hurwitz-Kriterium auch getestet werden, ob eine beliebige symmetrische Bilinearform auf einem endlich-dimensionalen $\mathbb{R}$-Vektorraum positiv definit ist.

(16.11) Proposition Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum und b eine symmetrische Bilinearform auf V. Sei $\mathscr{B}$ eine geordnete Basis von V und $A = \mathscr{M}_{\mathscr{B}}(b)$. Unter diesen Voraussetzungen ist b genau dann positiv definit, wenn A positiv definit ist.

Beweis: Nach Proposition (16.3) gilt $b(v,w) = {}^t\Phi_{\mathscr{B}}(v)A\Phi_{\mathscr{B}}(w)$ für alle $v,w \in V$. Weil die Koordinatenabbildung $\Phi_{\mathscr{B}}$ die Menge $V \setminus \{0_V\}$ der Vektoren ungleich null bijektiv auf $\mathbb{R}^n \setminus \{0_{\mathbb{R}^n}\}$ abbildet, gilt somit $b(v,v) > 0$ für alle $v \neq 0_V$ genau dann, wenn ${}^tvAv > 0$ für alle $v \neq 0_{\mathbb{R}^n}$ erfüllt ist. □

(16.12) Definition Eine Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ wird ***orthogonal*** genannt, wenn ${}^tAA = E_n$ gilt. Die orthogonalen Matrizen bilden eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$, die sogenannte ***orthogonale Gruppe*** $\mathscr{O}(n)$. Die Untergruppe $\mathrm{SO}(n) = \{A \in \mathscr{O}(n) \mid \det(A) = 1\}$ wird ***spezielle orthogonale Gruppe*** genannt.

Die Gleichung ${}^tAA = E_n$ zeigt, dass orthogonale Matrizen stets invertierbar sind; sie bilden also auf jeden Fall eine Teilmenge von $\mathrm{GL}_n(\mathbb{R})$. Die Gruppeneigenschaft folgt aus der Tatsache, dass für zwei orthogonale Matrizen A, B auch das Produkt AB und die inverse Matrix A^{-1} orthogonal sind. Denn aus ${}^tAA = E_n$ und ${}^tBB = E_n$ folgt ${}^tAB(AB) = {}^tB\,{}^tAAB = {}^tBE_nB = {}^tBB = E_n$, was zeigt, dass AB eine orthogonale Matrix ist. Für die Orthogonalität von A^{-1} schicken wir voraus, dass für jede Matrix $C \in \mathrm{GL}_n(\mathbb{R})$ Invertierung und Transposition vertauschbar sind. Denn die Rechnung ${}^tA\,{}^t(A^{-1}) = {}^t(A^{-1}A) = {}^tE_n = E_n$ zeigt, dass $({}^tA)^{-1} = {}^t(A^{-1})$ gilt. Aus ${}^tAA = E_n$ folgt außerdem ${}^tA = A^{-1}$ und $A\,{}^tA = E_n$. Damit erhalten wir schließlich ${}^t(A^{-1})A^{-1} = ({}^tA)^{-1}A^{-1} = (A\,{}^tA)^{-1} = E_n^{-1} = E_n$, wodurch die Orthogonalität von A^{-1} nachgewiesen ist.

Wichtige Beispiele für orthogonale Matrizen sind

$$D_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \text{ für } \alpha \in \mathbb{R} \quad , \quad S_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{und} \quad S_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Die Matrix D_α beschreibt die Drehung um den Nullpunkt mit Winkel α (gegen den Uhrzeigersinn), und S_x bzw. S_y beschreiben die Spiegelung an der x- bzw. y-Achse.

(16.13) Proposition Eine Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ ist genau dann orthogonal, wenn $\langle Av, Aw\rangle = \langle v, w\rangle$ für alle $v, w \in \mathbb{R}^n$ gilt.

Beweis: Sei $A \in \mathscr{M}_{n,\mathbb{R}}$ mit Spaltenvektoren $a_1, \ldots, a_n \in \mathbb{R}^n$. Offenbar ist eine Matrix A genau dann orthogonal, es gilt also ${}^tAA = E_n$ genau dann, wenn für $1 \leq k, \ell \leq n$ jeweils

$$\langle Ae_k, Ae_\ell\rangle \quad = \quad \langle a_k, a_\ell\rangle \quad = \quad \delta_{k\ell}$$

erfüllt ist, denn die Zahl $\langle a_k, a_\ell\rangle$ ist genau der Eintrag der Produktmatrix ${}^tAA$ an der Stelle (k,ℓ). Setzen wir diese Gleichung für alle k, ℓ voraus, dann folgt für $v, w \in \mathbb{C}^n$ mit $v = \sum_{k=1}^n \lambda_k e_k$ und $w = \sum_{\ell=1}^n \mu_\ell e_\ell$ jeweils

$$\langle Av, Aw\rangle \quad = \quad \left\langle A\left(\sum_{k=1}^n \lambda_k e_k\right), A\left(\sum_{\ell=1}^n \mu_\ell e_\ell\right)\right\rangle \quad = \quad \left\langle \sum_{k=1}^n \lambda_k Ae_k, \sum_{\ell=1}^n \mu_\ell Ae_\ell \right\rangle \quad =$$

$$\sum_{k=1}^n \sum_{\ell=1}^n \lambda_k \mu_\ell \langle Ae_k, Ae_\ell\rangle \quad = \quad \sum_{k=1}^n \sum_{\ell=1}^n \lambda_k \mu_\ell \delta_{k\ell} \quad = \quad \sum_{k=1}^n \lambda_k \mu_\ell \quad = \quad \langle v, w\rangle.$$

Setzen wir umgekehrt voraus, dass $\langle Av, Aw\rangle = \langle v, w\rangle$ für alle $v, w \in \mathbb{R}^n$ gilt, dann ist insbesondere

$$\langle Ae_k, Ae_\ell\rangle \quad = \quad \langle e_k, e_\ell\rangle \quad = \quad \delta_{k\ell} \qquad \text{für} \quad 1 \le k, \ell \le n. \qquad \square$$

(16.14) Definition Eine ***Bewegung*** im $\mathbb{R}^n$ ist eine bijektive, abstandserhaltende Abbildung $\phi : \mathbb{R}^n \to \mathbb{R}^n$, also eine bijektive Abbildung mit der Eigenschaft, dass $\|\phi(v) - \phi(w)\| = \|v - w\|$ für alle $v, w \in \mathbb{R}^n$ gilt.

Ein wichtige Klasse von Beispielen für Bewegungen sind die ***Translationen***, die Abbildungen der Form $\tau_u : \mathbb{R}^n \to \mathbb{R}^n$, $v \mapsto u + v$ mit einem festen Vektor $u \in \mathbb{R}^n$. Dass dies tatsächlich Bewegungen sind, erkennt man durch die Gleichung $\|\tau_u(v) - \tau_u(w)\| = \|(u + v) - (u + w)\| = \|v - w\|$, für beliebige $v, w \in \mathbb{R}^n$.

Entscheidend für den Beweis des folgenden Satzes ist die Beobachtung, dass man das euklidische Standard-Skalarprodukt aus der Längenfunktion $\|\cdot\|$ zurückgewinnen kann.

(16.15) Lemma Für alle $v, w \in \mathbb{R}^n$ gilt $\langle v, w\rangle = \frac{1}{2}\|v + w\|^2 - \frac{1}{2}\|v\|^2 - \frac{1}{2}\|w\|^2$.

Beweis: Dies ergibt sich aus der Rechnung

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

und anschließender Multiplikation der Gleichung mit dem Faktor $\frac{1}{2}$. $\square$

(16.16) Lemma Sei $\psi : \mathbb{R}^n \to \mathbb{R}^n$ eine Abbildung mit $\langle \psi(v), \psi(w)\rangle = \langle v, w\rangle$ für alle $v, w \in \mathbb{R}^n$. Dann gibt es eine Matrix $A \in \mathcal{O}(n)$ mit $\psi = \phi_A$, insbesondere ist ψ linear.

Beweis: Aus der Voraussetzung folgt, dass mit $(e_1, \ldots, e_n)$ auch die Menge $(\psi(e_1), \ldots, \psi(e_n))$ eine ON-Basis des $\mathbb{R}^n$ ist. Sei $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$ beliebig vorgegeben, und seien $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit $\psi(v) = \sum_{j=1}^n \lambda_j \psi(e_j)$. Dann gilt für $1 \le j \le n$ jeweils

$$\langle \psi(v), \psi(e_j)\rangle \quad = \quad \left\langle \sum_{i=1}^n \lambda_i \psi(e_i)\ ,\ \psi(e_j) \right\rangle \quad = \quad \sum_{i=1}^n \lambda_i \langle \psi(e_i), \psi(e_j)\rangle \quad = \quad \sum_{j=1}^n \lambda_i \delta_{ij} \quad = \quad \lambda_j$$

und somit

$$\psi(v) \quad = \quad \sum_{j=1}^n \lambda_j \psi(e_j) \quad = \quad \sum_{j=1}^n \langle \psi(v), \psi(e_j)\rangle \psi(e_j) \quad = \quad \sum_{j=1}^n \langle v, e_j\rangle \psi(e_j) \quad = \quad \sum_{j=1}^n v_j \psi(e_j).$$

Mit Hilfe dieser Gleichung lässt sich um leicht überprüfen, dass ψ linear ist. Sind nämlich $v, w \in \mathbb{R}^n$ und $\alpha \in \mathbb{R}$ vorgegeben, dann gilt

$$\psi(v + w) \quad = \quad \sum_{j=1}^n (v_j + w_j)\psi(e_j) \quad = \quad \sum_{j=1}^n v_j \psi(e_j) + \sum_{j=1}^n w_j \psi(e_j) \quad = \quad \psi(v) + \psi(w)$$

und ebenso $\psi(\alpha v) = \sum_{j=1}^{n}(\alpha v_j)\psi(e_j) = \alpha\sum_{j=1}^{n} v_j\psi(e_j) = \alpha\psi(v)$. Bezeichnet nun $A \in \mathscr{M}_{n,\mathbb{R}}$ die Matrix mit den Spalten $\psi(e_1), \ldots, \psi(e_n)$, dann gilt also $\psi(v) = \phi_A(v)$ für alle $v \in \mathbb{R}^n$. Wegen $\langle v, w\rangle = \langle \psi(v), \psi(w)\rangle = \langle \phi_A(v), \phi_A(w)\rangle = \langle Av, Aw\rangle$ ist die Matrix A nach Proposition (16.13) orthogonal. □

(16.17) Satz Die Bewegungen in $\mathbb{R}^n$ sind genau die Abbildungen der Form $\tau_u \circ \phi_A$, mit $u \in \mathbb{R}^n$ und $A \in \mathscr{O}(n)$. Die Darstellung dieser Form ist eindeutig. Liegt A sogar in $\mathrm{SO}(n)$, dann spricht man von einer ***orientierungserhaltenden***, ansonsten von einer ***orientierungsumkehrenden*** Bewegung.

Beweis: Sei nun $\phi : \mathbb{R}^n \to \mathbb{R}^n$ eine beliebige Bewegung und $u = \phi(0_{\mathbb{R}^n})$. Wie man leicht überprüft, ist dann auch $\psi = \tau_u^{-1} \circ \phi$ eine Bewegung, mit $\psi(0_{\mathbb{R}^n}) = 0_{\mathbb{R}^n}$. Für alle $v \in \mathbb{R}^n$ gilt außerdem $\|\psi(v)\| = \|\psi(v) - 0_{\mathbb{R}^n}\| = \|\psi(v) - \psi(0_{\mathbb{R}^n})\| = \|v - 0_{\mathbb{R}^n}\| = \|v\|$. Mit Hilfe des Lemmas erhalten wir für alle $v, w \in \mathbb{R}^n$ jeweils

$$\begin{aligned}\langle \psi(v), \psi(w)\rangle &= -\langle \psi(v), -\psi(w)\rangle = -\tfrac{1}{2}\|\psi(v) - \psi(w)\|^2 + \tfrac{1}{2}\|\psi(v)\|^2 + \tfrac{1}{2}\|-\psi(w)\|^2 = \\ &-\tfrac{1}{2}\|\psi(v) - \psi(w)\|^2 + \tfrac{1}{2}\|\psi(v)\|^2 + \tfrac{1}{2}\|\psi(w)\|^2 = -\tfrac{1}{2}\|v - w\|^2 + \tfrac{1}{2}\|v\|^2 + \tfrac{1}{2}\|w\|^2 = \\ &-\tfrac{1}{2}\|v - w\|^2 + \tfrac{1}{2}\|v\|^2 + \tfrac{1}{2}\|-w\|^2 = -\langle v, -w\rangle = \langle v, w\rangle.\end{aligned}$$

Nach Lemma (16.16) existiert also eine orthogonale Matrix A mit $\psi = \phi_A$. Insgesamt erhalten wir somit durch Einsetzen die Gleichung $\phi = \tau_u \circ \psi = \tau_u \circ \phi_A$. □

Beispiele für orientierungserhaltende Bewegungen sind die Drehungen im $\mathbb{R}^2$ um einen beliebig gewählten Punkt. Orientierungsumkehrende Bewegungen sind zum Beispiel die Spiegelungen an beliebigen affinen Geraden.

(16.18) Definition Sei (V, b) ein euklidischer Vektorraum. Man bezeichnet einen Endomorphismus ϕ von V als ***orthogonal***, wenn $b(\phi(v), \phi(w)) = b(v, w)$ für alle $v, w \in V$ gilt, und ***symmetrisch*** oder auch ***selbstadjungiert***, wenn $b(\phi(v), w) = b(v, \phi(w))$ für alle $v, w \in V$ gilt.

Wir zeigen, dass auch diese Eigenschaften wieder an der Darstellungsmatrix von ϕ bezüglich einer ON-Basis von V abgelesen werden können.

(16.19) Lemma Eine Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ ist symmetrisch genau dann, wenn $\langle Av, w\rangle = \langle v, Aw\rangle$ für alle $v, w \in \mathbb{R}^n$ erfüllt ist.

Beweis: Seien $a_{\bullet 1}, \ldots, a_{\bullet n}$ die Spaltenvektoren von A. Es gilt $\langle Ae_k, e_\ell\rangle = \langle a_{\bullet k}, e_\ell\rangle = a_{\ell k}$ und $\langle e_k, Ae_\ell\rangle = \langle e_k, a_{\bullet \ell}\rangle = a_{k\ell}$ für $1 \le k, \ell \le n$. Dies zeigt, dass die Matrix A symmetrisch ist, wenn $\langle Av, w\rangle = \langle v, Aw\rangle$ für alle $v, w \in \mathbb{R}^n$ gilt. Setzen wir umgekehrt die Symmetrie von A voraus, dann gilt $\langle Ae_k, e_\ell\rangle = \langle e_k, Ae_\ell\rangle$ für $1 \le k, \ell \le n$. Sind nun $v, w \in \mathbb{R}^n$

beliebige Vektoren, $v = \sum_{k=1}^{n} v_k e_k$ und $w = \sum_{\ell=1}^{n} w_\ell e_\ell$, dann folgt

$$\begin{aligned}\langle Av, w\rangle &= \sum_{k=1}^{n} v_k \langle Ae_k, w\rangle = \sum_{k=1}^{n}\sum_{\ell=1}^{n} v_k w_\ell \langle Ae_k, e_\ell\rangle = \sum_{k=1}^{n}\sum_{\ell=1}^{n} v_k w_\ell \langle e_k, Ae_\ell\rangle \\ &= \sum_{k=1}^{n} v_k \langle e_k, Aw\rangle = \langle v, Aw\rangle. \end{aligned}$$

□

(16.20) Proposition Sei (V, b) ein euklidischer Vektorraum, $\mathscr{B}$ eine ON-Basis von V, $\phi : V \to V$ ein Endomorphismus und $A = \mathscr{M}_{\mathscr{B}}(\phi)$. Der Endomorphismus ϕ ist genau dann orthogonal, wenn A orthogonal ist und genau dann selbstadjungiert, wenn A symmetrisch ist.

Beweis: Sei $\Phi_{\mathscr{B}} : V \to \mathbb{R}^n$ die Koordinatenabbildung. Weil $\mathscr{B}$ eine ON-Basis bezüglich b ist, gilt $\mathscr{M}_{\mathscr{B}}(b) = E_n$. Nach Proposition (16.3) gilt damit

$$b(v, w) = {}^{\mathrm{t}}\Phi_{\mathscr{B}}(v) E_n \Phi_{\mathscr{B}}(w) = \langle \Phi_{\mathscr{B}}(v), \Phi_{\mathscr{B}}(w)\rangle$$

für alle $v, w \in V$. Nach Definition der Darstellungsmatrix eines Endomorphismus gilt $\Phi_{\mathscr{B}}(\phi(v)) = A\Phi_{\mathscr{B}}(v)$ für alle $v \in V$, also $b(\phi(v), \phi(w)) = \langle A\Phi_{\mathscr{B}}(v), A\Phi_{\mathscr{B}}(w)\rangle$ für alle $v, w \in V$. Insgesamt zeigt dies, dass die Gleichung $b(\phi(v), \phi(w)) = b(v, w)$ für alle $v, w \in V$ äquivalent ist zu $\langle Av, Aw\rangle = \langle v, w\rangle$ für alle $v, w \in \mathbb{R}^n$. Ebenso ist $b(\phi(v), w) = b(v, \phi(w))$ äquivalent zu $\langle Av, w\rangle = \langle v, Aw\rangle$ für alle $v, w \in V$. □

Das euklidische Standard-Skalarprodukt, das wir zu Beginn eingeführt haben, lässt sich durch

$$\langle v, w\rangle = \sum_{k=1}^{n} \bar{v}_k w_k \qquad \text{für} \quad v = (v_1, ..., v_n),\ w = (w_1, ..., w_n)$$

zu einer Abbildung $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ ausdehnen. Wie man durch Nachrechnen unmittelbar überprüft, hat diese die Eigenschaft

$$\langle v + v', w\rangle = \langle v, w\rangle + \langle v', w\rangle \quad , \quad \langle v, w + w'\rangle = \langle v, w\rangle + \langle v, w'\rangle \quad , \quad \langle \lambda v, w\rangle = \bar{\lambda}\langle v, w\rangle \quad ,$$
$$\langle v, \lambda w\rangle = \lambda\langle v, w\rangle \qquad \text{und} \qquad \langle w, v\rangle = \overline{\langle v, w\rangle}$$

für alle $v, v', w, w' \in \mathbb{C}^n$ und $\lambda \in \mathbb{C}$, wobei $\bar{\lambda}$ jeweils die zu λ konjugiert-komplexe Zahl bezeichnet. Die Abbildung $\langle \cdot, \cdot \rangle$ ist „halb linear“ in der ersten Komponente (nur halb, weil das Skalar λ beim Herausziehen der komplexen Konjugation unterworfen wird) und linear in der zweiten Komponente. Auf Grund dieser Tatsache spricht man einer ***hermiteschen Sesquilinearform*** („anderthalbfach lineare Form“) auf dem Vektorraum $\mathbb{C}^n$.

(16.21) Proposition Jede symmetrische Matrix $A \in \mathscr{M}_{n,\mathbb{R}}$ besitzt einen reellen Eigenwert.

Beweis: Wir setzen als bekannt voraus, dass jedes Polynom in $\mathbb{C}[x]$ vom Grad ≥ 1 eine Nullstelle besitzt. Fassen wir das charakteristische Polynom χ_A von A als komplexes Polynom auf, dann liefert uns das die Existenz einer Nullstelle $\lambda \in \mathbb{C}$ von χ_A. Daraus folgt, dass der Endomorphismus $\phi : \mathbb{C}^n \to \mathbb{C}^n$, $v \mapsto Av$ den Wert λ als Eigenwert besitzt.

Sei $v \in \mathbb{C}^n$ ein beliebiger zugehöriger Eigenvektor, und $v = u + iw$ seine Zerlegung in Real- und Imaginärteil, mit $u, w \in \mathbb{R}^n$. Es gilt nun

$$\begin{aligned}\bar{\lambda}\langle v, v\rangle &= \langle \lambda v, v\rangle = \langle Av, v\rangle = \langle A(u+iw), u+iw\rangle = \langle Au, u\rangle + \langle Au, iw\rangle + \langle A(iw), u\rangle + \langle A(iw), iw\rangle \\ &= \langle Au, u\rangle + i\langle Au, w\rangle - i\langle Aw, u\rangle + \langle Aw, w\rangle = \langle u, Au\rangle + i\langle u, Aw\rangle - i\langle w, Au\rangle + \langle w, Aw\rangle = \\ &\langle u, Au\rangle + \langle u, A(iw)\rangle + \langle iw, Au\rangle + \langle iw, A(iw)\rangle = \langle v, Av\rangle = \langle v, \lambda v\rangle = \lambda\langle v, v\rangle.\end{aligned}$$

Division dieser Gleichung durch $\langle v, v\rangle \neq 0$ liefert $\bar{\lambda} = \lambda$. Die Nullstelle λ von χ_A ist also reell. □

Wir erhalten das folgenden fundamentale Resultat über symmetrische Matrizen.

(16.22) Satz *(Hauptachsentransformation)*
Sei $A \in \mathcal{M}_{n,\mathbb{R}}$ symmetrisch. Dann gibt es eine orthogonale Matrix T, so dass $D = {}^tTAT$ eine Diagonalmatrix ist.

Beweis: Sei (V, b) ein endlich-dimensionaler euklidischer $\mathbb{R}$-Vektorraum. Wir beweisen durch vollständige Induktion über $n = \dim V$ die folgende Aussage: Ist $\phi : V \to V$ ein selbstadjungierter Endomorphismus, dann gibt es eine ON-Basis $\mathcal{B}$ von V bestehend aus Eigenvektoren von ϕ. Für $n = 1$ ist jeder Vektor $v \in V$ mit $v \neq 0_V$ zwangsläufig ein Eigenvektor. Setzen wir $v_1 = \frac{1}{\|v\|_b} v$ und $\mathcal{B} = (v_1)$, so ist $\mathcal{B}$ eine Basis mit der gewünschten Eigenschaft.

Sei nun $n \in \mathbb{N}$ und $\dim V = n+1$, und setzen wir die Aussage für n voraus. Sei $\mathcal{B}$ eine ON-Basis von V. Weil ϕ selbstadjungiert ist, ist $A = \mathcal{M}_{\mathcal{B}}(\phi)$ nach Proposition (16.20) eine symmetrische Matrix. Nach Proposition (16.21) besitzt A einen reellen Eigenwert λ; damit gilt dasselbe auch für die Abbildung ϕ. Sei $v \in V$ ein zugehöriger Eigenvektor und $v_1 = \frac{1}{\|v\|} v$. Offenbar ist durch

$$U = \{w \in V \mid b(v_1, w) = 0\}$$

ein Untervektorraum V gegeben. Es gilt $\phi(U) \subseteq U$, denn für alle $w \in U$ gilt $b(v_1, \phi(w)) = b(\phi(v_1), w) = b(\lambda v_1, w) = \lambda b(v_1, w) = \lambda \cdot 0 = 0$ und somit $\phi(w) \in U$. Damit ist durch $\phi|_U$ ein selbstadjungierter Endomorphismus von U gegeben. Außerdem ist $\dim U = n$. Denn die lineare Abbildung $\psi : V \to \mathbb{R}$, $w \mapsto b(v_1, w)$ hat U als Kern und ist wegen $\psi(\alpha v_1) = b(v_1, \alpha v_1) = \alpha b(v_1, v_1) = \alpha$ für alle $\alpha \in \mathbb{R}$ surjektiv. Damit folgt $\dim U = \dim \ker(\psi) = \dim V - \dim \mathbb{R} = (n+1) - 1 = n$.

Wir können nun die Induktionsvoraussetzung auf den Endomorphismus $\phi|_U$ anwenden und erhalten eine ON-Basis $(v_2, ..., v_{n+1})$ von U bestehend aus Eigenvektoren von $\phi|_U$. Wegen $v_1 \perp_b v_k$ für $2 \leq k \leq n+1$ ist $\mathcal{B} = (v_1, ..., v_n)$ eine ON-Basis von V mit der gewünschten Eigenschaft.

Sei nun ϕ der Endmorphismus von $\mathbb{R}^n$ gegeben durch $\phi : \mathbb{R}^n \to \mathbb{R}^n$, $v \mapsto Av$ mit der vorgegebenen Matrix A. Es gilt dann $A = \mathcal{M}_{\mathcal{E}}(\phi)$ bezüglich der Einheitsbasis $\mathcal{E} = (e_1, ..., e_n)$ von $\mathbb{R}^n$. Nach Proposition (16.20) ist ϕ selbstadjungiert bezüglich des euklidischen Standard-Skalarprodukts. Durch Anwendung der soeben bewiesenen Aussage erhalten wir eine ON-Basis $\mathcal{B} = (v_1, ..., v_n)$ bestehend aus Eigenvektoren von ϕ. Damit ist $D = \mathcal{M}_{\mathcal{B}}(\phi)$ dann eine Diagonalmatrix.

Tragen wir die Vektoren $v_1, ..., v_n$ als Spalten in eine Matrix T ein, so gilt $T = \mathcal{T}_{\mathcal{E}}^{\mathcal{B}}$, und T ist orthogonal, weil die Spalten von T eine ON-Basis von $\mathbb{R}^n$ bilden. Es gilt also ${}^tT = T^{-1} = \mathcal{T}_{\mathcal{B}}^{\mathcal{E}}$. Mit dem Satz (11.16) vom Basiswechsel erhalten wir $D = \mathcal{M}_{\mathcal{B}}(\phi) = \mathcal{T}_{\mathcal{B}}^{\mathcal{E}} \mathcal{M}_{\mathcal{E}}(\phi) \mathcal{T}_{\mathcal{E}}^{\mathcal{B}} = {}^tTAT$. □

Der Vollständigkeit halber sei noch erwähnt, dass in Analogie zu den orthogonalen und den symmetrischen Matrizen die folgenden Begriffe im Komplexen existieren.

(16.23) Definition Eine Matrix $A \in \mathcal{M}_{n,\mathbb{C}}$ heißt ***unitär***, wenn ${}^t\bar{A}A = E_n$ und ***hermitesch***, wenn ${}^t\bar{A} = A$ gilt. Wie die orthogonalen bilden auch die unitären Matrizen bilden eine Gruppe, die sog. unitäre Gruppe $\mathrm{U}(n)$.

In Analogie zu den euklidischen $\mathbb{R}$-Vektorräumen betrachtet man ***unitäre*** $\mathbb{C}$-Vektorräume. Diese sind mit einer hermiteschen Sesquilinearform b ausgestattet, die außerdem wieder *positiv definit* ist, also $b(v, v) > 0$ für alle Vektoren v ungleich null erfüllt. Den unitären Matrizen entsprechen die *unitären Automorphismen* eines solchen Vektorraums, die hermiteschen Matrizen den (komplex) selbstadjungierten Endomorphismen.

Auch auf unitären $\mathbb{C}$-Vektorräumen kann mit geometrischen Begriffen gearbeitet werden. Man arbeitet mit ihnen beispielsweise in der Quantenmechanik, wo die unitären Automorphismen die Zeitentwicklung und Symmetrien eines quantenmechanischen Systems modellieren, während die selbstadjungierten Endomorphismen zur Beschreibung von sog. „Obervablen“, also physikalischen Messgrößen des Systems (wie etwa Ort, Impuls oder Energie eines Teilchens) dienen. Der Messvorgang wird modelliert durch die Projektion auf einen Eigenraum des selbstadjungierten Endomorphismus.

Übrigens ist die wegen der geometrischen Anwendungen erwünschte Eigenschaft „positiv definit“ der Grund, weshalb man über $\mathbb{C}$ an Stelle von Bilinearformen die Sesquilinearformen betrachtet. Positiv definite Bilinearformen auf einem $\mathbb{C}$-Vektorraum $V \neq \{0_V\}$ gibt es nicht, weil für jede Bilinearform b und jeden Vektor v stets $b(iv, iv) = ib(v, iv) = i^2 b(v, v) = -b(v, v)$ gilt. Es treten also immer positive und negative Werte auf, sobald b überhaupt Werte ungleich null annimmt.

Literaturverzeichnis

[Bo] S. Bosch, *Lineare Algebra*. Springer-Lehrbuch, Berlin 2006.

[dJ] T. de Jong, *Lineare Algebra*. Pearson-Studium, München 2013.

[Fi] G. Fischer, *Lernbuch Lineare Algebra und Geometrie*. Vieweg-Teubner, Wiesbaden 2011.

[Jn] K. Jaenich, *Lineare Algebra*. Springer-Verlag, Berlin 2001.